A L G E B R A I S K T A L T E O R I

Forår 1998

Forelæsninger ved Asmus L. Schmidt

KØBENHAVNS UNIVERSITET MATEMATISK AFDELING

Januar 1998

Asmus Schmidt, Algebraisk talteori, 2. oplag, marts 2004.

Indhold

0 Indledning **0.1**

1 Algebraiske udvidelser **1.1**
Norm og spor 1.6
Diskriminant 1.10
Galoisteori 1.12
Opgaver 1.20

2 Dedekindringe **2.1**
Noetherske ringe og Noetherske moduler 2.2
Hele elementer 2.9
Brudne idealer 2.12
Bevis for Sætning 16 (Karakterisering af Dedekindringe) 2.16
Bevis for Sætning 17 (Udvidelser af Dedekindringe) 2.24
Andre sætninger om Dedekindringe 2.29
Valuationer med henblik på Dedekindringe 2.39
Opgaver 2.42

3 Klassiske Dedekindringe **3.1**
Primidealer i kvadratiske tallegemer 3.10
Minkowski's sætninger 3.18
Klassegruppe og klassetal 3.25
Mordell's ligning 3.30
Imaginært kvadratiske tallegemer med klassetal 1 . . . . . 3.33
Euklidiske ringe 3.37
Dirichlet's enhedssætning 3.42

Bestemmelse af enheder 3.56
Regulatoren 3.62
Opgaver 3.65

4 Cirkeldelingslegemer. Kummer's sætning 4.1
Kummer's sætning 4.7
Opgaver 4.14

5 Dedekind's zeta-funktion 5.1
Dirichlet karakterer 5.12
L-rækker og Euler produkter 5.26
Summation af L-rækker 5.37
Klassetalsformler for kvadratiske tallegemer 5.40
Klassetalsformler for cirkeldelingslegemer 5.43
Opgaver 5.47

B Blandede opgaver B.1

P Programmer P.1
PARI-programmet UNITS P.1
PARI-programmet KUMMER P.2
PARI-programmet CLASSNBS P.4

A Alfabeter A.1

L Litteratur L.1

I Indeks I.1

0. Indledning

Den franske amatørmatematiker P. Fermat (1601-1665) blev interesseret i talteori bl.a. ved læsning i Bachet's latinske oversættelse (1621) af Diophantus' *Arithmetica* (ca. 250 f. Kr.). Ud for Arithmetica, bog 2, opgave 8, der handler om at dele et kvadrat i to kvadrater, skriver Fermat i margin de berømte ord:

"På den anden side er det umuligt at dele et kubiktal i to kubiktal eller et bikvadrat (fjerdepotens) i to bikvadrater, eller generelt en hvilkensomhelst potens – bortset fra et kvadrat – i to potenser med samme eksponent. Jeg har opdaget et vidunderligt bevis for dette, men denne margin er for lille til at indeholde det."

Fermat påstår altså, at ligningen

$$x^n + y^n = z^n,$$

for $n \in \mathbb{N},\ n \geq 3$, ikke har nogen løsning $(x, y, z) \in \mathbb{N}^3$.

Det eneste tilfælde, for hvilket Fermat (i breve) har leveret et bevis for uløsbarheden, er $n = 4$. Beviset føres inden for talringen $\mathbb{Z}$ ved en såkaldt *descente infinie* og benytter afgørende den entydige faktorisering af naturlige tal som produkt af primtal.

Fermat efterlod derfor følgende berømte problem: at vise uløsbarheden i naturlige tal for ligningen

$$(*) \qquad x^p + y^p = z^p,$$

når p er et ulige primtal. Dette problem kaldes ofte *Fermat's sidste sætning.*

L. Euler (1707-1783) betragtede tilfældet $p = 3$, som han kunne klare ved regninger i $\mathbb{Z}$. Hans metode svarer (som noteret af Gauss) til at regne i talringen $\mathbb{Z} + \mathbb{Z}\frac{1}{2}(1 + \sqrt{-3})$, som ligeledes har entydig faktorisering i primelementer.

I sit monumentale ungdomsværk *Disquisitiones Arithmeticae*, Leipzig 1801, behandlede C. F. Gauss (1777-1855) en række emner, som fik den allerstørste betydning for den senere udvikling af algebraisk talteori. For det første giver Gauss en systematisk teori for kvadratiske rester, herunder (flere) beviser for reciprocitetssætningen. Hovedemnet i *Disquisitiones* er teorien for kvadratiske former over $\mathbb{Z}$ i to og tre variable (inklusive genusteori samt klassegrupper og klassetal). Denne teori var et afgørende udgangspunkt for opbygningen af algebraisk talteori. Endvidere spiller teorien for gaussiske summer en vigtig rolle i den analytiske del af algebraisk talteori. Endelig bør nævnes Gauss'

konstruktion af den regulære 17-kant, som foregreb Galoisteorien, der har central betydning – også i algebraisk talteori.

Gauss' nære medarbejder (og efterfølger i Göttingen) P. G. L. Dirichlet (1805-1859) bidrog på væsentlige punkter til udvikling af algebraisk og analytisk talteori. Hvad angår Fermats problem, viste han uløsbarheden for $p = 5$. I 1837 viste han det berømte resultat, at enhver primisk restklasse modulo n ($n \in \mathbb{N}$) indeholder uendelig mange primtal, ved at betragte *Dirichlet karakterer* χ på den primiske restklassegruppe (starten på gruppere præsentationsteori) og dertil hørende *L-rækker*:

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} \quad \text{for} \quad s > 1.$$

I sammenhæng hermed viste han også analytiske formler for klassetal for kvadratiske former. Dirichlet anses derfor for grundlæggeren af den analytiske talteori.

I 1847 viste han et andet berømte resultat, nemlig *Dirichlets enhedssætning*, der nøje beskriver strukturen af gruppen af enheder i et algebraisk tallegeme. Kort forinden (1845) havde Kummers daværende elev L. Kronecker (1823-1891) dog vist denne sætning i det vigtige specialtilfælde, hvor det algebraiske tallegeme er et cirkeldelingslegeme $\mathbb{Q}(e^{2\pi i/n})$.

Ved forsøg på at vise uløsbarheden af (*) for et ulige primtal p, tvinges man (som Gauss og Dirichlet) til at udvide $\mathbb{Z}$ til en talring $R = \mathbb{Z}[r]$, hvori (*) kan faktoriseres

$$(x + y)(x + ry)(x + r^2 y) \dots (x + r^{p-1} y) = z^p.$$

Men der dukker da et nyt problem op, idet det viser sig, at det naturlige bud på en sådan talring

$$R = \{a_0 + a_1 r + a_2 r^2 + \cdots + a_{p-1} r^{p-1} | a_0, a_1, \dots, a_{p-1} \in \mathbb{Z}\},$$

hvor $r = e^{2\pi i/p}$, kun for $p \leq 19$ har entydig faktorisering i primelementer.

Den tyske matematiker E. E. Kummer (1810-1893) løste dette problem ved at udvide tallene i R med såkaldte *ideale tal*, således at der for disse gælder entydig primidealfaktorisering.

Kummers berømte resultat (1847) – som senere indbragte ham en af *Acadèmie des Sciences de Paris* udsat guldmedalje for en løsning af Fermatproblemet – er følgende:

A. Fermats ligning (*) er uløsbar, når p er et *regulært* primtal, dvs p ikke går op i ordenen h for den af Kummer indførte klassegruppe hørende til ringen R.

B. Et ulige primtal p er regulært, hvis og kun hvis p ikke går op i nogen af tællerne i Bernoullitallene $B_2, B_4, \ldots, B_{p-3}$.

Her er *Bernoullitallene* B_n, $n \geq 1$, rationale tal givet ved de symbolske formler

$$(1+B)^m = B^m \quad \text{for} \quad m \geq 2,$$

eller eksplicit ved

$$1 + \binom{m}{1} B_1 + \cdots + \binom{m}{m-1} B_{m-1} + B_m = B_m.$$

F. eks. er

$$B_1 = -\tfrac{1}{2},\ B_2 = \tfrac{1}{6},\ B_4 = -\tfrac{1}{30},\ B_6 = \tfrac{1}{42},\ B_8 = -\tfrac{1}{30},\ B_{10} = \tfrac{5}{66}.$$

Det er bevist, at der er uendelig mange ikke regulære primtal (det mindste er 37), men det er ukendt om der er uendelig mange regulære primtal.

Ved supplerende meget omfattende undersøgelser af Bernoullital og små divisorer i disse har man (før Andrew Wiles) kunnet vise uløsbarheden af (*) for alle ulige primtal $p < 4.000.000$.

Det bør nævnes, at resultater af G. Faltings (1983) inden for algebraisk geometri har som konsekvens, at Fermats ligning for givet $n \geq 3$ kun har endelig mange løsninger $(x, y, z) \in \mathbb{N}^3$ med x, y, z indbyrdes primiske.

Andrew Wiles' generelle bevis (1995) for Fermats sidste sætning – altså uløsbarheden af (*) for alle ulige primtal p – benytter på væsentlig måde elliptiske kurver og modulære grupper og funktioner.

For en omfattende beskrivelse af den rolle Fermatproblemet har spillet for udviklingen af algebraisk talteori henvises til H. M. Edwards: *Fermat's Last Theorem*, 1977.

B. Riemann (1826-1866) publicerede i 1859 sit eneste arbejde om talteori: *Über die Anzahl der Primzahlen unter einer gegebene Grösse*. Med udgangspunkt i Eulers formel

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \sum_{n=1}^{\infty} n^{-s}$$

indfører Riemann den komplekse funktion $\zeta(s)$, der nu kaldes *Riemanns ζ-funktion*. Han viser bl.a. *funktionalligningen* for $\zeta(s)$:

$$F(s) = F(1-s), \quad \text{hvor} \quad F(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s),$$

og $\Gamma(s)$ er *Eulers* Γ*-funktion*. Derefter fremsætter han den berømte hypotese, at alle ikke trivielle nulpunkter for $\zeta(s)$ ligger på linien $\Re s = \frac{1}{2}$.

R. Dedekind (1831-1916) videreførte de nævnte ideer hos Gauss, Dirichlet, Kummer og Riemann. I det over 200 sider lange *Supplement* 11: *Über die Theorie der ganzen algebraischen Zahlen* til 3. udgave af Dirichlet: *Vorlesungen über Zahlentheorie* (1879), indfører Dedekind idealer, som vi kender dem i dag. Han viser bl.a. det fundamentale resultat, at ringen R af hele elementer i et algebraisk tallegeme har entydig primidealfaktorisering. Endvidere indfører han på naturlig måde en ζ-funktion (nu kaldet *Dedekind's* ζ*-funktion*) for ethvert algebraisk tallegeme, og han viser sin berømte analytiske klassetalsformel relateret til denne funktion.

H. Minkowski (1864-1909) indførte i sin berømte bog *Geometrie der Zahlen* (1896) en ny matematisk disciplin: *geometrisk talteori*, der kombinerer geometriske egenskaber ved figurer med talteoretiske. Som demonstreret af Minkowski har denne teori har en række anvendelser i algebraisk talteori, inden for diophantisk approksimation (titlen på en anden bog af Minkowski) og i teorien for kvadratiske former i n variable over $\mathbb{Z}$.

D. Hilbert (1862-1943) giver (1897) en sammenfattende beskrivelse af algebraisk talteori i den næsten 400 sider lange afhandling *Die Theorie der algebraischen Zahlkörper* i Jahresberichte der Deutschen Mathematikervereinigung, kendt som "Hilberts Zahlbericht". Denne fremstilling har haft afgørende indflydelse på den senere udvikling af algebraisk talteori. Hilbert valgte i sin fremstilling at lægge idealteorien til grund, og han forbigik derved anvendelsen af *p-adisk analyse*, en teori, der var udviklet sideløbende med idealteorien af Kummer, Kronecker og K. Hensel (1861-1941). (Jf A. Weil's kritiske bemærkninger til Hilberts Zahlbericht i indledningen til E. E. Kummer: *Collected Papers*, 1975.)

I øvrigt fik Hensels bog: *Theorie der algebraischen Zahlen* (1908) stor betydning for den videre udvikling af denne teori, nu kendt under betegnelsen *valuationsteori*. Mange nutidige fremstillinger af algebraisk talteori (fx Z. I. Borevich, I. R. Shafarevich: *Number Theory*, 1966) er baseret på valuationsteori.

Det er en interessant historisk omstændighed, at Kronecker udviklede en tredie ramme om algebraisk talteori, nemlig *divisor teori*, men denne forblev næsten ukendt. (Jf. H. M. Edwards: *Divisor Theory*, 1990.)

Blandt de mange betydende matematikere, som har videreført algebraisk talteori i dette århundrede skal nævnes: E. Noether, E. Artin og H. Hasse.

1. Algebraiske udvidelser

I det følgende er alle legemer *kommutative*. Når to legemer k og K opfylder relationen $k \subseteq K$, kaldes k et *dellegeme* af K og K et *udvidelseslegeme* for k.

En *relativ* udvidelse $k \subseteq K$ kaldes en *absolut* udvidelse, når *grundlegemet* k er et *primlegeme*, dvs. $k = \mathbb{Q}$, når karakteristikken er 0, og $k = \mathbb{F}_p$, når karakteristikken er p.

I situationen $k \subseteq K$ kaldes et element $\alpha \in K$ *algebraisk* over k, hvis α er nulpunkt i et egentligt polynomium $f \in k[x]$. K siges at være en *algebraisk* udvidelse af k, hvis ethvert $\alpha \in K$ er algebraisk over k.

For en relativ udvidelse $k \subseteq K$ kan K på naturlig måde opfattes som et vektorrum over k. Vektorrumsdimensionen for K over k betegnes $[K : k]$ og kaldes *graden* af udvidelsen. En udvidelse $k \subseteq K$ kaldes *endelig*, hvis $[K : k] \in \mathbb{N}$. Et *tallegeme* er et dellegeme af $\mathbb{C}$. Det kaldes et *algebraisk tallegeme*, hvis graden over $\mathbb{Q}$ er endelig.

Sætning 1. *Når $[K : k] \in \mathbb{N}$, er K algebraisk over k.*

Bevis. Lad $[K : k] = n$, og lad $\alpha \in K$ være vilkårligt. Da er sættet

$$(1, \alpha, \alpha^2, \ldots, \alpha^n)$$

lineært afhængigt over k, men dette betyder netop, at α er nulpunkt i et egentligt polynomium af grad $\leq n$ i $k[x]$. □

Sætning 2. *(Kæderegel for endelige udvidelser). Lad $k \subseteq K \subseteq L$ være legemer med $[K : k] = m \in \mathbb{N}, [L : K] = n \in \mathbb{N}$. Såfremt $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ er en basis for K/k, og $(\beta_1, \beta_2, \ldots, \beta_n)$ er en basis for L/K, så betemmer*

$$(*) \qquad \{\alpha_\mu \beta_\nu \mid 1 \leq \mu \leq m, 1 \leq \nu \leq n\}$$

en basis for L/k. Specielt gælder produktformlen

$$[L : k] = [L : K][K : k].$$

Bevis. Lad $\vartheta \in L$. Da kan ϑ skrives som

$$\vartheta = \sum_{\nu=1}^{n} \kappa_\nu \beta_\nu, \quad \kappa_\nu \in K.$$

Her kan hvert κ_ν skrives på formen

$$\kappa_\nu = \sum_{\mu=1}^{m} k_{\mu\nu}\alpha_\mu, \quad k_{\mu\nu} \in k.$$

Følgelig er

$$\vartheta = \sum_{\nu=1}^{n}\sum_{\mu=1}^{m} k_{\mu\nu}\alpha_\mu\beta_\nu,$$

hvorfor sættet (*) frembringer L/k.

For at vise at (*) er et lineært uafhængigt sæt over k betragtes en vilkårlig lineær relation

$$\sum_{\nu=1}^{n}\sum_{\mu=1}^{m} k_{\mu\nu}\alpha_\mu\beta_\nu = 0, \quad k_{\mu\nu} \in k.$$

Af omskrivningen

$$\sum_{\nu=1}^{n}\left(\sum_{\mu=1}^{m} k_{\mu\nu}\alpha_\mu\right)\beta_\nu = 0$$

følger, at

$$\sum_{\mu=1}^{m} k_{\mu\nu}\alpha_\mu = 0 \quad \text{for} \quad 1 \le \nu \le n,$$

og derfor at

$$k_{\mu\nu} = 0 \quad \text{for} \quad 1 \le \mu \le m,\ 1 \le \nu \le n. \quad \square$$

Lad $k \subseteq K$, $\alpha \in K$, og betragt

$$I = \{f \in k[x] \mid f(\alpha) = 0\}.$$

Det er klart, at I er et ægte ideal i $k[x]$, og da $k[x]$ er en hovedidealring (PID), er I et ægte hovedideal.

Såfremt $I = (0)$, dvs. α ikke er algebraisk over k, kaldes α *transcendent* over k.

Hvis $I \neq (0)$, dvs. α er algebraisk over k, kan I på netop en måde skrives på formen $I = (p)$, hvor p er et normeret polynomium. Dette polynomium kaldes *minimalpolynomiet* for α, og dets grad, som betegnes ∂p, kaldes også *graden* af α. Bemærk, at α's minimalpolynomium og grad afhænger af grundlegemet

k. Det er klart, at minimalpolynomiet p for α er irreducibelt i $k[x]$, thi ellers fandtes et egentligt polynomium $f \in (p)$ med $\partial f < \partial p$, og dette er umuligt.

Lad $k \subseteq K$, $\alpha \in K$, og lad $k[\alpha]$ og $k(\alpha)$, hvor

$$k \subseteq k[\alpha] \subseteq k(\alpha) \subseteq K,$$

være henholdvis den mindste ring og det mindste legeme, der indeholder α. Da gælder følgende

Sætning 3. *Lad $k \subseteq K, \alpha \in K$, og antag at α er algebraisk af grad $n \in \mathbb{N}$. Da er*

$$k[\alpha] = k(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_\nu \in k\}.$$

Sættet $(1, \alpha, \ldots, \alpha^{n-1})$ er en basis for $k(\alpha)/k$, specielt er $[k(\alpha) : k] = n$.

Bevis. Det er klart, at

$$k[\alpha] = \{f(\alpha) \mid f \in k[x]\}.$$

Lad minimalpolynomiet for α være p. Af den principale divisionsligning

$$f = pq + r, \quad \text{hvor} \quad q, r \in k[x],\ \partial r < n = \partial p,$$

følger da ved indsættelse af α, at $f(\alpha) = r(\alpha)$. Dette viser imidlertid, at

$$k[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_\nu \in k\}.$$

Vi påstår nu, at idealet $(p) \subset k[x]$ er et maksimalt ideal i $k[x]$. Thi ellers fandtes et ideal J med $(p) \subset J \subset k[x]$. Da $k[x]$ er PID, er $J = (q)$, hvor q er et normeret polynomium. Da $q \mid p$ og p er irreducibelt, er enten $q = 1$ eller $q = p$ i strid med $(p) \subset (q) \subset k[x]$. Følgelig er $k[x]/(p)$ et legeme.

Betragtes den naturlige homomorfi $\varphi : k[x] \to k[\alpha]$ defineret ved $\varphi(f) = f(\alpha)$, fås af homomorfisætningen tillige:

$$k[x]/(p) \simeq \varphi(k[x]) = k[\alpha].$$

Hermed er vist, at $k[\alpha]$ er et legeme, og da $k(\alpha)$ er det mindste dellegeme af K, som indeholder $k[\alpha]$, er $k(\alpha) = k[\alpha]$.

At sættet $(1, \alpha, \ldots, \alpha^{n-1})$ er en basis for $k(\alpha)/k$, følger af, at sættet frembringer $k(\alpha)$ over k og $[k(\alpha) : k] = \partial p = n$. □

Eksempel 1. For $n > 1$ er $\sqrt[n]{2} \in \mathbb{R} \supset \mathbb{Q}$ og $\sqrt[n]{2}$ er algebraisk af grad n, idet minimalpolynomiet for $\sqrt[n]{2}$ er $x^n - 2$. At dette polynomium er irreducibelt i $\mathbb{Q}[x]$ følger af Eisensteins irreducibilitetskriterium anvendt på primtallet 2 samt af Gauss' lemma.

Som bekendt siger Eisensteins kriterium, at et polynomium

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

er irreducibelt i $\mathbb{Z}[x]$, såfremt der findes et primtal p så

$$p \,|\, a_\nu \quad \text{for} \quad 0 \leq \nu \leq n-1 \quad \text{men} \quad p^2 \nmid a_0.$$

Gauss' lemma siger, at et normeret polynomium i $\mathbb{Z}[x]$ er irreducibelt i $\mathbb{Q}[x]$, hvis og kun hvis det er irreducibelt i $\mathbb{Z}[x]$.

Vi har derfor

$$\mathbb{Q}(\sqrt[n]{2}) = \{a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1}(\sqrt[n]{2})^{n-1} \mid a_\nu \in \mathbb{Q}\}.$$

Eksempel 2. Antag at $D \in \mathbb{Z}$, men at D ikke er et kvadrattal. Lad $\sqrt{D}$ betegne den positive kvadratrod, hvis $D > 0$, og kvadratroden med positiv imaginærværdi, hvis $D < 0$. Da er $\sqrt{D} \in \mathbb{C} \supset \mathbb{Q}$ algebraisk af grad 2, idet minimalpolynomiet er $x^2 - D$. At dette polynomium er irreducibelt i $\mathbb{Q}[x]$ følger af Gauss' lemma. Legemet $\mathbb{Q}(\sqrt{D})$ kaldes et *kvadratisk* tallegeme og mere præcist et *reelt kvadratisk* tallegeme, hvis $D > 0$, og et *imaginært kvadratisk* tallegeme, hvis $D < 0$. I begge tilfælde er

$$\mathbb{Q}(\sqrt{D}) = \{a_0 + a_1\sqrt{D} \mid a_0, a_1 \in \mathbb{Q}\}.$$

Eksempel 3. Den imaginære enhed $i = \sqrt{-1} \in \mathbb{C} \supset \mathbb{R}$ er algebraisk af grad 2 over $\mathbb{R}$ med minimalpolynomiet $x^2 + 1$. I overensstemmelse hermed er

$$\mathbb{C} = \mathbb{R}(i) = \{a_0 + a_1 i \mid a_0, a_1 \in \mathbb{R}\}.$$

Eksempel 4. For $n \in \mathbb{N}$ er $\zeta = e^{2\pi i/n} \in \mathbb{C} \supset \mathbb{Q}$, idet ζ er nulpunkt i polynomiet $x^n - 1$. Det kan vises (ikke trivielt), at ζ's minimalpolynomium Φ_n er givet ved

$$\Phi_n(x) = \prod_{1 \leq m \leq n, \gcd(m,n)=1} (x - \zeta^m),$$

og at $\Phi_n \in \mathbb{Z}[x]$. Graden af ζ er derfor givet ved Eulers funktion $\varphi(n)$, hvor $\varphi(n)$ er antallet af primiske restklasser modulo n.

Legemet

$$\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + \cdots + a_{\varphi(n)-1}\zeta^{\varphi(n)-1} \mid a_\nu \in \mathbb{Q}\}$$

kaldes det n'te *cirkeldelingslegeme* (eng: *cyclotomic field*), og Φ_n kaldes det n'te *cirkeldelingspolynomium*.

Fx er

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1,$$
$$\Phi_4(x) = x^2 + 1, \Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \Phi_6(x) = x^2 - x + 1.$$

Eksempel 5. Betragt $k = \mathbb{F}_2(x^2, y^2) \subset \mathbb{F}_2(x, y) = K$, hvor $\mathbb{F}_2$ er legemet med 2 elementer, og x, y er kommuterende variable. Elementerne $x, y \in K$ er begge algebraiske af grad 2 over k, da $x^2, y^2 \in k$. Derfor er udvidelsen $k \subset K$ af grad 4, og $(1, x, y, xy)$ er en basis for K/k. Et vilkårligt element $\alpha \in K$ har formen

$$\alpha = a_0 + a_1x + a_2y + a_3xy, \quad \text{hvor} \quad a_\nu \in k.$$

Da karakteristikken er 2, fås heraf at

$$\alpha^2 = a_0^2 + a_1^2x^2 + a_2^2y^2 + a_3^2x^2y^2 \in k.$$

Heraf følger, at ethvert element $\alpha \in K \setminus k$ har grad 2 over k. Der findes derfor intet $\alpha \in K$ med egenskaben $K = k(\alpha)$. På den anden side er det klart, at $K = k(x, y)$ fremgår af k ved adjunktion af de to elementer x, y.

Sætning 4. *Lad $k \subseteq K$. Mængden af elementer i K, som er algebraiske over k, udgør et legeme.*

Bevis. Vi skal vise: Såfremt $\alpha, \beta \in K$ er algebraiske over k, er også $\alpha + \beta, \alpha - \beta, \alpha\beta$ og (for $\beta \neq 0$) α/β algebraiske over k. Dette følger imidlertid af, at $k(\alpha, \beta) = k(\alpha)(\beta)$ ifølge sætningerne 2 og 3 er en endelig udvidelse af k og derfor ifølge sætning 1 en algebraisk udvidelse af k. □

Sætning 5. *(Kæderegel for algebraiske udvidelser). Lad $k \subseteq K \subseteq L$ og antag, at K er algebraisk over k og L algebraisk over K. Da er L algebraisk over k.*

Bevis. Lad $\alpha \in L$ være et vilkårligt element, og lad

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

være α's minimalpolynomium over K. Legemet

$$k(a_0, a_1, \ldots, a_{n-1}, \alpha) = k(a_0, a_1, \ldots, a_{n-1})(\alpha)$$

er ifølge sætningerne 1 og 2 en endelig og derfor ifølge sætning 3 algebraisk udvidelse af k. Da α tilhører dette legeme, er α algebraisk over k. □

Et legeme k kaldes *algebraisk afsluttet*, hvis der ikke findes noget legeme K med $k \subset K$, så at K er algebraisk over k. Det kan vises, at ethvert legeme k har en snævreste udvidelse til et algebraisk afsluttet legeme, og en sådan udvidelse er entydig bestemt pånær en *k-isomorfi*, dvs. en isomorfi, hvor hvert element i k afbildes i sig selv. Et sådant legeme kaldes en *algebraisk afslutning* af k og betegnes $\overline{k}$.

Fx har $\mathbb{Q}$ en algebraisk afslutning $\overline{\mathbb{Q}} \subset \mathbb{C}$, nemlig

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisk over } \mathbb{Q}\}.$$

Dette følger umiddelbart ved brug af sætningerne 4 og 5 samt algebraens fundamentalsætning: $\overline{\mathbb{C}} = \mathbb{C}$. Legemet $\overline{\mathbb{Q}}$ kaldes *legemet af algebraiske tal*. Det følger af eksempel 1, at $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Legemet $\overline{\mathbb{Q}}$, som er foreningsmængden af alle algebraiske tallegemer, er derfor ikke selv noget algebraisk tallegeme.

Norm og spor. Lad $k \subseteq K$ være en endelig udvidelse med $[K : k] = n$, og lad $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ være en basis for K/k. For hvert $\alpha \in K$ betragtes den lineære afbildning $\varphi_\alpha : K \to K$ givet ved $\varphi_\alpha(\vartheta) = \alpha\vartheta$. Udtrykt ved basen ω er denne afbildning givet ved

$$\begin{pmatrix} \alpha\omega_1 \\ \vdots \\ \alpha\omega_n \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix},$$

hvor $a_{rs} \in k$ for $1 \leq r, s \leq n$.

Det er velkendt fra den lineære algebra, at det karakteristiske polynomium for φ_α:

$$p_A(x) = \det(A - xE) \in k[x]$$

er uafhængigt af den valgte basis, dvs kun afhænger af α. Specielt afhænger

$$\operatorname{tr} A = \sum_1^n a_{rr} \quad \text{og} \quad \det A$$

alene af α, hvorfor vi kan skrive

$$\operatorname{tr} \varphi_\alpha = \operatorname{tr} A, \quad \det \varphi_\alpha = \det A.$$

Vi definerer nu afbildninger $S : K \to k, \quad N : K \to k$ ved

$$S(\alpha) = S_{K/k}(\alpha) = \operatorname{tr} \varphi_\alpha, \quad N(\alpha) = N_{K/k}(\alpha) = \det \varphi_\alpha.$$

$S(\alpha)$ og $N(\alpha)$ kaldes henholdsvis *sporet* og *normen* af α ved udvidelsen $k \subseteq K$.

Sætning 6. *Lad $k \subseteq K$ med $[K : k] = n \in \mathbb{N}$. For vilkårlige $\alpha, \beta \in K, a \in k$, gælder da*

$$\begin{aligned} S(\alpha + \beta) &= S(\alpha) + S(\beta), \\ N(\alpha\beta) &= N(\alpha)N(\beta), \\ S(a\alpha) &= aS(\alpha), \\ S(a) &= na, \\ N(a) &= a^n. \end{aligned}$$

Bevis. Ved brug af velkendte regneregler for tr og det fås:

$$\begin{aligned} S(\alpha + \beta) &= \operatorname{tr} \varphi_{\alpha+\beta} = \operatorname{tr} (\varphi_\alpha + \varphi_\beta) = \operatorname{tr} \varphi_\alpha + \operatorname{tr} \varphi_\beta = S(\alpha) + S(\beta), \\ N(\alpha\beta) &= \det \varphi_{\alpha\beta} = \det(\varphi_\alpha \varphi_\beta) = \det \varphi_\alpha \det \varphi_\beta = N(\alpha)N(\beta), \\ S(a\alpha) &= \operatorname{tr} \varphi_{a\alpha} = a \operatorname{tr} \varphi_\alpha = aS(\alpha). \end{aligned}$$

De to sidste regler følger af, at afbildningen φ_a har afbildningsmatricen $A = aE$ for enhver basis ω for K/k. □

Eksempel 6. For $\mathbb{R} \subset \mathbb{C}$ (jf eksempel 3) med basis $(1, i)$ og $\alpha = a_0 + a_1 i$ bliver afbildningsmatricen A for afbildningen φ_α:

$$A = \begin{pmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{pmatrix},$$

hvorfor

$$S(\alpha) = \operatorname{tr} A = 2a_0, \quad N(\alpha) = \det A = a_0^2 + a_1^2.$$

For $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D})$ (jf eksempel 2) med basis $(1, \sqrt{D})$ og $\alpha = a_0 + a_1\sqrt{D}$ bliver afbildningsmatricen A for afbildningen φ_α:

$$A = \begin{pmatrix} a_0 & a_1 \\ Da_1 & a_0 \end{pmatrix},$$

hvorfor

$$S(\alpha) = \operatorname{tr} A = 2a_0, \quad N(\alpha) = \det A = a_0^2 - Da_1^2.$$

For $k = \mathbb{F}_2(x^2, y^2) \subset \mathbb{F}_2(x, y) = K$ (jf eksempel 5) med basis $(1, x, y, xy)$ og $\alpha = a_0 + a_1 x + a_2 y + a_3 xy$ bliver afbildningsmatricen A for φ_α:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1x^2 & a_0 & a_3x^2 & a_2 \\ a_2y^2 & a_3y^2 & a_0 & a_1 \\ a_3x^2y^2 & a_2y^2 & a_1x^2 & a_0 \end{pmatrix}.$$

Da karakteristikken er 2, fås

$$\begin{aligned} S(\alpha) &= \operatorname{tr} A = 4a_0 = 0, \\ N(\alpha) &= \det A = (a_0^2 + (a_1x)^2 + (a_2y)^2 + (a_3xy)^2)^2 = \alpha^4. \end{aligned}$$

I den følgende sætning studeres sammenhængen mellem minimalpolynomium og karakteristisk polynomium.

Sætning 7. *Lad $k \subseteq K$ med $[K : k] = n \in \mathbb{N}$, og $\alpha \in K$. Lad f være minimalpolynomiet for α:*

$$f(x) = x^l + a_{l-1}x^{l-1} + \cdots + a_1 x + a_0.$$

Lad $\varphi_\alpha : K \to K$ være afbildningen givet ved $\varphi_\alpha(\vartheta) = \alpha\vartheta$ med karakteristisk polynomium F. Der gælder da:

$$F = (-1)^n f^m, \quad \textit{hvor} \quad m = n/l.$$

For udvidelsen K/k gælder

$$S_{K/k}(\alpha) = mS_{k(\alpha)/k}(\alpha), \quad N_{K/k}(\alpha) = (N_{k(\alpha)/k}(\alpha))^m.$$

For udvidelsen $k(\alpha)/k$ gælder

$$S_{k(\alpha)/k}(\alpha) = -a_{l-1}, \quad N_{k(\alpha)/k} = (-1)^l a_0.$$

Betegner $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(l)}$ samtlige nulpunkter i f (i en passende udvidelse af k, fx $\overline{k}$ – disse kaldes α's konjugerede) kan sidstnævnte formler også skrives

$$S_{k(\alpha)/k}(\alpha) = \sum_{j=1}^{l} \alpha^{(j)}, \quad N_{k(\alpha)/k} = \prod_{j=1}^{l} \alpha^{(j)}.$$

Bevis. Ifølge sætning 3 er $(1, \alpha, \ldots, \alpha^{l-1})$ en basis for $k(\alpha)/k$. Endvidere vælges en vilkårlig basis $(\vartheta_1, \ldots, \vartheta_m)$ for $K/k(\alpha)$. Ifølge sætning 2 er da $n = lm$, og

$$(\vartheta_1, \alpha\vartheta_1, \ldots, \alpha^{l-1}\vartheta_1, \ldots, \vartheta_m, \alpha\vartheta_m, \ldots, \alpha^{l-1}\vartheta_m)$$

er en basis for K/k. Mht. denne basis bliver afbildningsmatricen A for φ_α:

$$A = M \oplus \cdots \oplus M, \quad \text{(m addender)},$$

hvor

$$M = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{l-1} \end{pmatrix},$$

og hvor skrivemåden angiver, at A er en blokmatrix med m blokke langs diagonalen, hver lig M, og med 0'er iøvrigt.

Dette følger umiddelbart, idet det benyttes, at

$$\alpha^l = -a_0 - a_1\alpha - \cdots - a_{l-1}\alpha^{l-1}.$$

Bemærk også, at restriktionen af φ_α til $k(\alpha)$ netop har afbildningsmatricen M mht. basen $(1, \alpha, \ldots, \alpha^{l-1})$.

Af blokstrukturen fremgår nu, at

$$F(x) = \det(A - xE) = (\det(M - xE))^m,$$

hvor E er enhedsmatricen af den relevante størrelse. Da α er en egenværdi for den lineære afbildning $\varphi_\alpha : K \to K$, er α også rod i $F(x)$, dvs. α er rod i $\det(M - xE)$. Da dette polynomium har grad l, og højestegradkoefficienten er $(-1)^l$, må der følgelig gælde

$$\det(M - xE) = (-1)^l f(x),$$

og dette viser den første formel i sætningen.

Det fremgår også af blokstrukturen, at

$$\operatorname{tr} A = m \operatorname{tr} M, \quad \det A = (\det M)^m,$$

og dette viser de følgende to formler i sætningen. De næste to formler følger af, at der gælder

$$\operatorname{tr} M = -a_{l-1}, \quad \det M = (-1)^l a_0.$$

Da

$$(-1)^l f(x) = \prod_{j=1}^{l} (\alpha^{(j)} - x),$$

fremkommer de sidste to formler af de tidligere ved at sammenholde konstantled og led af grad $l - 1$. □

Diskriminant. Lad $k \subseteq K$ være en endelig udvidelse med $[K : k] = n \in \mathbb{N}$, og lad $\omega = (\omega_1, \omega_2, \dots, \omega_n)$ være en basis for K/k. Ved *diskriminanten* for ω forstås

$$D(\omega) = \det(S(\omega_r \omega_s))_{r,s=1,\dots,n}.$$

Lad

$$\underline{\omega} = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Når $\omega' = (\omega'_1, \dots, \omega'_n)$ er en anden basis for K/k givet ved $\underline{\omega}' = C\underline{\omega}$, hvor C er en $n \times n$-matrix over k med $\det C \neq 0$. Da er

$$(\omega'_r \omega'_s) = \underline{\omega}' \underline{\omega}'^t = C \underline{\omega} \underline{\omega}^t C^t = C(\omega_r \omega_s) C^t.$$

På grund af lineariteten af sporet er derfor

$$(S(\omega'_r\omega'_s)) = C(S(\omega_r\omega_s))C^t,$$

hvorfor

$$D(\omega') = (\det C)^2 D(\omega).$$

Da $\det C \neq 0$, er diskriminanten følgelig enten lig 0 for enhver basis for K/k eller forskellig fra 0 for enhver basis for K/k.

Sætning 8. *Lad $k \subseteq K$ med $[K : k] = n \in \mathbb{N}$. Da er diskriminanten $\neq 0$ for enhver basis for K/k, hvis og kun hvis afbildningen $S : K \to k$ ikke er nulafbildningen.*

Bevis. Hvis S er nulafbildningen, er det klart, at diskriminanten er 0 for enhver basis for K/k.

Antag omvendt, at der findes en basis ω, for hvilken diskriminanten er 0. Da er søjlerne i matricen $(S(\omega_r\omega_s))$ lineært afhængige over k, dvs. der findes $c_1, \ldots, c_n \in k$, som ikke alle er 0, så at

$$(*) \qquad \sum_{s=1}^{n} S(\omega_r\omega_s)c_s = 0 \quad \text{for} \quad r = 1, \ldots, n.$$

Sættes $\gamma = c_1\omega_1 + \cdots + c_n\omega_n$, kan (*) skrives

$$(**) \qquad S(\omega_r\gamma) = 0 \quad \text{for} \quad r = 1, \ldots, n.$$

Da $\gamma \neq 0$, er $(\omega_1\gamma, \ldots, \omega_n\gamma)$ en basis for K/k. Da $S_{K/k}$ er 0 på en basis for K/k, vil $S_{K/k}$ på grund af linearitet være nulafbildningen. □

Eksempel 7. For udvidelsen $\mathbb{R} \subset \mathbb{C}$ (jf eksempler 3 og 6) og basis $\omega = (1, i)$ er

$$D(\omega) = \det \begin{pmatrix} S(1) & S(i) \\ S(i) & S(-1) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = -4.$$

For udvidelsen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D})$ (jf eksempler 2 og 6) og basis $\omega = (1, \sqrt{D})$ er

$$D(\omega) = \det \begin{pmatrix} S(1) & S(\sqrt{D}) \\ S(\sqrt{D}) & S(D) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$

For udvidelsen $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ (jf eksempel 4) og basis $\omega = (1, \zeta, \zeta^2, \zeta^3)$ er

$$D(\omega) = \det \begin{pmatrix} S(1) & S(\zeta) & S(\zeta^2) & S(\zeta^3) \\ S(\zeta) & S(\zeta^2) & S(\zeta^3) & S(\zeta^4) \\ S(\zeta^2) & S(\zeta^3) & S(\zeta^4) & S(\zeta^5) \\ S(\zeta^3) & S(\zeta^4) & S(\zeta^5) & S(\zeta^6) \end{pmatrix}.$$

Da minimalpolynomiet for ζ (og dermed for $\zeta^2, \zeta^3, \zeta^4, \zeta^6 = \zeta$) er cirkeldelingspolynomiet

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

haves ifølge sætning 7

$$S(\zeta^r) = \begin{cases} -1 & \text{for} \quad r = 1, 2, 3, 4, 6 \\ 4 & \text{for} \quad r = 0, 5 \end{cases}.$$

Efter passende søjleoperationer fås derfor

$$D(\omega) = \det \begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 4 \\ -1 & -1 & 4 & -1 \end{pmatrix} = \det \begin{pmatrix} 5 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 5 \\ 0 & -1 & 5 & 0 \end{pmatrix} = 5^3.$$

For $k = \mathbb{F}_2(x^2, y^2) \subset \mathbb{F}_2(x, y) = K$ (jf eksempler 5 og 6) er diskriminanten 0 for enhver basis for K/k ifølge sætning 8, da $S : K \to k$ er nulafbildningen.

Sætning 9. *Lad $K = k(\vartheta)$, hvor ϑ er algebraisk over k af grad $n \in \mathbb{N}$. Da kan diskriminanten for basen $\omega = (1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1})$ skrives på formen*

$$D(\omega) = (\det M)^2,$$

hvor M er Vandermonde matricen

$$M = \begin{pmatrix} 1 & \vartheta^{(1)} & {\vartheta^{(1)}}^2 & \ldots & {\vartheta^{(1)}}^{n-1} \\ 1 & \vartheta^{(2)} & {\vartheta^{(2)}}^2 & \ldots & {\vartheta^{(2)}}^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \vartheta^{(n)} & {\vartheta^{(n)}}^2 & \ldots & {\vartheta^{(n)}}^{n-1} \end{pmatrix},$$

og $(\vartheta^{(1)}, \vartheta^{(2)}, \ldots, \vartheta^{(n)})$ er de konjugerede til ϑ, dvs. rødderne i minimalpolynomiet for ϑ over k.

Følgelig gælder formlen

$$D(\omega) = \prod_{1 \le i < j \le n} (\vartheta^{(j)} - \vartheta^{(i)})^2.$$

Bevis. Ved brug af sætning 7 fås umiddelbart

$$(S(\vartheta^{r+s-2}))_{r,s=1,\dots,n} = M^t M,$$

hvoraf den første formel fås ved at tage determinanten.

Den anden formel følger da af et velkendt udtryk for Vandermonde determinanten. □

Galoisteori. I dette afsnit vil vi kort omtale nogle begreber, der spiller en rolle i algebraisk talteori. Hvad angår beviser henvises til bøger om emnet fx E. Artin: *Galoische Theorie*.

Lad $f \in k[x]$ være et polynomium af grad n. Et legeme K med $k \subseteq K$ kaldes et *spaltningslegeme* for f over k, såfremt

(i) $$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n),$$

(ii) $$K = k(\alpha_1, \dots, \alpha_n).$$

En udvidelse $k \subseteq K$ kaldes *normal*, hvis ethvert irreducibelt polynomium $f \in k[x]$ med et nulpunkt i K kan skrives som produkt af polynomier af første grad med koefficienter fra K.

Vi anfører uden bevis:

Sætning 10. *Såfremt K og K' begge er spaltningslegemer for samme polynomium $f \in k[x]$, da findes en k-isomorfi mellem K og K'.*

Sætning 11. *En endelig udvidelse $k \subseteq K$ er normal, hvis og kun hvis K er spaltningslegeme for et polynomium $f \in k[x]$.*

Eksempel 8. Alle udvidelser i eksemplerne 2-5 er normale. I eksempel 5 er således $K = \mathbb{F}_2(x, y)$ spaltningslegeme for polynomiet f givet ved $f(t) =$

$(t^2 - x^2)(t^2 - y^2)$ over $k = \mathbb{F}_2(x^2, y^2)$. Derimod er udvidelsen $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2})$ (jf eksempel 1) ikke normal for $n \geq 3$. Et spaltningslegeme for $f(x) = x^n - 2$ over $\mathbb{Q}$ (og det eneste inden for $\mathbb{C}$) er $K = \mathbb{Q}(\sqrt[n]{2}, \zeta)$, hvor $\zeta = e^{2\pi i/n}$. Opspaltningen af f i førstegradspolynomier over K er da

$$f(x) = x^n - 2 = \prod_{\nu=0}^{n-1} (x - \sqrt[n]{2}\zeta^\nu).$$

Sætning 12. *Lad $f \in k[x]$ være et polynomium over k af grad > 0, og lad K være et spaltningslegeme for f over k. Da har f lutter simple rødder i K, hvis og kun hvis $gcd(f, f') = 1$, hvor f' er den formelle afledede af f.*

Korollar. *Hvis k har karakteristik 0, har ethvert irreducibelt polynomium over k af grad > 0 lutter simple rødder.*

Et irreducibelt polynomium $f \in k[x]$ kaldes *separabelt*, hvis f i et spaltningslegeme K har lutter simple rødder. En algebraisk udvidelse $k \subseteq K$ kaldes *separabel*, hvis minimalpolynomiet for ethvert $\alpha \in K$ er separabelt over k.

Eksempel 9. Lad $k = \mathbb{F}_2(x^2, y^2)$ (jf eksemplerne 5 og 8). Polynomiet $f(t) = t^2 - x^2$ er irreducibelt over k, men er ikke separabelt. Et spaltningslegeme for f over k er $K = F_2(x, y^2)$, hvori $f(t) = (t + x)(t - x) = (t - x)^2$. Bemærk også, at $f'(t) = 2t$, således at f' er nulpolynomiet, da karakteristikken er 2.

En endelig udvidelse $k \subseteq K$ kaldes *galois*, hvis den er normal og separabel. (I karakteristik 0 er galois altså identisk med normal).

Lad $k \subseteq K$ af grad $[K : k] = n \in \mathbb{N}$. En afbildning $\sigma : K \to K$, som er en isomorfi (mht. $+$ og $\cdot$), og for hvilken $\sigma(a) = a$ for ethvert $a \in k$ kaldes en *k-automorfi*. Mængden af k-automorfier udgør med sammensætning som komposition en gruppe kaldet *Galoisgruppen* for K/k. Den betegnes $\mathrm{Gal}(K/k)$.

Eksempel 10. $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ (jf eksempel 3) er den cykliske gruppe af orden 2 bestående af de to elementer $\{id, \kappa\}$, hvor id er den identiske afbildning af $\mathbb{C}$ og κ er den komplekse konjugering af $\mathbb{C}$.

På tilsvarende måde er $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ den cyklisk gruppe af orden 2 bestående af de to elementer $\{id, \kappa\}$, hvor id er den identiske afbildning af $\mathbb{Q}(\sqrt{D})$ og κ er konjugeringen defineret ved $\kappa : a_0 + a_1\sqrt{D} \mapsto a_0 - a_1\sqrt{D}$.

Derimod er $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ den cykliske gruppe af orden 1, der kun består af identiske afbildning af $\mathbb{Q}(\sqrt[3]{2})$. Begrundelsen herfor er, at enhver $\mathbb{Q}$-automorfi af $\mathbb{Q}(\sqrt[3]{2})$ må afbilde $\sqrt[3]{2}$ på et nulpunkt for x^3-2, dvs. på sig selv, da legemet er reelt, og de øvrige rødder i dette polynomium ikke er reelle.

Endelig er $\mathrm{Gal}(\mathbb{F}_2(x,y)/\mathbb{F}_2(x^2,y^2)) = \{id\}$. Ved enhver $\mathbb{F}_2(x^2,y^2)$-automorfi af $\mathbb{F}_2(x,y)$ må x afbildes i et nulpunkt for $t^2 - x^2$, dvs. på x, da $-x = x$. Tilsvarende må y afbildes på y. Da $\mathbb{F}_2(x,y) = \mathbb{F}_2(x^2,y^2)(x,y)$ følger påstanden.

Sætning 13. *For enhver endelig udvidelse $k \subseteq K$ gælder uligheden*

$$|Gal(K/k)| \leq [K:k].$$

Sætning 14 (Galoisteoriens hovedsætning). *For en galois udvidelse $k \subseteq K$ gælder*

$$|Gal(K/k)| = [K:k].$$

Der er en bijektiv korrespondance mellem undergrupper $G' \subseteq G = Gal(K/k)$ og legemer K', som opfylder $k \subseteq K' \subseteq K$ svarende til følgende diagram:

$$\begin{array}{ccc} K & \longleftrightarrow & E \\ \cup & & \cap \\ K' & \longleftrightarrow & G' \\ \cup & & \cap \\ k & \longleftrightarrow & G \end{array}$$

Her betegner E gruppen, der kun består af etelementet. Korrespondancen er defineret ved, at K' er fixpunktlegemet for undergruppen G':

$$K' = \{x \in K \mid \sigma(x) = x \quad \textit{for ethvert} \quad \sigma \in G'\},$$

eller ækvivalent hermed ved, at

$$G' = \{\sigma \in G \mid \sigma(x) = x \quad \textit{for ethvert} \quad x \in K'\}.$$

Ved korrespondancen gælder (idet [G:G'] betegner undergruppeindexet):

$$[K' : k] = [G : G'].$$

Yderligere gælder, at konjugerede undergrupper korresponderer med konjugerede legemer:

$$G' \longleftrightarrow K' \Longleftrightarrow \sigma G' \sigma^{-1} \longleftrightarrow \sigma(K') \quad for \quad \sigma \in G.$$

Specielt er K' en normal udvidelse af k, hvis og kun hvis G' er en normal undergruppe af G. I dette specielle tilfælde er

$$Gal(K'/k) \simeq G/G'.$$

Sætning 15 (Abels sætning om primitivt element). *For enhver endelig og separabel udvidelse $k \subseteq K$ gælder, at der findes et $\vartheta \in K$, så at $K = k(\vartheta)$.*

Bevis. 1. $|k| = \infty$. Da $[K : k] < \infty$, findes $\alpha_1, \ldots, \alpha_r \in K$, så at $K = k(\alpha_1, \ldots, \alpha_r)$. Lad $f_\rho \in k[x]$ være minimalpolynomiet for α_ρ mht. k, og lad $f = f_1 \cdots f_r$. Lad K^* være et spaltningslegeme for f mht. k. Da er K^* en endelig, separabel og normal udvidelse af k, dvs. $k \subseteq K^*$ er galois. Det kan (pånær isomorfi) antages, at $K \subseteq K^*$, og K^* kaldes da *det normale hylster* for K mht. k. Ifølge Galoisteoriens hovedsætning er der kun endeligt mange legemer K', så at $k \subseteq K' \subseteq K^*$, idet disse legemer er i bijektiv korrespondance med de endeligt mange undergrupper i $\mathrm{Gal}(K^*/k)$. Derfor er der også kun endeligt mange legemer K', så at $k \subseteq K' \subseteq K$. Beviset føres nu ved induktion efter antallet r af frembringere for K/k, og det er derfor nok at vise resultatet for $r = 2$. Betragt dertil de uendeligt mange legemer

$$\{k_a = k(\alpha_1 + a\alpha_2) \mid a \in k\},$$

som alle opfylder $k \subseteq k_a \subseteq K$. Da der kun er endeligt mange legemer mellem k og K, må der findes $a, b \in k,\ a \neq b$, så at

$$k_a = k_b = K' \subseteq k(\alpha_1, \alpha_2) = K.$$

På den anden side følger det af $\alpha_1 + a\alpha_2,\ \alpha_1 + b\alpha_2 \in K'$, at $(a - b)\alpha_2 \in K'$ og dermed $\alpha_2 \in K'$, hvorfor også $\alpha_1 \in K'$. Derfor gælder også $K \subseteq K'$, altså $K = K'$. Dette viser det ønskede.

2. $|k| < \infty$. Da fungerer ovenstående bevis ikke, men sætningen følger i dette tilfælde umiddelbart af det velkendte resultat, at den multiplikative gruppe $K^\times$ for et endeligt legeme K er cyklisk (jf. eksempel 13). □

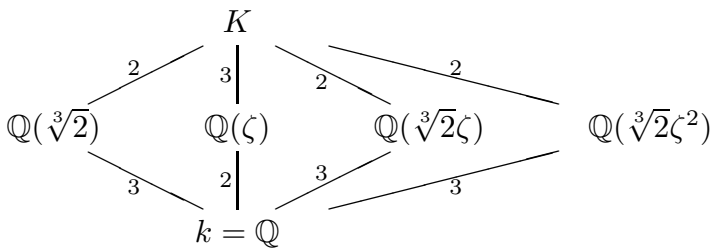
Vi illustrerer endvidere Galoisteoriens hovedsætning ved følgende tre eksempler:

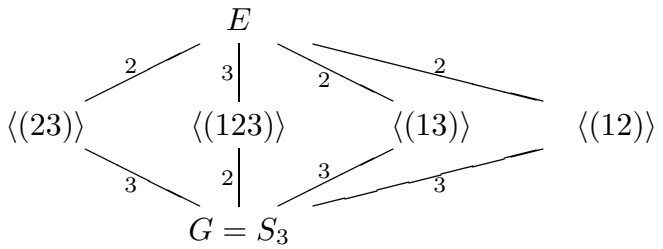
Eksempel 11. $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ er galois over $k = \mathbb{Q}$, idet K er spaltningslegeme for polynomiet $f(x) = x^3 - 2$. Det fremgår, at

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})][K : \mathbb{Q}(\sqrt[3]{2})] = 3 \cdot 2 = 6.$$

Sæt $\zeta = e^{2\pi i/3}$. Da er rødderne i f : $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\zeta$, $\alpha_3 = \sqrt[3]{2}\zeta^2$. En automorfi i $G = \mathrm{Gal}(K/k)$ er givet ved den permutation af $(\alpha_1, \alpha_2, \alpha_3)$ den bevirker. Da $|G| = [K : k] = 6$, er derfor $G \simeq S_3 =$ permutationsgruppen for $(1, 2, 3)$.

De korresponderende diagrammer af legemer mellem k og K og undergrupper i G (med relative grader og indices anført) er angivet nedenfor:





Her betegner fx $\langle(123)\rangle$ gruppen frembragt af elementet (123), som er den cykliske permutation: $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. I øvrigt er $\langle(123)\rangle$ den alternerende gruppe A_3, som er en normal undergruppe i $G = S_3$.

Eksempel 12. For $n \in \mathbb{N}$ er $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/n}$, galois over $k = \mathbb{Q}$. Dette følger af, at K er spaltningslegeme for ζ's minimalpolynomium Φ_n over $\mathbb{Q}$, hvor (jf eksempel 4)

$$\Phi_n(x) = \prod_{1 \le m \le n,\, \gcd(m,n)=1} (x - \zeta^m).$$

Derfor er

$$|G| = |\mathrm{Gal}(K/k)| = [K : k] = \varphi(n).$$

Det er klart, at

$$\mathrm{Gal}(K/k) = \{\sigma_\nu : \zeta \mapsto \zeta^\nu \mid \gcd(\nu, n) = 1,\ 1 \leq \nu \leq n\}.$$

Da $\sigma_\mu \circ \sigma_\nu = \sigma_{\mu\nu}$ er

$$\mathrm{Gal}(K/k) \simeq (\mathbb{Z}/(n\mathbb{Z}))^\times,$$

altså den primiske restklassegruppe modulo n.

For $n = p$, hvor p er et ulige primtal, er denne gruppe cyklisk af orden $\varphi(p) = p - 1$. I dette tilfælde er der præcis én (cyklisk) undergruppe C_m for hver divisor $m \,|\, (p-1)$. Da specielt $2 \,|\, (p-1)$, findes netop én cyklisk undergruppe C_2 i $\mathrm{Gal}(K/k)$, og $C_2 = \{\sigma_1 = id, \sigma_{p-1} = \text{komplex konjugering}\}$. Det dertil svarende fixpunktlegeme er legemet $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(2\cos(2\pi)/p)$. Det kaldes det *maksimale reelle dellegeme* i $K = \mathbb{Q}(\zeta)$.

Er specielt $p = 2^{2^m} + 1$ et Fermat-primtal, er $\mathrm{Gal}(K/k) \simeq C_{2^{2^m}}$, hvorfor der findes en kæde af undergrupper $C_{2^l}, 0 \leq l \leq 2^m$. Den dertil svarende kæde af dellegemer i K viser, at K fremkommer af $\mathbb{Q}$ ved successive kvadratiske udvidelser. Dette blev opdaget af Gauss (før Galoisteorien), som derved kunne vise, at den regulære p-kant er konstruerbar med passer og lineal for Fermat-primtal. Af disse kendes fortsat kun: 3, 5, 17, 257, 65537.

Eksempel 13. (Endelige legemer). Ethvert endeligt legeme K må have primtalskarakteristik p, dvs. $K \supseteq \mathbb{F}_p$. Lad $[K : \mathbb{F}_p] = n$, og lad $(\omega_1, \ldots, \omega_n)$ være en basis for K over $\mathbb{F}_p$. Da kan elementerne i K fremstilles entydigt på formen $a_1\omega_1 + \cdots + a_n\omega_n$, hvor $a_1, \ldots, a_n \in \mathbb{F}_p$. Følgelig er elementantallet $|K| = p^n$. Den multiplikative gruppe $K^\times = K \setminus \{0\}$ har orden $p^n - 1$, og ifølge Lagrange's sætning gælder derfor

$$\alpha^{p^n - 1} = 1 \quad \text{for ethvert} \quad \alpha \in K^\times.$$

Dette viser, at K er spaltningslegeme for polynomiet f over $\mathbb{F}_p$, hvor

$$f(x) = x^{p^n - 1} - 1 = \prod_{\alpha \in K^\times} (x - \alpha).$$

Af sætning 10 følger derfor, at der pånær en $\mathbb{F}_p$-isomorfi højst er et legeme K med $|K| = p^n$.

Det kan omvendt let vises, at spaltningslegemet K for polynomiet f over $\mathbb{F}_p$ faktisk har $|K| = p^n$. For hvert primtal p og hvert $n \in \mathbb{N}$ findes derfor

pånær en $\mathbb{F}_p$-isomorfi præcist et endeligt legeme K med $|K| = p^n$. Dette legeme betegnes ofte $\mathbb{F}_{p^n}$. Der gælder yderligere det vigtige resultat, at den multiplikative gruppe $\mathbb{F}_{p^n}^\times$ heri er cyklisk.

$K = \mathbb{F}_{p^n}$ er galois over $k = \mathbb{F}_p$, da K er spaltningslegeme for polynomiet $f(x) = x^{p^n-1} - 1$. Endvidere er

$$|G| = |\mathrm{Gal}(K/k)| = [K : k] = n.$$

For at beskrive elementerne i G betragtes afbildningen $\sigma_F : K \to K$, der er defineret ved $\sigma_F(x) = x^p$. Da

$$\begin{aligned}\sigma_F(x+y) &= (x+y)^p = x^p + \cdots + \binom{p}{j} x^{p-j}y^j + \cdots + y^p \\ &= x^p + y^p = \sigma_F(x) + \sigma_F(y), \\ \sigma_F(xy) &= (xy)^p = x^p y^p = \sigma_F(x)\sigma_F(y),\end{aligned}$$

er σ_F en homomorfi. Da

$$\ker \sigma_F = \{x \in K \mid x^p = 0\} = \{0\},$$

er σ_F injektiv, og da K er endelig derfor bijektiv. Da

$$\sigma_F(1) = 1^p = 1, \sigma_F(1+1) = 1+1, \quad \text{etc.},$$

er σ_F en k-automorfi af K. Med andre ord: $\sigma_F \in G = \mathrm{Gal}(K/k)$. σ_F kaldes *Frobenius automorfien* for K over k.

Vi viser endelig, at

$$G = \mathrm{Gal}(K/k) = \langle \sigma_F \rangle = \{\sigma_F^\nu \mid 0 \le \nu < n\} \simeq C_n.$$

Det er klart, at σ_F^ν er en k-automorfi for $\nu \in \mathbb{Z}$. Endvidere er de anførte n automorfier alle forskellige, da de virker forskelligt på et frembringerelement for den cykliske gruppe $K^\times$ af orden $p^n - 1$. På den anden side er $|G| = n$, hvorfor vi har vist det ønskede.

Da en cyklisk gruppe C_n har undergrupper $G' = C_{n/m}$, hvor $m \,|\, n$, følger det af Galoisteoriens hovedsætning, at $\mathbb{F}_{p^n}$ har korresponderende dellegemer $K' = \mathbb{F}_{p^m}$, jf nedenstående diagram:

$$\begin{array}{ccc} K = \mathbb{F}_{p^n} & \longleftrightarrow & E \\ \cup & & \cap \\ K' = \mathbb{F}_{p^m} & \longleftrightarrow & G' = \langle \sigma_F^m \rangle \simeq C_{n/m} \\ \cup & & \cap \\ k = \mathbb{F}_p & \longleftrightarrow & G = \langle \sigma_F \rangle \simeq C_n \end{array}$$

Opgaver:

Opgave 1. Bevis Eisensteins irreducibilitetskriterium (jf eksempel 1). Vink: Betragt den naturlige homomorfi $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ og den dertil svarende homomorfi $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$. Benyt derefter et indirekte bevis.

Opgave 2. Bevis Gauss' lemma (jf eksempel 1). Vink: Et polynomium

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

kaldes *primitivt*, hvis $\gcd(a_n, a_{n-1}, \ldots, a_0) = 1$. Vis, at fg er primitivt, hvis f og g er det. Benyt dette til at vise, at en faktorisering af

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

inden for $\mathbb{Q}[x]$ automatisk er en faktorisering inden for $\mathbb{Z}[x]$.

Opgave 3. Lad p være et primtal. Vis, at cirkeldelingspolynomiet

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

er irreducibelt i $\mathbb{Q}[x]$. Vink: Betragt i stedet polynomiet g givet ved $g(x) = \Phi_p(x + 1)$, og benyt Eisensteins irreducibilitetskriterium og Gauss' lemma.

Opgave 4. Lad p være et ulige primtal, og betragt cirkeldelingslegemet $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/p}$. Vis, at basen $\omega = (1, \zeta, \zeta^2, \ldots, \zeta^{p-2})$ har diskriminant $(-1)^{\frac{p-1}{2}} p^{p-2}$. Vink: Generalisér betragtningen i eksempel 7.

Opgave 5. Lad $n > 1$, og betragt legemet $K = \mathbb{Q}(\sqrt[n]{2})$ (jf eksempel 1). Find diskriminanten for basen

$$\omega = (1, \sqrt[n]{2}, (\sqrt[n]{2})^2, \ldots, (\sqrt[n]{2})^{n-1}).$$

2. Dedekindringe

I det følgende betegner R en kommutativ ring med etelement. Som bekendt kaldes et ideal $\mathfrak{p} \subset R$ et primideal, hvis $R \backslash \mathfrak{p}$ er afsluttet overfor multiplikation, dvs. hvis $R/\mathfrak{p}$ er et integritetsområde (med mindst 2 elementer). Tilsvarende kaldes et ideal $\mathfrak{m} \subset R$ et maksimalt ideal, hvis der ikke findes noget ideal $\mathfrak{a}$, så at $\mathfrak{m} \subset \mathfrak{a} \subset R$, dvs. hvis $R/\mathfrak{m}$ er et legeme (med mindst 2 elementer).

Definition. Et integritetsområde R kaldes en *Dedekindring*, hvis ethvert ideal $\neq (0)$ i R på en og kun en måde kan skrives som produkt af primidealer i R. I den forbindelse opfattes R som det tomme produkt af primidealer.

Vi vil – efter passende forberedelser – vise følgende to hovedsætninger om Dedekindringe:

Sætning 16. *(Karakterisering af Dedekindringe). For et integritetsområde R er følgende fire egenskaber ækvivalente:*

N. R opfylder aksiomerne (Noether betingelserne):

N1. R er noethersk.

N2. Ethvert primideal $\neq (0)$ i R er maksimalt.

N3. R er helt afsluttet.

D. R er en Dedekindring.

G. De brudne idealer $\neq (0)$ i R udgør en multiplikativ gruppe.

P. Ethvert helt ideal $\mathfrak{a}$ i R er en projektiv R-modul. Dette betyder, at der for ethvert diagram af formen:

$$\begin{array}{ccccc} & & \mathfrak{a} & & \\ & & \downarrow{\scriptstyle f} & & \\ X & \xrightarrow{\varphi} & Y & \longrightarrow & 0 \end{array}$$

hvor X, Y er R-moduler, f en homomorfi og φ en surjektiv homomorfi, findes en homomorfi $\tilde{f} : \mathfrak{a} \to X$, så at $\varphi\tilde{f} = f$, dvs. så nedenstående diagram kommuterer:

$$\begin{array}{ccccc} & & \mathfrak{a} & & \\ & \swarrow^{\tilde{f}} & \downarrow{\scriptstyle f} & & \\ X & \xrightarrow{\varphi} & Y & \longrightarrow & 0 \end{array}$$

Sætning 17. *(Udvidelser af Dedekindringe). Lad R være et integritetsområde, K dets brøklegeme, og lad K' være en endelig udvidelse af K. Lad R' være mængden af elementer i K' som er hele mht. R, jf diagrammet:*

$$\begin{array}{ccc} K & \subseteq & K' \\ \cup & & \cup \\ R & \subseteq & R' \end{array}$$

Da gælder: Såfremt R er en Dedekindring, er R' det også, og K' er brøklegeme for R'.

Bemærkning. En hovedidealring (PID) R er en Dedekindring. Der gælder nemlig som bekendt: R er PID $\Rightarrow$ R er UFD (*unique factorization domain* = *faktoriel*). I en faktoriel ring kan ethvert $a \in R$ ($a \neq 0$) på netop en måde skrives $a = rp_1 \cdots p_s$, hvor r er et *invertibelt* element i R, og $p_1, \ldots, p_s$ er *irreducible* elementer i R. Hovedidealet $(a) \neq (0)$ har derfor faktoriseringen $(a) = (p_1) \cdots (p_s)$ – og kun denne – som produkt af primidealer.

Specielt er $\mathbb{Z}$ derfor en Dedekindring. Vi kan derfor anvende udvidelsessætningen med $R = \mathbb{Z}$ og (K, K') erstattet af $(\mathbb{Q}, K)$, hvor K er et vilkårligt algebraisk tallegeme (altså $K \subset \mathbb{C}$ med $[K : \mathbb{Q}] \in \mathbb{N}$). Herved fås, at ringen R af hele algebraiske elementer i K er en Dedekindring. Disse specielle – men vigtige – Dedekindringe vil vi kalde *klassiske* Dedekindringe. Dette hovedresultat for de klassiske Dedekindringe blev først vist af R. Dedekind (1831-1916). I en klassisk Dedekindring kaldes invertible og irreducible elementer traditionelt *enheder* og *primelementer*.

De tre betingelser under N er opkaldt efter Emmy Noether (1882-1935), der var datter af geometeren Max Noether (1844-1921).

I modsætning til klassen af Dedekindringe er hverken klassen PID eller UFD stabil over for en udvidelse af den betragtede art, hvilket illustreres af følgende eksempel.

Eksempel 14. For $R = \mathbb{Z}, K = \mathbb{Q}, K' = \mathbb{Q}(\sqrt{-5}), R' = \{a_0 + a_1\sqrt{-5} \mid a_0, a_1 \in \mathbb{Z}\}$, er R' ikke UFD – og derfor heller ikke PID, da $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ har (mindst) to væsentligt forskellige faktoriseringer i primelementer i R'.

Noetherske ringe og noetherske moduler. En ring R siges at opfylde den *opstigende kædes betingelse* (ACC = *ascending chain condition*), hvis enhver opstigende kæde af idealer i R:

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

er *stationær*, dvs. $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$ for n tilstrækkelig stor.

Et ideal $\mathfrak{a}$ i R kaldes *endeligt frembragt* (forkortes ofte fg = *finitely generated*), hvis der findes endeligt mange elementer $a_1, \ldots, a_k \in \mathfrak{a}$, således at

$$\mathfrak{a} = \{r_1 a_1 + \cdots + r_k a_k \mid r_\kappa \in R\}.$$

Man skriver da

$$\mathfrak{a} = (a_1, \ldots, a_k) = Ra_1 + \cdots + Ra_k.$$

Sætning 18. *R opfylder ACC $\Leftrightarrow$ ethvert ideal i R er endeligt frembragt.*

Bevis. $\Rightarrow$: Lad $\mathfrak{a}$ være et vilkårligt ideal i R. Vælg $a_1 \in \mathfrak{a}$. Hvis $\mathfrak{a} = (a_1)$, er vi færdige, og ellers vælges $a_2 \in \mathfrak{a} \setminus (a_1)$. Hvis $\mathfrak{a} = (a_1, a_2)$, er vi færdige, og ellers vælges $a_3 \in \mathfrak{a} \setminus (a_1, a_2)$ etc. Hvis denne procedure ikke standser efter endeligt mange skridt med $\mathfrak{a} = (a_1, a_2, \ldots, a_k)$, fås en uendelig ægte opstigende kæde

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots,$$

i strid med at R opfylder ACC.

$\Leftarrow$: Betragt en vilkårlig opstigende kæde af idealer i R:

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

Da er

$$\mathfrak{a} = \bigcup_1^\infty \mathfrak{a}_n$$

ligeledes et ideal i R, altså efter antagelsen

$$\mathfrak{a} = (a_1, \ldots, a_k).$$

Lad $n \in \mathbb{N}$ være så stor, at $a_1, \ldots, a_k \in \mathfrak{a}_n$. Da er

$$\mathfrak{a} \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \mathfrak{a}_{n+2} \subseteq \cdots \subseteq \mathfrak{a},$$

hvorfor $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$. □

Definition. En ring R kaldes *noethersk*, hvis R opfylder ACC.

Sætning 19. *(Hilberts basissætning). R noethersk $\Rightarrow$ $R[x]$ noethersk.*

Bevis. Dette deles i fire skridt:

1. Til hvert ideal $\mathfrak{a}$ i $R[x]$ tilordnes en følge af idealer $\mathfrak{a}_n$ i R:

$$\mathfrak{a} \mapsto (\mathfrak{a}_0, \mathfrak{a}_1, \dots)$$

på følgende måde:

$$\mathfrak{a}_n = \{a_n \in R \mid \exists f(x) = a_n x^n + \cdots + a_0 \in \mathfrak{a}\} \quad \text{for} \quad n \in \mathbb{N}_0.$$

Det er let at se, at $\mathfrak{a}_n$ er et ideal i R, og at

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \cdots .$$

For fx at vise, at $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ betragtes et vilkårligt $a_n \in \mathfrak{a}_n$. Dertil findes et polynomium $f(x) = a_n x^n + \cdots + a_0 \in \mathfrak{a}$. Da $\mathfrak{a}$ er et ideal i $R[x]$, vil også $xf(x) = a_n x^{n+1} + \cdots + a_0 x \in \mathfrak{a}$, hvorfor $a_n \in \mathfrak{a}_{n+1}$.

2. Lad $\mathfrak{a}, \mathfrak{b}$ være idealer i $R[x]$ med tilordnede følger af idealer $\mathfrak{a}_n, \mathfrak{b}_n$ i R. Da gælder:

$$\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{a}_n \subseteq \mathfrak{b}_n \quad \text{for} \quad n \in \mathbb{N}_0.$$

Lad nemlig $a_n \in \mathfrak{a}_n$, og lad $f(x) = a_n x^n + \cdots + a_0 \in \mathfrak{a}$. Da $\mathfrak{a} \subseteq \mathfrak{b}$, er også $f \in \mathfrak{b}$, hvorfor $a_n \in \mathfrak{b}_n$.

3. Lad $\mathfrak{a}, \mathfrak{b}$ være idealer i $R[x]$ med tilordnede følger af idealer $\mathfrak{a}_n, \mathfrak{b}_n$ i R. Da gælder:

$$\mathfrak{a} \subseteq \mathfrak{b} \quad \text{og} \quad \mathfrak{a}_n = \mathfrak{b}_n \quad \text{for} \quad n \in \mathbb{N}_0 \quad \Rightarrow \quad \mathfrak{a} = \mathfrak{b}.$$

Det er nok at vise, at $\mathfrak{b} \subseteq \mathfrak{a}$. Vi viser ved induktion efter n, at ethvert n'te gradspolynomium $f \in \mathfrak{b}$ også er i $\mathfrak{a}$. For $n = 0$ er $f(x) = b_0 \in \mathfrak{b}_0 = \mathfrak{a}_0$, hvorfor $f(x) \in \mathfrak{a}$. Antag dernæst, at påstanden er rigtig for ethvert polynomium af grad $< n$, og betragt polynomiet $f \in \mathfrak{b}$ af grad n. Lad $f(x) = b_n x^n + \cdots + b_0$. Da $b_n \in \mathfrak{b}_n = \mathfrak{a}_n$ findes et polynomium $g(x) = b_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathfrak{a}$. Da $\mathfrak{a} \subseteq \mathfrak{b}$ er $h = f - g \in \mathfrak{b}$, og da $\partial h < n$, er h ifølge induktionsantagelsen i $\mathfrak{a}$. Altså er også $f = g + h \in \mathfrak{a}$.

4. Lad $\mathfrak{a}^0 \subseteq \mathfrak{a}^1 \subseteq \cdots$ være en vilkårlig opstigende kæde af idealer i $R[x]$ med tilordnede følger:

$$\begin{array}{lcllll} \mathfrak{a}^0 & \mapsto & (\mathfrak{a}_0^0, & \mathfrak{a}_1^0, & \mathfrak{a}_2^0, & \dots) \\ \mathfrak{a}^1 & \mapsto & (\mathfrak{a}_0^1, & \mathfrak{a}_1^1, & \mathfrak{a}_2^1, & \dots) \\ \mathfrak{a}^2 & \mapsto & (\mathfrak{a}_0^2, & \mathfrak{a}_1^2, & \mathfrak{a}_2^2, & \dots) \\ \vdots & & \vdots & \vdots & \vdots & \ddots \end{array}$$

Af 1 og 2 følger, at de tilordnede idealer i skemaet er opstigende mod højre og nedad. Heraf følger, at diagonalfølgen er opstigende:

$$\mathfrak{a}_0^0 \subseteq \mathfrak{a}_1^1 \subseteq \mathfrak{a}_2^2 \subseteq \cdots .$$

Da R er noethersk findes et $n_0 \in \mathbb{N}_0$ så at $\mathfrak{a}_n^n = \mathfrak{a}_{n+1}^{n+1}$ for $n \geq n_0$. På grund af mængdeinklusionerne i skemaet ovenfor er følgelig

$$\mathfrak{a}_n^k = \mathfrak{a}_{n_0}^{n_0} \quad \text{for} \quad k, n \geq n_0.$$

Da R er noethersk findes et $n_1 \in \mathbb{N}_0$, således at hver af de endeligt mange opstigende kæder

$$\mathfrak{a}_n^0 \subseteq \mathfrak{a}_n^1 \subseteq \cdots \mathfrak{a}_n^k \subseteq \cdots$$

hvor $(0 \leq n < n_0)$, er stationær for $k \geq n_1$. For $k \geq \max(n_0, n_1)$ er da de tilordnede følger for $\mathfrak{a}^k$ helt identiske, hvorfor

$$\mathfrak{a}^k = \mathfrak{a}^{k+1} = \cdots \quad \text{for} \quad k \geq \max(n_0, n_1)$$

ifølge 3. □

Definition. En mængde M kaldes en *R-modul*, hvis M er en additiv abelsk gruppe, og der er defineret en skalær multiplikation $R \times M \to M$, hvor $(r, m) \mapsto rm$, således at følgende aksiomer er opfyldt:

1) $(r_1 + r_2)m = r_1 m + r_2 m$,

2) $r(m_1 + m_2) = rm_1 + rm_2$,

3) $(r_1 r_2)m = r_1(r_2 m)$,

4) $1m = m$.

Aksiomerne er altså de samme som for et vektorrum.

$N \subseteq M$ kaldes en *undermodul*, hvis N er en undergruppe i M og $RN = N$, hvor $RN = \{rn \mid r \in R, n \in N\}$.

En R-modul M siges at være ACC, hvis enhver opstigende kæde af undermoduler i M er stationær.

En undermodul $N \subseteq M$ kaldes *endeligt frembragt* (som R-modul), hvis der findes endeligt mange elementer $n_1, \ldots, n_k \in N$, således at

$$(*) \qquad N = \{r_1 n_1 + \cdots + r_k n_k \mid r_\kappa \in R\}.$$

Man skriver da

$$N = (n_1, \ldots, n_k) = Rn_1 + \cdots + Rn_k.$$

Hvis N har entydig fremstilling på formen (*) (altså $r_1 n_1 + \cdots + r_k n_k = 0 \Rightarrow r_1 = \cdots = r_k = 0$), kaldes N en *fri* R-modul, og $(n_1, \ldots, n_k)$ kaldes en *basis* for N (som R-modul).

Mere generelt kaldes en R-modul M *fri*, hvis der findes en indekseret delmængde $\{e_j \mid j \in J\}$ af M, så at hvert element $m \in M$ på en og kun en måde fremstilles som en endelig sum af formen

$$m = \sum_{j \in J} r_j e_j, \quad \text{hvor} \quad r_j \in R.$$

Sætning 20. *M opfylder ACC $\Leftrightarrow$ enhver undermodul i M er endeligt frembragt.*

Bevis. Som for sætning 18. □

Definition. En R-modul M kaldes *noethersk*, hvis M opfylder ACC.

Sætning 21. *Såfremt R er noethersk og $M = (m_1, \ldots, m_k)$ er en endeligt frembragt R-modul, er M noethersk.*

Bevis. Til hver undermodul N i M tilordnes et endeligt sæt af idealer

$$N \mapsto (\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$$

på følgende måde:

$$\mathfrak{a}_\kappa = \{r_\kappa \in R \mid \exists r_1, \ldots, r_{\kappa-1} \in R,\ r_1 m_1 + \cdots + r_\kappa m_\kappa \in N\}.$$

Beviset er herefter analogt med beviset for sætning 19, men uden diagonalargumentet. □

Eksempel 15. Enhver abelsk gruppe M kan på naturlig måde gøres til en $\mathbb{Z}$-modul ved fastsættelsen $(n, m) \mapsto n \times m$.

Ifølge sætning 21 er enhver endeligt frembragt abelsk gruppe en noethersk $\mathbb{Z}$-modul, dvs. enhver undergruppe af en endeligt frembragt abelsk gruppe er selv endeligt frembragt. En abelsk gruppe kaldes *fri*, hvis den er fri som $\mathbb{Z}$-modul.

Sætning 22. *R er PID $\Leftrightarrow$ enhver undermodul af en (endeligt frembragt) fri R-modul er igen fri.*

Bevis. $\Leftarrow$: R er på naturlig måde en R-modul med basis (1), dvs. R er fri. En undermodul i R (som R-modul) er det samme som et ideal I af R (som ring). Denne del af beviset føres i to skridt:

1. R er en hovedidealring (PIR). Et vilkårligt ideal I af R er ifølge antagelse en fri R-modul, $I = (a_j \mid j \in J)$. Her er $|J| = 1$, thi ellers var fx $a_{i_2}a_{i_1} - a_{i_1}a_{i_2} = 0$ med $(a_{i_1}, a_{i_2}) \neq (0, 0)$.

2. R er et integritetsområde. Antag, at der for $r_1, r_2 \in R$ gælder: $r_1 r_2 = 0$ og $r_2 \neq 0$. Vi skal vise, at $r_1 = 0$. Hovedidealet $(r_2) = Rr_2$ er ifølge antagelse og det under punkt 1 viste en fri R-modul frembragt af ét element $e \in R$, altså $Rr_2 = Re$. Der findes derfor et $r_0 \in R$, så at $e = r_0 r_2$. Nu er $0 = r_0 r_1 r_2 = r_1 e$, hvoraf $r_1 = 0$, da (e) er en R-basis.

$\Rightarrow$: Det er givet, at R er PID. Lad M være en vilkårlig fri R-modul med basis $(e_1, \ldots, e_k)$. Vi skal da vise, at en vilkårlig undermodul N heri er fri. Til N tilordnes som i beviset for sætning 21 et sæt af idealer $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$, hvor

$$\mathfrak{a}_\nu = \{r_\nu \in R \mid \exists r_1, \ldots, r_{\nu-1} \in R,\, r_1 e_1 + \cdots + r_\nu e_\nu \in N\}.$$

Da R er PID, er der for hvert ν, $1 \leq \nu \leq k$, to muligheder:

(i) $\mathfrak{a}_\nu = (0)$,
(ii) $\mathfrak{a}_\nu = (\hat{r}_\nu)$, hvor $\hat{r}_\nu \neq 0$.

I tilfælde (ii) findes derfor et element $\hat{e}_\nu \in N$ af formen

$$(*) \qquad \hat{e}_\nu = \sum_{\mu<\nu} r_{\mu\nu} e_\mu + \hat{r}_\nu e_\nu.$$

Lad $(\nu_1, \ldots, \nu_q)$ være sættet af $\nu \in \{1, 2, \ldots, k\}$ af type (ii), og antag, at $\nu_1 < \cdots < \nu_q$. Da er $(\hat{e}_{\nu_1}, \ldots, \hat{e}_{\nu_q})$ en R-basis for N. Dette vises i to skridt:

3. $(\hat{e}_{\nu_1}, \ldots, \hat{e}_{\nu_q})$ er et uafhængigt sæt over R. Antag, at

$$\lambda_1 \hat{e}_{\nu_1} + \cdots + \lambda_q \hat{e}_{\nu_q} = 0, \quad \text{hvor} \quad \lambda_1, \ldots, \lambda_q \in R.$$

Indsættes (*) heri fås

$$\lambda_1 \left(\sum_{\mu < \nu_1} r_{\mu\nu_1} e_\mu + \hat{r}_{\nu_1} e_{\nu_1} \right) + \cdots + \lambda_q \left(\sum_{\mu < \nu_q} r_{\mu\nu_q} e_\mu + \hat{r}_{\nu_q} e_{\nu_q} \right) = 0.$$

Ved at betragte koefficienterne til $e_{\nu_q}, e_{\nu_{q-1}}, \ldots, e_{\nu_1}$ fås successivt

$$\lambda_q \hat{r}_{\nu_q} = 0 \Rightarrow \lambda_q = 0, \ldots, \lambda_1 \hat{r}_{\nu_1} = 0 \Rightarrow \lambda_1 = 0,$$

idet det benyttes, at R er et integritetsområde (nulregel), og at

$$\hat{r}_{\nu_q}, \ldots, \hat{r}_{\nu_1} \neq 0.$$

4. $(\hat{e}_{\nu_1}, \ldots, \hat{e}_{\nu_q})$ frembringer N. Lad $n \in N$ være skrevet entydigt på formen $n = \sum r_\alpha e_\alpha$. Ved *højden* af n forstås det maksimale α, for hvilket $r_\alpha \neq 0$. Antag nu (indirekte), at $(\hat{e}_{\nu_1}, \ldots, \hat{e}_{\nu_q})$ ikke frembringer hele N. Da findes et $n \in N$ af minimal højde β, så at $n \notin R\hat{e}_{\nu_1} + \cdots + R\hat{e}_{\nu_q}$. Lad

$$n = \sum_{\alpha < \beta} r_\alpha e_\alpha + r_\beta e_\beta, \quad r_\beta \neq 0.$$

Da $r_\beta \in \mathfrak{a}_\beta$ og $r_\beta \neq 0$, er $\beta = \nu_j$ af type (ii) ovenfor. Følgelig er

$$r_\beta \in R\hat{r}_\beta, \quad \text{og} \quad \hat{e}_\beta = \sum_{\mu < \beta} r_{\mu\beta} e_\mu + \hat{r}_\beta e_\beta \in N.$$

Lad $r_\beta = r\hat{r}_\beta, r \in R$, og betragt elementet

$$n - r\hat{e}_\beta = \sum_{\alpha < \beta} r_\alpha e_\alpha - r \sum_{\mu < \beta} r_{\mu\beta} e_\mu.$$

Dette element har højde $< \beta$, hvorfor

$$n - r\hat{e}_\beta = \sum_{\alpha < \beta} r_\alpha e_\alpha \in R\hat{e}_{\nu_1} + \cdots + R\hat{e}_{\nu_q}.$$

Da også $\hat{e}_\beta = \hat{e}_{\nu_j}$, er dette i strid med antagelsen. □

Korollar. *Enhver undergruppe af en (fg) fri abelsk gruppe er (fg) fri.*

Definition. For en fri R-modul M med basis $(e_1, \dots, e_k)$ kaldes k *rangen* af M.

Bemærkning. Det er en simpel opgave i lineær algebra at vise, at rangen er veldefineret. Bemærk også, at det af beviset for sætning 22 fremgår, at når R er PID og M en fri R-modul, er $\text{rang}(N) \leq \text{rang}(M)$ for enhver undermodul N af M.

Hele elementer. I dette afsnit er alle ringe integritetsområder, og R er en delring af T.

Definition. Et element $t \in T$ kaldes *helt* mht. R, hvis det tilfredsstiller en ligning af formen

$$t^m + r_{m-1}t^{m-1} + \cdots + r_1 t + r_0 = 0, \quad \text{hvor} \quad r_\mu \in R,$$

dvs. hvis t er nulpunkt i et polynomium $f_t \in R[x]$ med ledende koefficient 1.

Sætning 23. *Mængden $\overline{R}$ af elementer i T, som er hele mht. R, udgør en ring.*

Bevis. Lad $s, t \in T$ være nulpunkter i polynomier $f_s, f_t \in R[x]$ med ledende koefficienter 1 og sæt $\partial f_s = l$, $\partial f_t = m$. Ved at betragte principale divisionsligninger

$$x^k = f(x)q(x) + r(x), \quad \partial r < \partial f,$$

for $f = f_s$ og $f = f_t$ og indsætte $x = s$ og $x = t$ indses, at

$$\{1, s, s^2, \dots, s^k, \dots\} \subseteq R1 + \cdots + Rs^{l-1} = M_s,$$

og

$$\{1, t, t^2, \dots, t^k, \dots\} \subseteq R1 + \cdots + Rt^{m-1} = M_t.$$

Heraf følger, at

$$(*) \qquad \{s^{k_1}t^{k_2} \mid k_1, k_2 \in \mathbb{N}_0\} \subseteq \sum_{0 \leq \lambda < l, 0 \leq \mu < m} Rs^\lambda t^\mu = M = M_{s,t},$$

hvor $M = Re_1 + \cdots + Re_{lm}$ er en endeligt frembragt R-modul.

For at vise, at $\overline{R}$ er en ring skal det blot vises, at $s,t \in \overline{R} \Rightarrow s-t, s\cdot t \in \overline{R}$. Idet $\circ$ betegner enten $-$ eller $\cdot$, følger det af (*), at $(s\circ t)M \subseteq M$, og derfor er

$$(s\circ t)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{lm} \end{pmatrix} = A\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{lm} \end{pmatrix},$$

hvor A er en $(lm)\times(lm)$-matrix over R. Da $(s\circ t)$ således er en egenværdi for A, er

$$\det(A-(s\circ t)E)=0,$$

hvilket (evt. pånær fortegn) er en ligning af den ønskede art. □

Sætning 24. *Betragt integritetsområder $R\subseteq S\subseteq T$, og antag, at ethvert $s\in S$ er helt mht. R. Da er $\overline{R}=\overline{S}$, hvor overstregning angiver hel afslutning inden for T.*

Bevis. Da det er klart, at $\overline{R}\subseteq\overline{S}$, skal vi vise $\overline{S}\subseteq\overline{R}$. Lad derfor $t\in\overline{S}$ tilfredsstille ligningen

$$t^n+s_{n-1}t^{n-1}+\cdots+s_0=0, \quad s_\nu\in S.$$

Hvert s_ν er helt mht. R, dvs. nulpunkt i et polynomium $f_\nu\in R[x]$ med ledende koefficient 1. Som ovenfor følger derfor, at

$$\{s_0^{k_0}\cdots s_{n-1}^{k_{n-1}} \mid k_\nu\in\mathbb{N}_0\}\subseteq \sum_{0\le k_\nu<\partial f_\nu,\,0\le\nu<n} Rs_0^{k_0}\cdots s_{n-1}^{k_{n-1}} = (e_1,\ldots,e_p).$$

Betragt endelig R-modulen

$$M=(e_1,\ldots,e_p,te_1,\ldots,te_p,\ldots,t^{n-1}e_1,\ldots,t^{n-1}e_p).$$

Da $t^n=-s_{n-1}t^{n-1}-\cdots-s_0$, fremgår det, at $tM\subseteq M$, og som ovenfor giver det karakteristiske polynomium for afbildningen: $m\mapsto tm$ af $M\to M$ det ønskede polynomium. □

I det følgende er R et integritetsområde og K dets brøklegeme.

Definition. Et integritetsområde R kaldes *helt afsluttet*, hvis ethvert element i K, som er helt mht. R tilhører R.

Sætning 25. *R er UFD $\Rightarrow$ R er helt afsluttet.*

Bevis. Betragt $\frac{p}{q} \in K$, hvor $p, q(\neq 0) \in R$, er helt mht. R, og antag uden indskrænkning, at $\gcd(p,q) = 1$. Da vil $\frac{p}{q}$ tilfredsstille en ligning

$$(\frac{p}{q})^n + r_{n-1}(\frac{p}{q})^{n-1} + \cdots + r_0 = 0, \quad r_\nu \in R,$$

hvorfor

$$p^n + r_{n-1}p^{n-1}q + \cdots + r_0 q^n = 0.$$

Heraf følger, at $q \,|\, p^n$ inden for R, og da p og q er indbyrdes primiske, er q er en enhed i R. Altså er $\frac{p}{q} \in R$. □

Sætning 26. *Antag, at R er noethersk og helt afsluttet. Hvis et element $x \in K$ har følgende egenskab:*

$$\exists t \in R \setminus \{0\} \, \forall n \in \mathbb{N} : tx^n \in R,$$

da er $x \in R$. {Et sådant $t \in R \setminus \{0\}$ kaldes en fællesnævner for $x, x^2, \dots$}.

Bevis. Af fællesnævneregenskaben følger, at

$$\{x, x^2, \dots\} \subseteq R \cdot \frac{1}{t} = M.$$

Da R er noethersk fremgår af sætning 21, at M er en noethersk R-modul. Den opstigende kæde

$$(x) \subseteq (x, x^2) \subseteq (x, x^2, x^3) \subseteq \cdots$$

af undermoduler i M er følgelig stationær. Der findes derfor et $n \in \mathbb{N}$, så at

$$x^n \in (x, x^2, \dots, x^{n-1}),$$

hvilket indebærer, at

$$x^n = r_1 x + r_2 x^2 + \cdots + r_{n-1}x^{n-1}, \quad \text{hvor} \quad r_\nu \in R.$$

Denne ligning viser, at x er hel mht. R, og da R er helt afsluttet, at $x \in R$. □

Brudne idealer. I dette afsnit betegner R et integritetsområde med brøklegeme K.

Definition. En ikke tom delmængde $\mathfrak{a}$ af K kaldes et *brudent ideal*, hvis følgende aksiomer er opfyldt:

(i) $$x_1, x_2 \in \mathfrak{a} \Rightarrow x_1 \pm x_2 \in \mathfrak{a}, \quad r \in R,\, x \in \mathfrak{a} \Rightarrow rx \in \mathfrak{a},$$

(ii) $$\exists d \in R \setminus \{0\}\, \forall x \in \mathfrak{a} : dx \in R.$$

Et element d med egenskaben (ii) kaldes en *fællesnævner* for $\mathfrak{a}$.

Bemærkning 1. Et sædvanligt ideal i R er også et brudent ideal (med fællesnævner 1). Fremtidigt kaldes et sådant ideal også et *helt ideal*. Primidealer og maksimale idealer er altid hele idealer.

Bemærkning 2. For $a_1, \ldots, a_r \in K$ betegner $Ra_1 + \cdots + Ra_r = (a_1, \ldots, a_r)$ det brudne ideal frembragt af $a_1, \ldots, a_r$. Det verificeres let, at aksiomerne (i), (ii) er opfyldt. Et brudent ideal $\mathfrak{a}$, der kan skrives på denne form kaldes endeligt frembragt. Specielt betegner $Ra = (a)$ det brudne hovedideal frembragt af $a \in K$.

Definition. Lad $\mathfrak{a}$, $\mathfrak{b}$ være brudne idealer. Da defineres *idealprodukt* og (for $\mathfrak{b} \neq (0)$) *idealkvotient* ved:

$$\mathfrak{ab} = \left\{ \sum_{\text{endelig sum}} a_i b_i \mid a_i \in \mathfrak{a},\, b_i \in \mathfrak{b} \right\},$$

og

$$\mathfrak{a} : \mathfrak{b} = \{x \in K \mid x\mathfrak{b} \subseteq \mathfrak{a}\}.$$

Det må eftervises, at $\mathfrak{ab}$ og $\mathfrak{a} : \mathfrak{b}$ igen er brudne idealer. At betingelse (i) er opfyldt er oplagt i begge tilfælde. Lad $\mathfrak{a}$ og $\mathfrak{b}$ have fællesnævnere d_1 og d_2, da er $d_1 d_2$ en fællesnævner for $\mathfrak{ab}$, og $bd_1 d_2$ er en fællesnævner for $\mathfrak{a} : \mathfrak{b}$ for ethvert $b \in \mathfrak{b} \setminus \{0\}$. Det bemærkes, at produktet er associativt og kommutativt. Endvidere er produktet af to endeligt frembragte brudne idealer igen endeligt frembragt, idet

$$(a_1, \ldots, a_r) \cdot (b_1, \ldots, b_s) = (a_\rho b_\sigma \mid 1 \leq \rho \leq r,\, 1 \leq \sigma \leq s).$$

Sætning 27. *Lad* $\mathfrak{a} = (a)$ *og* $\mathfrak{b} = (b)$ *være brudne hovedidealer i* K *mht.* R*. Da er produktet*

$$\mathfrak{ab} = (ab),$$

et brudent hovedideal. For $\mathfrak{b} \neq (0)$ *er kvotienten*

$$\mathfrak{a} : \mathfrak{b} = (\frac{a}{b})$$

et brudent hovedideal, og der gælder

$$(\mathfrak{a} : \mathfrak{b})\mathfrak{b} = \mathfrak{a}.$$

Mængden af brudne hovedidealer $\neq (0)$ *i* K *mht.* R *udgør en multiplikativ gruppe med* $R = (1)$ *som etelement.*

Bevis. Den eneste påstand, som ikke er helt triviel er, at $\mathfrak{a} : \mathfrak{b} = (\frac{a}{b})$. Da

$$\frac{a}{b}\mathfrak{b} = \frac{a}{b}(b) = \frac{a}{b}Rb = Ra = \mathfrak{a},$$

er $\frac{a}{b} \in \mathfrak{a} : \mathfrak{b}$, hvorfor $(\frac{a}{b}) \subseteq \mathfrak{a} : \mathfrak{b}$. Er omvendt $x \in \mathfrak{a} : \mathfrak{b}$, så er $xb \in \mathfrak{a} = Ra$, altså $x \in R\frac{a}{b} = (\frac{a}{b})$, hvorfor $\mathfrak{a} : \mathfrak{b} \subseteq (\frac{a}{b})$. □

Definition. Et brudent ideal $\mathfrak{a} \neq (0)$ kaldes *invertibelt*, hvis der findes et brudent ideal $\mathfrak{a}'$, så at $\mathfrak{aa}' = (1) = R$.

Sætning 28. *Hvis* $\mathfrak{a}$ *er et invertibelt ideal, er der præcis et ideal* $\mathfrak{a}'$ *med* $\mathfrak{aa}' = R$*, nemlig* $\mathfrak{a}' = R : \mathfrak{a}$*. I dette tilfælde skrives også* $R : \mathfrak{a} = \mathfrak{a}^{-1}$*, og* $\mathfrak{a}^{-1}$ *kaldes* $\mathfrak{a}$*'s inverse ideal.*

Bevis. Da $\mathfrak{aa}' = R$ følger af definitionen på $R : \mathfrak{a}$, at $\mathfrak{a}' \subseteq R : \mathfrak{a}$. Omvendt følger det af definitionen på idealkvotient, at $\mathfrak{a}(R : \mathfrak{a}) \subseteq R$, hvorfor

$$R : \mathfrak{a} = \mathfrak{a}'\mathfrak{a}(R : \mathfrak{a}) \subseteq \mathfrak{a}'.$$

Dette viser, at $\mathfrak{a}' = R : \mathfrak{a}$. □

Sætning 29. *Ethvert invertibelt ideal $\mathfrak{a}$ er endeligt frembragt.*

Bevis. Da $1 \in R = \mathfrak{a}\mathfrak{a}'$ følger af definitionen på idealprodukt, at 1 har en fremstilling

$$1 = a_1 a_1{}' + \cdots + a_n a_n{}', \quad \text{hvor} \quad a_\nu \in \mathfrak{a},\ a'_\nu \in \mathfrak{a}'.$$

For ethvert $a \in \mathfrak{a}$ er derfor

$$a = a \cdot 1 = a(a_1 a_1{}' + \cdots + a_n a_n{}') = (a a_1{}')a_1 + \cdots + (a a_n{}')a_n,$$

hvor $r_\nu = a a_\nu{}' \in \mathfrak{a}\mathfrak{a}' = R$ for alle ν. Dette viser, at $\mathfrak{a} = (a_1, \ldots, a_n)$. □

Sætning 30. *Hvis et primideal $\mathfrak{p}$ indeholder et produkt $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ af hele ideal er, da indeholder $\mathfrak{p}$ mindst en af faktorerne.*

Bevis. Antag (indirekte), at $\mathfrak{p}$ ikke indeholder noget $\mathfrak{a}_\nu$. Da findes for hvert ν, $1 \le \nu \le n$, et $a_\nu \in \mathfrak{a}_\nu$, så at $a_\nu \notin \mathfrak{p}$. Altså er

$$a_1, \ldots, a_n \in R \setminus \mathfrak{p}, \quad \text{men} \quad a_1 \cdots a_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{p}$$

i strid med, at $R \setminus \mathfrak{p}$ er multiplikativt afsluttet (definition af primideal). □

Sætning 31. *Et produkt af brudne idealer er invertibelt, hvis og kun hvis hver faktor er det.*

Bevis. Hvis $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ alle er invertible, er $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ åbenbart invertibelt med

$$\mathfrak{a}^{-1} = \mathfrak{a}_1{}^{-1} \cdots \mathfrak{a}_n{}^{-1}.$$

Hvis omvendt $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ er invertibelt, er $\mathfrak{a}^{-1}\mathfrak{a}_1 \cdots \mathfrak{a}_n = R$. Heraf aflæses, at hvert $\mathfrak{a}_\nu$ har et inverst. □

Sætning 32. *Lad $\mathfrak{a}$ være et helt ideal, som kan skrives som produkt af invertible primidealer. Da har $\mathfrak{a}$ kun denne ene fremstilling (pånær rækkefølge) som produkt af primidealer.*

Bevis. Dette føres ved induktion efter antallet n af primidealer i det givne produkt af invertible primidealer. For $n = 0$ er $\mathfrak{a} = R$ det tomme produkt af

primidealer. I dette tilfælde følger påstanden af, at der for ethvert ikke tomt produkt af primidealer gælder

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1 \cdot R \cdots R = \mathfrak{p}_1 \subset R.$$

Antag dernæst, at påstanden er vist for alle hele idealer, der kan skrives som produkt af færre end $n(> 0)$ invertible primidealer, og betragt et helt ideal $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, hvor $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ er invertible primidealer. Lad $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ være en vilkårlig fremstilling af $\mathfrak{a}$ som produkt af primidealer. Disse er da invertible ifølge sætning 31. Blandt idealerne $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ findes et minimalt, fx $\mathfrak{p}_1$. Da

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

følger det af sætning 30, at $\mathfrak{p}_1$ indeholder et $\mathfrak{q}_\sigma$, fx $\mathfrak{q}_1$. Analogt må $\mathfrak{q}_1$ indeholde et $\mathfrak{p}_\nu$, $1 \leq \nu \leq n$. Altså gælder $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \supseteq \mathfrak{p}_\nu$. Da $\mathfrak{p}_1$ var minimalt blandt $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, er derfor $\mathfrak{p}_1 = \mathfrak{q}_1 = \mathfrak{p}_\nu$. Ved multiplikation med ${\mathfrak{p}_1}^{-1} = {\mathfrak{q}_1}^{-1}$ fås $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_s$, hvorefter entydigheden nu følger af induktionsantagelsen. □

Sætning 33. *Lad R være et noethersk integritetsområde. Da indeholder ethvert helt ideal $\mathfrak{a} \neq (0)$ et produkt af primidealer: $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$, $n \in \mathbb{N}_0$, hvor hvert $\mathfrak{p}_\nu \neq (0)$.*

Bevis. Hvis $\mathfrak{a}$ er lig R eller er et primideal, er påstanden klar. Hvis $\mathfrak{a} \neq R$ ikke er et primideal, findes elementer $b, c \notin \mathfrak{a}$, så at $bc \in \mathfrak{a}$ ($R \setminus \mathfrak{a}$ er ikke multiplikativt afsluttet). Betragt de hele idealer

$$\mathfrak{b} = \mathfrak{a} + (b), \quad \mathfrak{c} = \mathfrak{a} + (c).$$

Da er $\mathfrak{b} \supset \mathfrak{a}$, $\mathfrak{c} \supset \mathfrak{a}$, medens

$$\mathfrak{bc} = (\mathfrak{a} + (b))(\mathfrak{a} + (c)) \subseteq \mathfrak{a} + (bc) \subseteq \mathfrak{a} + \mathfrak{a} = \mathfrak{a}.$$

Hvis både $\mathfrak{b}$ og $\mathfrak{c}$ indeholder produkter af fra (0) forskellige primidealer, gør $\mathfrak{a}$ det også. Hvis $\mathfrak{a}$ derfor ikke indeholder et produkt af fra (0) forskellige primidealer, kan vi ved gentagelse af ræsonnementet konstruere en ægte opstigende kæde af hele idealer med samme egenskab. Men dette er i strid med, at R var antaget noethersk. □

Sætning 34. *I et noethersk integritetsområde R er ethvert helt ideal $\mathfrak{a} \neq R$ indeholdt i et maksimalt ideal.*

Bevis. Antag (indirekte), at $\mathfrak{a}$ ikke er indeholdt i noget maksimalt ideal. Da er specielt $\mathfrak{a}$ ikke maksimalt, hvorfor der findes et helt ideal $\mathfrak{a}_1$ med $\mathfrak{a} \subset \mathfrak{a}_1 \subset R$. Da $\mathfrak{a}$ ikke er indeholdt i et maksimalt ideal er specielt $\mathfrak{a}_1$ ikke er maksimalt. Ræsonnementet giver derfor ved fortsættelse en ægte opstigende kæde af hele idealer. Men dette er i strid med, at R var antaget noethersk. □

Bemærkning. Sætning 34 kan ved Zorn's lemma vises under svagere antagelser om ringen R, fx er *noethersk* ikke påkrævet. Specielt viser sætningen, at der findes maksimale idealer i R.

Bevis for Sætning 16 (Karakterisering af Dedekindringe). Beviset deles i en række afsnit:

$N \Rightarrow D$. Vi antager i dette afsnit, at R opfylder Noetherbetingelserne N1, N2, N3 og viser først to lemmaer:

Lemma 1. *Lad $\mathfrak{p} \neq (0)$ være et primideal i R. Da er $R : \mathfrak{p} \supset R$.*

Bevis. Vælg $b \in \mathfrak{p}$, $b \neq 0$. Ifølge sætning 33 indeholder (b) et produkt af primidealer: $(b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Vi skelner mellem to tilfælde:

1. $\exists \nu \in \{1, \ldots, n\}$, så at $(b) \supseteq \mathfrak{p}_\nu$. Da er $\mathfrak{p} \supseteq (b) \supseteq \mathfrak{p}_\nu$, og da $\mathfrak{p}_\nu$ er maksimalt, er $\mathfrak{p} = (b) = \mathfrak{p}_\nu$. Altså er $R : \mathfrak{p}$ et hovedideal og derfor invertibelt. Ifølge sætning 27 (eller sætning 28) er $\mathfrak{p}(R : \mathfrak{p}) = R$, hvorfor $R : \mathfrak{p} \neq R$. Da vi altid har $R : \mathfrak{p} \supseteq R$, er derfor $R : \mathfrak{p} \supset R$ i dette tilfælde.

2. $\forall \nu \in \{1, \ldots, n\}$: $(b) \not\supseteq \mathfrak{p}_\nu$. Vi kan gerne antage, at $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ er valgt, så at $(b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$, men $(b) \not\supseteq \prod \mathfrak{p}_\nu$, hvis et af primidealerne udelades. Om nødvendigt kan dette opnås ved at slette nogle af primidealerne. Da $\mathfrak{p} \supseteq (b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ og $\mathfrak{p}$ er et primideal, følger det af sætning 30, at $\mathfrak{p}$ indeholder en af faktorerne fx $\mathfrak{p}_1$. Da $\mathfrak{p}_1$ er maksimal, er derfor $\mathfrak{p} = \mathfrak{p}_1$, dvs der gælder

$$(b) \supseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_n, \quad \text{men} \quad (b) \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_n.$$

Vælg nu $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \setminus (b)$. Da $a \notin (b)$, er $\frac{a}{b} \notin R$. På den anden side er $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$, hvorfor $a\mathfrak{p} \subseteq (b)$, altså $\frac{a}{b}\mathfrak{p} \subseteq R$, dvs. $\frac{a}{b} \in R : \mathfrak{p}$. □

Lemma 2. *Ethvert primideal $\mathfrak{p} \neq (0)$ i R er invertibelt.*

Bevis. Ifølge sætning 28 skal vi vise, at $\mathfrak{p}(R:\mathfrak{p}) = R$. Da $\mathfrak{p}$ er et helt ideal følger af definitionen på kvotientideal, at

$$\mathfrak{p} = \mathfrak{p}R \subseteq \mathfrak{p}(R:\mathfrak{p}) \subseteq R.$$

Da $\mathfrak{p}$ er maksimalt, er derfor enten $\mathfrak{p}(R:\mathfrak{p}) = \mathfrak{p}$ eller $\mathfrak{p}(R:\mathfrak{p}) = R$. Da vi ønsker at vise det sidste, er det nok at vise, at antagelsen $\mathfrak{p}(R:\mathfrak{p}) = \mathfrak{p}$ fører til en modstrid. Af antagelsen følger umiddelbart

$$(*) \qquad \forall n \in \mathbb{N} : \mathfrak{p}(R:\mathfrak{p})^n = \mathfrak{p}.$$

For et vilkårligt $x \in (R:\mathfrak{p}) \setminus \{0\}$ og et vilkårligt $t \in \mathfrak{p} \setminus \{0\}$ følger da af (*), at

$$\forall n \in \mathbb{N} : tx^n \in \mathfrak{p} \subseteq R.$$

Af sætning 26 følger derfor, at $x \in R$, dvs. $R:\mathfrak{p} \subseteq R$. Men dette er i strid med lemma 1. □

Bevis for $N \Rightarrow D$. Vi skal vise, at ethvert helt ideal $\mathfrak{a} \neq (0)$ i R, på en og kun en måde kan skrives som produkt af primidealer. Det bemærkes, at entydigheden følger af sætning 32 i forbindelse med lemma 2.

For at vise eksistensen af en produktfremstilling definerer vi for $n \in \mathbb{N}_0$:

$$\mathcal{P}_n = \{\text{hele idealer}\,\mathfrak{a} \neq (0) \mid \mathfrak{a} \supseteq \text{ et produkt af højst}\,n\,\text{primidealer} \neq (0)\}.$$

Det er klart, at $\mathcal{P}_0 \subseteq \mathcal{P}_1 \subseteq \cdots$, og det følger af sætning 33, at

$$\bigcup_{n=0}^{\infty} \mathcal{P}_n = \{\text{hele idealer}\,\mathfrak{a} \neq (0)\ i\ R\}.$$

Vi vil nu ved induktion efter $n \in \mathbb{N}_0$ vise, at $\mathfrak{a} \in \mathcal{P}_n$ har en fremstilling som produkt af primidealer ($\neq (0)$). Da $\mathcal{P}_0 = \{R\}$, er påstanden rigtig for $n = 0$, idet R er det tomme produkt af primidealer $\neq (0)$. Antag dernæst, at påstanden er rigtig for ethvert $\mathfrak{a} \in \mathcal{P}_{n-1}$, $(n > 0)$, og betragt et vilkårligt $\mathfrak{a} \in \mathcal{P}_n \setminus \mathcal{P}_{n-1}$. Vi har da $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Ifølge sætning 34 findes et maksimalt ideal $\mathfrak{p}$, så at $\mathfrak{p} \supseteq \mathfrak{a}$. Da $\mathfrak{p} \supseteq \mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ og $\mathfrak{p}$ er et maksimalt ideal og dermed et primideal i R, følger af sætning 30, at der findes et $\nu \in \{1, \ldots, n\}$, så at $\mathfrak{p} \supseteq \mathfrak{p}_\nu$. Vi kan gerne antage, at $\nu = 1$, dvs. $\mathfrak{p} \supseteq \mathfrak{p}_1$. Da $\mathfrak{p}_1$ er maksimalt er

derfor $\mathfrak{p} = \mathfrak{p}_1$, hvorfor $\mathfrak{p} \supseteq \mathfrak{a} \supseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_n$. Da $\mathfrak{p}$ er invertibelt ifølge lemma 2, fås heraf

$$R = \mathfrak{p}(R : \mathfrak{p}) \supseteq \mathfrak{a}(R : \mathfrak{p}) \supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_n.$$

Ifølge induktionsantagelsen findes primidealer $\mathfrak{q}_\sigma$, så at

$$\mathfrak{a}(R : \mathfrak{p}) = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

hvoraf $\mathfrak{a} = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_s$, hvilket er en produktfremstilling som ønsket. □

Udover egenskaben D (= Dedekindring) betragtes følgende tilsyneladende svagere egenskab for et integritetsområde R:

D'. Ethvert helt ideal $\mathfrak{a} \neq (0)$ i R kan skrives som produkt af primidealer.

$D \Rightarrow D'$. Klart.

$D' \Rightarrow G$. Vi antager i dette afsnit, at R opfylder D' og viser først to lemmaer:

Lemma 1'. *Ethvert invertibelt primideal i R er maksimalt.*

Bevis. Antag (indirekte), at $\mathfrak{p}$ er et invertibelt primideal, som ikke er maksimalt i R. Da findes et helt ideal $\mathfrak{a}$ i R med $\mathfrak{p} \subset \mathfrak{a} \subset R$. Vælg $a \in \mathfrak{a} \setminus \mathfrak{p}$, og betragt

$$\mathfrak{p} \subseteq \mathfrak{p} + (a^2) \subseteq \mathfrak{p} + (a) \subseteq \mathfrak{a} \subset R.$$

Ved den naturlige homomorfi $\varphi : R \to R/\mathfrak{p}$ er der en bijektiv forbindelse mellem idealer $\mathfrak{b}$ i R for hvilke $\mathfrak{b} \supseteq \mathfrak{p}$ og idealer i $R/\mathfrak{p}$, og specielt svarer primidealerne til hinanden. Ifølge D' er

$$\mathfrak{p} + (a) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \quad \text{og} \quad \mathfrak{p} + (a^2) = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

hvor $\mathfrak{p}_\nu$, $\mathfrak{q}_\sigma$ er primidealer. Anvendes homomorfien φ på disse produkter fås:

$$(\varphi(a)) = \varphi(\mathfrak{p}_1) \cdots \varphi(\mathfrak{p}_n) \quad \text{og} \quad (\varphi(a))^2 = (\varphi(a)^2) = (\varphi(a^2)) = \varphi(\mathfrak{q}_1) \cdots \varphi(\mathfrak{q}_s).$$

Da $R/\mathfrak{p}$ er et integritetsområde, og $(\varphi(a)) \neq (0)$ er et hovedideal i $R/\mathfrak{p}$, er $(\varphi(a))$ invertibelt. Ifølge sætning 31 er derfor $\varphi(\mathfrak{p}_1), \ldots, \varphi(\mathfrak{p}_n)$ og $\varphi(\mathfrak{q}_1), \ldots,$

$\varphi(\mathfrak{q}_s)$ invertible primidealer. Af sætning 32 følger da, at $s = 2n$ og at der efter omnummerering gælder:

$$\varphi(\mathfrak{p}_1) = \varphi(\mathfrak{q}_1) = \varphi(\mathfrak{q}_2), \ldots, \varphi(\mathfrak{p}_n) = \varphi(\mathfrak{q}_{2n-1}) = \varphi(\mathfrak{q}_{2n}).$$

På grund af den bijektive forbindelse mellem idealerne gælder derfor også:

$$\mathfrak{p}_1 = \mathfrak{q}_1 = \mathfrak{q}_2, \ldots, \mathfrak{p}_n = \mathfrak{q}_{2n-1} = \mathfrak{q}_{2n},$$

hvorfor

$$\mathfrak{p} + (a^2) = (\mathfrak{p} + (a))^2.$$

Vi vil dernæst vise, at

$$(*) \qquad \mathfrak{p}(\mathfrak{p} + (a)) = \mathfrak{p}.$$

Det er klart, at

$$\mathfrak{p}(\mathfrak{p} + (a)) \subseteq \mathfrak{p}R = \mathfrak{p}.$$

Betragt omvendt

$$x \in \mathfrak{p} \subseteq \mathfrak{p} + (a^2) = (\mathfrak{p} + (a))^2.$$

Da kan x skrives som en endelig sum af formen

$$\begin{aligned} x &= \sum \left(p_1^{(\nu)} + ar_1^{(\nu)}\right)\left(p_2^{(\nu)} + ar_2^{(\nu)}\right) \\ &= \sum \left(p_1^{(\nu)}p_2^{(\nu)} + p_1^{(\nu)}ar_2^{(\nu)} + p_2^{(\nu)}ar_1^{(\nu)} + r_1^{(\nu)}r_2^{(\nu)}a^2\right), \end{aligned}$$

hvor $p_1^{(\nu)}, p_2^{(\nu)} \in \mathfrak{p}$ og $r_1^{(\nu)}, r_2^{(\nu)} \in R$. I denne fremstilling er

$$p_1^{(\nu)}p_2^{(\nu)}, p_1^{(\nu)}ar_2^{(\nu)}, p_2^{(\nu)}ar_1^{(\nu)} \in \mathfrak{p},$$

hvorfor også

$$\sum r_1^{(\nu)}r_2^{(\nu)}a^2 = \left(\sum r_1^{(\nu)}r_2^{(\nu)}\right)a^2 \in \mathfrak{p}.$$

Da $a^2 \notin \mathfrak{p}$, er derfor $\sum r_1^{(\nu)}r_2^{(\nu)} = p \in \mathfrak{p}$. Det aflæses nu, at

$$x = \sum \left(p_1^{(\nu)}p_2^{(\nu)} + p_1^{(\nu)}(ar_2^{(\nu)}) + p_2^{(\nu)}(ar_1^{(\nu)})\right) + pa^2 \in \mathfrak{p}(\mathfrak{p} + (a)),$$

og dette viser (*). Da $\mathfrak{p}$ er invertibelt, følger det nu af (*), at $\mathfrak{p} + (a) = R$, og dette er den ønskede modstrid. □

Lemma 2'. *Ethvert primideal $\mathfrak{p} \neq (0)$ i R er invertibelt.*

Bevis. Vælg $a \in \mathfrak{p}$, $a \neq 0$. Ifølge D' gælder

$$\mathfrak{p} \supseteq (a) = \mathfrak{p}_1 \cdots \mathfrak{p}_n,$$

hvor $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ er primidealer. Da (a) er invertibelt, er $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ifølge sætning 31 alle invertible og derfor maksimale ifølge lemma 1'. Da $\mathfrak{p}$ ifølge sætning 30 indeholder et $\mathfrak{p}_\nu$ og $\mathfrak{p}_\nu$ er maksimalt, er $\mathfrak{p} = \mathfrak{p}_\nu$. Altså er $\mathfrak{p}$ invertibelt. □

Bevis for $D' \Rightarrow G$. Da multiplikation af brudne idealer i K mht. R er associativ og har R som etelement, skal det blot vises, at ethvert brudent ideal $\mathfrak{a} \neq (0)$ er invertibelt. Beviset herfor deles i 2 skridt:

1. Ethvert helt ideal $\mathfrak{a} \neq (0)$ er invertibelt. Dette er klart for $\mathfrak{a} = R = (1)$. For $(0) \subset \mathfrak{a} \subset R$ har vi ifølge D': $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, hvor $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ er primidealer. Ifølge lemma 2' er $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ alle invertible, hvorfor $\mathfrak{a}$ er invertibelt ifølge sætning 31.

2. Ethvert brudent ideal $\mathfrak{a} \neq (0)$ er invertibelt. Lad nemlig $d \in R \setminus \{0\}$ være en fællesnævner for $\mathfrak{a}$. Da er $(d)\mathfrak{a} \subseteq R$, hvorfor $(d)\mathfrak{a}$ er et helt ideal $\neq (0)$. Ifølge punkt 1 er $(d)\mathfrak{a}$ invertibelt, hvorfor $\mathfrak{a}$ er invertibelt ifølge sætning 31. □

Bevis for $G \Rightarrow N$. Ifølge sætning 29 er ethvert invertibelt ideal endeligt frembragt, og da (0) er endeligt frembragt, er samtlige brudne idealer ifølge G endeligt frembragt. Dette viser $N1$.

Antag dernæst (indirekte), at $\mathfrak{p} \neq (0)$ er et ikke maksimalt primideal. Da findes et helt ideal $\mathfrak{a}$, så at $(0) \subset \mathfrak{p} \subset \mathfrak{a} \subset R$. Heraf følger, at $\mathfrak{p}\mathfrak{a}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} = R$, så at $\mathfrak{p}\mathfrak{a}^{-1}$ er et helt ideal. Da $\mathfrak{p} = \mathfrak{a}(\mathfrak{p}\mathfrak{a}^{-1})$, og $\mathfrak{p} \subset \mathfrak{a}$, følger det derfor af sætning 30, at $\mathfrak{p} \supseteq \mathfrak{p}\mathfrak{a}^{-1}$. Følgelig er $R \supseteq \mathfrak{a}^{-1}$ eller $\mathfrak{a} \supseteq R$, hvilket er en modstrid. Dette viser $N2$.

Antag endelig, at $x \in K$ er helt mht. R, dvs. x tilfredsstiller en ligning af formen

$$(*) \qquad x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0, \quad \text{hvor} \quad r_\nu \in R.$$

Betragt det brudne ideal $\mathfrak{a}$ givet ved

$$\mathfrak{a} = (1, x, \ldots, x^{n-1}) = R + Rx + \cdots + Rx^{n-1}.$$

Af (*) følger da, at $\forall m \in \mathbb{N} : x^m \in \mathfrak{a}$. Specielt gælder derfor

$$\mathfrak{a}^2 = (1, x, \ldots, x^{2n-2}) = (1, x, \ldots, x^{n-1}) = \mathfrak{a}.$$

Da $\mathfrak{a} \neq (0)$ er invertibelt, fås ved forkortning $\mathfrak{a} = R$. Specielt følger heraf at $x \in R$. Dette viser $N3$. □

Ved beviset for ækvivalensen mellem G og P benyttes følgende tekniske lemma, hvis bevis overlades som en øvelse til læseren.

Lemma 3. *Lad X, Y, Z være R-moduler, og betragt følgen*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

hvor der for homomorfierne f, g gælder: f er injetiv, g er surjektiv, og $\mathrm{im} f = \ker g$. Så er følgende udsagn ensbetydende:

(i) Følgen er spliteksakt, dvs. $Y \simeq X \oplus Z$.

(ii) Der findes en homomorfi $f' : Y \to X$, så at $f'f = 1_X$.

(iii) Der findes en homomorfi $g' : Z \to Y$, så at $gg' = 1_Y$.

Bevis for $G \Rightarrow P$. Lad $\mathfrak{a}$ være et helt ideal i R, og betragt diagrammet

$$\begin{array}{ccccc} & & \mathfrak{a} & & \\ & & \downarrow{\scriptstyle f} & & \\ X & \xrightarrow{\varphi} & Y & \longrightarrow & 0 \end{array}$$

Vi søger nu $\tilde{f} \in \mathrm{Hom}(\mathfrak{a}, X)$, så at $\varphi\tilde{f} = f$. Såfremt $\mathfrak{a} = (0)$, kan vi vælge $\tilde{f} = 0$. I det følgende antages derfor, at $\mathfrak{a} \neq (0)$. Ifølge antagelsen G er $\mathfrak{a}$ invertibel, og da $1 \in (1) = \mathfrak{a}\mathfrak{a}^{-1}$, findes der elementer $a_1, \ldots, a_n \in \mathfrak{a}$ og $b_1, \ldots, b_n \in \mathfrak{a}^{-1}$, så at

$$(*) \qquad 1 = a_1b_1 + \cdots + a_nb_n.$$

Definér nu homomorfier $g' : R^n \to \mathfrak{a}$ og $g : \mathfrak{a} \to R^n$ ved

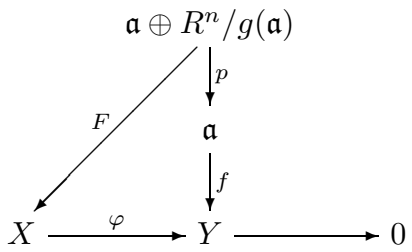
$$g' : (r_1, \ldots, r_n) \mapsto r_1a_1 + \cdots + r_na_n \quad \text{og} \quad g : a \mapsto (ab_1, \ldots, ab_n).$$

Af (*) ses, at $g'g = 1_{\mathfrak{a}}$. Lemma 3 viser derfor, at følgen

$$0 \longrightarrow \mathfrak{a} \xrightarrow{g} R^n \longrightarrow R^n/g(\mathfrak{a}) \longrightarrow 0$$

er spliteksakt, dvs. $R^n \simeq \mathfrak{a} \oplus R^n/g(\mathfrak{a})$. Heraf fremgår, at $\mathfrak{a} \oplus R^n/g(\mathfrak{a})$ er fri; lad (e_i) være en basis for $\mathfrak{a} \oplus R^n/g(\mathfrak{a})$.

Betragt nu diagrammet



hvor $p : \mathfrak{a} \oplus R^n/g(\mathfrak{a}) \to \mathfrak{a}$ er projektionen givet ved $p : (a, x) \mapsto a$. Vi søger her $F : \mathfrak{a} \oplus R^n/\mathfrak{a} \to X$, så at $\varphi F = fp$.

Da φ er surjektiv, findes $x_i \in X$, så at $\varphi(x_i) = (fp)(e_i)$, og da (e_i) er en basis for $\mathfrak{a} \oplus R^n/g(\mathfrak{a})$ findes dernæst en homomorfi $F : \mathfrak{a} \oplus R^n/g(\mathfrak{a}) \to X$ med $F(e_i) = x_i$. Altså gælder:

$$\forall i : (\varphi F)(e_i) = \varphi(x_i) = (fp)(e_i),$$

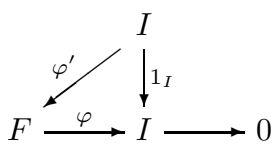
hvilket viser, at $\varphi F = fp$.

Lad nu $\iota : \mathfrak{a} \to \mathfrak{a} \oplus R^n/g(\mathfrak{a})$ være injektionen givet ved $\iota : a \mapsto (a, 0)$. Sæt $\tilde{f} = F\iota \in \mathrm{Hom}(\mathfrak{a}, X)$. Så gælder

$$\varphi \tilde{f} = \varphi F \iota = fp\iota = f.$$

Dette viser, at $\mathfrak{a}$ er en projektiv R-modul. □

Bevis for $P \Rightarrow G$. Lad $\mathfrak{a} \neq (0)$ være et brudent ideal. Vi vil vise, at $\mathfrak{a}$ er invertibelt. Lad d være en fællesnævner for $\mathfrak{a}$. Da er $(d)\mathfrak{a} \subseteq R$, dvs. $I = (d)\mathfrak{a}$ er et helt ideal $\neq (0)$. Vælg en fri R-modul F (tilstrækkelig stor) og en surjektion $\varphi : F \to I$. Betragt nu nedenstående diagram:



Ifølge antagelsen P er I projektiv, hvorfor der findes $\varphi' \in \mathrm{Hom}(I, F)$, så at $\varphi\varphi' = 1_I$. Herefter sluttes af Lemma 3, at følgen:

$$0 \longrightarrow \ker\varphi \xrightarrow{\iota} F \xrightarrow{\varphi} I \longrightarrow 0$$

er spliteksakt, dvs. $F \simeq I \oplus \ker\varphi$.

Dette viser, at $I \oplus \ker\varphi$ er fri; lad (e_i) være en basis for $I \oplus \ker\varphi$. Basiselementet $e_i \in I \oplus \ker\varphi$ har formen

$$e_i = x_i + k_i, \quad \text{hvor} \quad x_i \in I \quad \text{og} \quad k_i \in \ker\varphi.$$

Da $I \neq (0)$ findes et $x \in I \setminus (0)$. Elementet x har en fremstilling af formen

$$x = \sum r_i e_i = \sum r_i x_i + \sum r_i k_i, \quad \text{hvor} \quad r_i \in R.$$

Da I og $\ker\varphi$ danner direkte sum, er $I \cap \ker\varphi = \{0\}$. Af fremstillingen følger derfor

$$x - \sum r_i x_i = \sum r_i k_i \in I \cap \ker\varphi = \{0\} \Rightarrow x = \sum r_i x_i,$$

dvs.

$$(*) \qquad 1 = \sum \frac{r_i}{x} x_i.$$

Men der gælder også

$$(**) \qquad \forall i : \frac{r_i}{x} \in R : I.$$

Thi lad $y \in I$. Så har y formen $y = \sum \rho_i e_i,\ \rho_i \in R$, dvs.

$$\sum x\rho_i e_i = xy = \sum y r_i e_i \Rightarrow \forall i : x\rho_i = y r_i \Rightarrow \forall i : \frac{r_i}{x} y = \rho_i \in R.$$

Af (*) og (**) følger nu, at

$$1 = \sum \frac{r_i}{x} x_i \in (R : I)I \Rightarrow R = (1) \subseteq (R : I)I \subseteq R \Rightarrow R = (R : I)I.$$

Dette viser, at $I = (d)\mathfrak{a}$ er invertibelt, og dermed at $\mathfrak{a}$ er invertibelt. □

Med slutningskæderne $N \Rightarrow D \Rightarrow D' \Rightarrow G \Rightarrow N$ og $G \Leftrightarrow P$ er beviset for den første hovedsætning komplet. □

Bemærkning. At egenskaben D' (eksistens af en fremstilling af helt ideal $\neq (0)$ som produkt af primidealer) er ensbetydende med egenskaben D (Dedekindring), er først vist af Matusita.

Bevis for Sætning 17 (Udvidelser af Dedekindringe). Vi betragter situationen i diagrammet:

$$\begin{array}{ccc} K & \subseteq & K' \\ \cup & & \cup \\ R & \subseteq & R' \end{array}$$

hvor R er den givne Dedekindring med brøklegeme K. Legemet K' er en endelig udvidelse af K, og R' er mængden af elementer i K', som er hele mht. R. Vi viser først to lemmaer.

Lemma 1. *Ethvert $x \in K'$ kan skrives på formen*

$$x = \frac{r'}{r}, \quad \textit{hvor} \quad r' \in R',\, r \in R \setminus \{0\}.$$

Bevis. Da $[K' : K] \in \mathbb{N}$, er x algebraisk over K, dvs.

$$(*) \qquad x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0 = 0, \quad \text{hvor} \quad k_\nu \in K.$$

Da K er brøklegeme for R har vi (med fælles nævner r)

$$(**) \qquad k_\nu = \frac{r_\nu}{r}, \quad \text{hvor} \quad r_\nu \in R,\, r \in R \setminus \{0\}.$$

Indsættes (**) i (*) og ganges igennem med r^n fås:

$$(rx)^n + r_{n-1}(rx)^{n-1} + \cdots + r_1 r^{n-2}(rx) + r_0 r^{n-1} = 0,$$

som viser, at rx er helt mht. R. Følgelig er $rx \in R'$, dvs. $rx = r' \in R'$ eller $x = \frac{r'}{r}$. □

Korollar. *K' er brøklegeme for R'.*

Lemma 2. *For ethvert $r' \in R'$ gælder, at de konjugerede til r' mht. K (inden for en passende udvidelse K^* af K), er hele mht. R. Minimalpolynomiet f for r' mht K tilhører $R[x]$.*

Bevis. Da $r' \in R'$ er helt mht. R, er r' rod i et normeret polynomium $g \in R[x]$. Lad $f \in K[x]$ være minimalpolynomiet for r' mht. K, og lad dette have

rødderne $r_1{}' = r', \ldots, r_k{}'$ $(k = \partial f)$ i et passende udvidelseslegeme K^* for K. Da er $g = fh$, hvor $h \in K[x]$. Følgelig er alle $r_j{}'$ også rødder i g, hvorfor de er hele mht. R. Af

$$f(x) = (x - r_1{}') \cdots (x - r_k{}')$$

følger da ved brug af sætning 23, at alle koefficienter i f er hele mht. R. Da disse koefficienter også tilhører K, og R er helt afsluttet, er $f \in R[x]$. □

Vi skal derpå vise, at R' er en Dedekindring. Dette gøres ved at eftervise Noetherbetingelserne, og beviset falder derfor naturligt i 3 afsnit.

1. R' opfylder $N3$. Da ethvert $r' \in R'$ er helt mht. R, følger det af sætning 24 og definitionen af R', at $\overline{R'} = \overline{R} = R'$, hvor overstregning angiver hel afslutning inden for K'. Da K' ifølge lemma 1 (korollar) er brøklegeme for R', har vi vist $N3$.

2. R' opfylder $N2$. Lad $\mathfrak{p}' \neq (0)$ være et primideal i R'. Vi skal vise, at $\mathfrak{p}'$ er maksimalt, altså at $R'/\mathfrak{p}'$ er et legeme. Dertil skal blot vises, at ethvert fra 0 forskelligt element i $R'/\mathfrak{p}'$ har et inverst eller med andre ord: For ethvert $t \in R'$, $t \not\equiv 0 \pmod{\mathfrak{p}'}$ har kongruensen

$$(*) \qquad tx \equiv 1 \pmod{\mathfrak{p}'}$$

en løsning $x \in R'$. Da R' er hel mht. R, tilfredstiller t en ligning af formen

$$t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0 = 0, \quad \text{hvor} \quad r_\nu \in R,$$

og dermed en kongruens

$$(**) \qquad t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0 \equiv 0 \pmod{\mathfrak{p}'}.$$

Her kan vi gerne antage, at $r_0 \not\equiv 0 \pmod{\mathfrak{p}'}$, thi ellers sættes i (**) en passende potens af t uden for parentes og forkortes væk, da $t \not\equiv 0 \pmod{\mathfrak{p}'}$ og $\mathfrak{p}'$ er et primideal.

Vi viser nu, at $\mathfrak{p} = R \cap \mathfrak{p}'$ er et fra (0) forskelligt primideal i R. At $\mathfrak{p}$ er et ideal er klart. Endvidere er $\mathfrak{p} \subset R$, da $1 \notin \mathfrak{p}' \supseteq \mathfrak{p}$. At $\mathfrak{p}$ er et primideal følger nu af, at der for $x, y \in R$ gælder:

$$\begin{aligned} xy \equiv 0 \pmod{\mathfrak{p}} &\Rightarrow xy \equiv 0 \pmod{\mathfrak{p}'} \Rightarrow x \in \mathfrak{p}' \vee y \in \mathfrak{p}' \\ &\Rightarrow x \in R \cap \mathfrak{p}' = \mathfrak{p} \vee y \in R \cap \mathfrak{p}' = \mathfrak{p}. \end{aligned}$$

For at indse at $\mathfrak{p} \neq (0)$ betragtes $r' \in \mathfrak{p}' \setminus \{0\}$.

De til r' konjugerede mht. R: ${r_1}' = r', \ldots, {r_k}'$(i et passende udvidelseslegeme K^* for K) er da alle hele mht. R ifølge lemma 2, hvorfor ${r_1}' \cdots {r_k}' = N_{K(r')/K}(r')$ er helt mht. R. Da $N_{K(r')/K}(r') \in K$, og R er helt afsluttet, er derfor $r = N_{K(r')/K}(r') \in R$. Endvidere er ${r_2}' \cdots {r_k}' = \frac{r}{r'} \in K'$ og helt mht. R, hvorfor ${r_2}' \cdots {r_k}' \in R'$. Følgelig er $r = ({r_2}' \cdots {r_k}')r' \in \mathfrak{p}'$, altså $r \in \mathfrak{p}' \cap R = \mathfrak{p}$. Da ${r_1}', \ldots, {r_k}'$ alle er $\neq 0$, er $r \neq 0$, altså $\mathfrak{p} \neq (0)$.

I kongruensen (**) er (som antaget) $r_0 \not\equiv 0 \pmod{\mathfrak{p}'}$, hvorfor $r_0 \not\equiv 0 \pmod{\mathfrak{p}}$. Da $\mathfrak{p} \neq (0)$ er et primideal i R og derfor et maksimalt ideal i R, er $R/\mathfrak{p}$ et legeme. Der findes derfor et $c \in R$, så at

$$(***) \qquad r_0 c \equiv -1 \pmod{\mathfrak{p}}.$$

Af (**) og (***) fås nu

$$ct^n + cr_{n-1}t^{n-1} + \cdots + cr_1 t \equiv -r_0 c \equiv 1 \pmod{\mathfrak{p}'},$$

hvilket viser, at

$$x = ct^{n-1} + cr_{n-1}t^{n-2} + \cdots + cr_1$$

løser kongruensen (*). Dette viser $N2$.

3. R' opfylder $N1$. Ved beviset herfor må vi gøre den ekstra antagelse, at udvidelsen K'/K er separabel, skønt sætningen er gyldig i den givne formulering (jf afsnittet om valuationer). Ifølge sætning 15 findes da et primitivt element $\vartheta \in K'$, så $K' = K(\vartheta)$. Ifølge lemma 1 er $\vartheta = \frac{r'}{r}$, hvor $r' \in R'$, $r \in R \setminus \{0\}$, og da $K(\vartheta) = K(r')$, kan vi gerne fra starten antage, at $\vartheta \in R'$. Betragt minimalpolynomiet f_ϑ for ϑ over K:

$$f_\vartheta(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0, \quad r_\nu \in R \quad \text{for} \quad 0 \leq \nu < n = [K' : K],$$

og lad $K^* \supseteq K'$ være spaltningslegeme for f_ϑ. I $K^*[x]$ har vi da

$$f_\vartheta(x) = (x - \vartheta^{(1)}) \cdots (x - \vartheta^{(n)}),$$

hvor $\vartheta^{(1)} = \vartheta, \ldots, \vartheta^{(n)}$ er de konjugerede til ϑ. Disse er indbyrdes forskellige, da K'/K er separabel.

Et vilkårligt element $\xi \in K'$ kan på entydig måde skrives

$$\xi = a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1}, \quad a_\nu \in K.$$

Erstattes her ϑ med sine konjugerede fås:

$$(*)\qquad \begin{aligned} \xi^{(1)} &= a_0 + a_1\vartheta^{(1)} + \cdots + a_{n-1}{\vartheta^{(1)}}^{n-1}, \\ &\vdots \\ \xi^{(n)} &= a_0 + a_1\vartheta^{(n)} + \cdots + a_{n-1}{\vartheta^{(n)}}^{n-1}. \end{aligned}$$

(Her er $\xi^{(1)}, \ldots, \xi^{(n)}$ er de konjugerede til ξ, hver med multiplicitet $n/\mathrm{grad}(\xi)$, men dette bruges ikke.)

Det fremgår af (*) opfattet som lineært ligningssystem i a'_νerne, at ligningssystemets determinant er

$$\Delta = \det \begin{pmatrix} 1 & \vartheta^{(1)} & {\vartheta^{(1)}}^2 & \ldots & {\vartheta^{(1)}}^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \vartheta^{(n)} & {\vartheta^{(n)}}^2 & \ldots & {\vartheta^{(n)}}^{n-1} \end{pmatrix} = \prod_{1\le i<j\le n} (\vartheta^{(j)} - \vartheta^{(i)}) \neq 0$$

ifølge formlen for Vandermonde determinant (jf sætning 9). Ligningssystemet (*) bestemmer derfor $a_0, \ldots, a_{n-1}$ entydigt ud fra $\vartheta^{(1)}, \ldots, \vartheta^{(n)}, \xi^{(1)}, \ldots, \xi^{(n)}$. Efter Cramers formel fås

$$(**)\qquad a_\nu = \frac{1}{\Delta} \det \begin{pmatrix} 1 & \vartheta^{(1)} & \ldots & \xi^{(1)} & \ldots & {\vartheta^{(1)}}^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 1 & \vartheta^{(n)} & \ldots & \xi^{(n)} & \ldots & {\vartheta^{(n)}}^{n-1} \end{pmatrix},$$

hvor

$$\Delta^2 = \det\left(S_{K'/K}(\vartheta^{r+s-2})\right)_{r,s=1,\ldots,n} = D(1, \vartheta, \ldots, \vartheta^{n-1})$$

ifølge sætning 9.

Da $\vartheta \in R'$, er $S_{K'/K}(\vartheta^k) \in R$ for alle $k \in \mathbb{N}_0$. ($S_{K'/K}(\vartheta^k)$ er helt mht. R og ligger i K.) Heraf følger nu, at

$$\Delta^2 \in R.$$

Af (**) fås nu ved forlængelse med Δ

$$a_\nu = P_\nu(\vartheta^{(1)}, \ldots, \vartheta^{(n)}, \xi^{(1)}, \ldots, \xi^{(n)})/\Delta^2,$$

hvor P_ν $(1 \le \nu \le n)$ er et heltalspolynomium. Antager vi derfor, at $\xi = \xi^{(1)} \in R'$, er $\xi^{(1)}, \ldots, \xi^{(n)}$ alle hele mht. R, hvorfor $P_\nu(\cdots)$ er helt mht. R.

Endvidere er $P_\nu(\cdots) = a_\nu \Delta^2 \in K$, altså $P_\nu(\cdots) \in R$. Vi har altså vist, at ethvert $\xi \in R'$ kan skrives på formen:

$$\xi = r_0 \frac{1}{\Delta^2} + r_1 \frac{\vartheta}{\Delta^2} + \cdots + r_{n-1} \frac{\vartheta^{n-1}}{\Delta^2}, \quad r_\nu \in R.$$

Da R selv er en R-modul, er R' altså en undermodul i en endeligt frembragt R-modul, og da R er noethersk, er R' en endeligt frembragt R-modul. Samme ræsonnement gælder (uændret) for enhver R-undermodul af R', hvorfor R' er en noethersk R-modul. Specielt er ethvert ideal i R' endeligt frembragt, altså R' noethersk. □

Bemærkning. Hvis R er PID, er R' en fri R-modul. Det samme gælder for ethvert brudent ideal $\mathfrak{a}'$ i K' mht. R'. Rangen for alle disse frie R-moduler er lig $[K' : K] = n$, bortset fra tilfældet $\mathfrak{a}' = (0)$, som har rang 0.

Bevis. Med $\vartheta \in R'$ som ovenfor er ethvert helt ideal $\mathfrak{a}'$ i R' undermodul i den frie R-modul,

$$R\frac{1}{\Delta^2} + \cdots + R\frac{\vartheta^{n-1}}{\Delta^2},$$

hvorfor $\mathfrak{a}'$ er fri med $\operatorname{rang}_R \mathfrak{a}' \leq n$.

På den anden side gælder for ethvert helt ideal $\mathfrak{a}' \neq (0)$ og $0 \neq r' \in \mathfrak{a}'$ (med betegnelser og argumenter som under punkt 2):

$$0 \neq r = N_{K(r')/K}(r') = r' \cdots r_k{}' \in R \cap \mathfrak{a}'.$$

Altså er

$$\mathfrak{a}' \supseteq rR' \supseteq rR[\vartheta] = \{rr_0 + rr_1\vartheta + \cdots + rr_{n-1}\vartheta^{n-1} \mid r_\nu \in R\},$$

hvorfor

$$\operatorname{rang}_R \mathfrak{a}' \geq \operatorname{rang}_R(rR[\vartheta]) = \operatorname{rang}_R R[\vartheta] = n.$$

Dette viser resultatet for hele idealer i R'. Udvidelsen til brudne idealer er umiddelbar (jf lemma 1). □

Andre sætninger om Dedekindringe.

Sætning 35. *Lad R være en Dedekindring. Da gælder: R er UFD $\Leftrightarrow$ R er PID.*

Bevis. $\Leftarrow$: gælder altid. $\Rightarrow$: Lad $\mathfrak{p} \neq (0)$ være et vilkårligt primideal i R. Vælg $a \in \mathfrak{p}$, $a \neq 0$, og skriv (da R er UFD) $a = rp_1 \cdots p_n$, hvor r er et regulært element, og $p_1, \ldots, p_n$ er irreducible elementer. Da

$$\mathfrak{p} \supseteq (a) = (p_1) \cdots (p_n),$$

og $\mathfrak{p}$ er et primideal, findes et $\nu \in \{1, \ldots, n\}$, så at $\mathfrak{p} \supseteq (p_\nu)$. Da R er UFD og p_ν er irreducibelt, er (p_ν) et primideal. Da R også er en Dedekindring, er (p_ν) maksimalt, og derfor er $\mathfrak{p} = (p_\nu)$. Hermed er vist, at ethvert primideal i R er et hovedideal, og da ethvert helt ideal i R er produkt af primidealer, følger at R er PID. □

Sætning 36. *Lad R være en Dedekindring. Da kan ethvert brudent ideal $\mathfrak{a} \neq (0)$ i R på en og kun en måde skrives på formen*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})},$$

hvor produktet udstrækkes over alle primidealer $\neq (0)$, og $n_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$, således at $n_{\mathfrak{p}} = 0$ for næsten alle $\mathfrak{p}$ (dvs. produktet er endeligt).

Bevis. Det bemærkes først, at ethvert produkt af formen

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})},$$

hvor $n_{\mathfrak{p}} \in \mathbb{Z}$ og næsten alle $n_{\mathfrak{p}} = 0$, ifølge egenskab G bestemmer et brudent ideal i R.

Lad dernæst $\mathfrak{a} \neq (0)$ være et brudent ideal. Da findes et $d \in R \setminus \{0\}$, så at $(d)\mathfrak{a}$ er et helt ideal i R. Følgelig er der fremstillinger

$$(d)\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n, \quad (d) = \mathfrak{p}_1{}' \cdots \mathfrak{p}_m{}',$$

hvor $\mathfrak{p}_\nu$, $\mathfrak{p}_\mu{}'$ er primidealer $\neq (0)$ i R. Vi har da

$$\mathfrak{a} = (d)\mathfrak{a}(d)^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{p}_1{}'^{-1} \cdots \mathfrak{p}_m{}'^{-1},$$

hvilket er en fremstilling af den ønskede art.

Antag endelig, at der findes et brudent ideal $\mathfrak{a} \neq (0)$ med to væsentligt forskellige produktfremstillinger

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}}.$$

Da er

$$\prod_{n_\mathfrak{p} > m_\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = \prod_{m_\mathfrak{p} > n_\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p} - n_\mathfrak{p}}$$

et helt ideal $\neq (0)$ med to væsentligt forskellige fremstillinger som produkt af primidealer. Modstrid! □

Bemærkning. For brudne idealer $\mathfrak{a}$, $\mathfrak{b} \neq (0)$ gælder følgende:

$\mathfrak{a}$ er et helt ideal $\Leftrightarrow \forall \mathfrak{p} : n_\mathfrak{p}(\mathfrak{a}) \geq 0$.

$\forall \mathfrak{p} : n_\mathfrak{p}(\mathfrak{ab}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{b})$.

$\forall \mathfrak{p} : n_\mathfrak{p}(\mathfrak{a}^{-1}) = -n_\mathfrak{p}(\mathfrak{a})$.

$\forall \mathfrak{p} : n_\mathfrak{p}(\mathfrak{a} : \mathfrak{b}) = n_\mathfrak{p}(\mathfrak{ab}^{-1}) = n_\mathfrak{p}(\mathfrak{a}) - n_\mathfrak{p}(\mathfrak{b})$.

Sætning 37. *Lad R være en Dedekindring og $\mathfrak{a}$ og $\mathfrak{b}$ fra (0) forskellige brudne idealer mht. R. Da er følgende egenskaber ækvivalente:*

(i) $\mathfrak{a} \subseteq \mathfrak{b}$.

(ii) $n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b})$ *for alle* $\mathfrak{p}$.

(iii) $\mathfrak{b} \mid \mathfrak{a}$ *(dvs. der findes et helt ideal* $\mathfrak{c}$ *i* R*, så at* $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$*).*

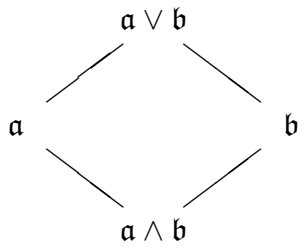
Bevis. At $(ii) \Leftrightarrow (iii)$ følger af, at

$$n_\mathfrak{p}(\mathfrak{ab}^{-1}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{b}^{-1}) = n_\mathfrak{p}(\mathfrak{a}) - n_\mathfrak{p}(\mathfrak{b}).$$

$(iii) \Rightarrow (i)$: $\mathfrak{b} \mid \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c} \subseteq \mathfrak{b} \cdot R = \mathfrak{b}$.
$(i) \Rightarrow (ii)$: $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{ab}^{-1} \subseteq \mathfrak{bb}^{-1} = R \Rightarrow n_\mathfrak{p}(\mathfrak{ab}^{-1}) \geq 0$ for alle $\mathfrak{p} \Rightarrow n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b})$ for alle $\mathfrak{p}$. □

De fra (0) forskellige brudne idealer i en Dedekindring udgør med mængdeinklusionen "$\subseteq$" en partielt ordnet mængde. Denne partielt ordnede mængde er et såkaldt *lattice*, dvs. for vilkårlige $\mathfrak{a}$, $\mathfrak{b}$ i mængden findes et mindste ideal

$\mathfrak{a} \vee \mathfrak{b}$, som indeholder både $\mathfrak{a}$ og $\mathfrak{b}$, og et største ideal $\mathfrak{a} \wedge \mathfrak{b}$, som er indeholdt i både $\mathfrak{a}$ og $\mathfrak{b}$. Jf. nedenstående diagram:



Det er nemlig klart, at

$$\mathfrak{a} \vee \mathfrak{b} = \mathfrak{a} + \mathfrak{b} \quad \text{og} \quad \mathfrak{a} \wedge \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}.$$

Det følger derfor umiddelbart af sætning 37, at

$$n_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})) \quad \text{og} \quad n_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})).$$

Bemærk, at der for vilkårlige brudne idealer $\mathfrak{a}$, $\mathfrak{b}$ gælder

$$\mathfrak{a}\mathfrak{b} = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}),$$

idet påstanden er klar, hvis $\mathfrak{a}$ eller $\mathfrak{b}$ er (0), og ellers følger af

$$n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b}) = \min(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})) + \max(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})).$$

Det betragtede lattice er *distributivt*, idet følgende distributive regler gælder for vilkårlige fra (0) forskellige brudne idealer $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$:

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}) \quad \text{og} \quad \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

Sættes nemlig

$$n_{\mathfrak{p}}(\mathfrak{a}) = A, \quad n_{\mathfrak{p}}(\mathfrak{b}) = B, \quad n_{\mathfrak{p}}(\mathfrak{c}) = C,$$

er disse regler ensbetydende med henholdsvis

$$\max(A, \min(B, C)) = \min(\max(A, B), \max(A, C))$$

og

$$\min(A, \max(B, C)) = \max(\min(A, B), \min(A, C)).$$

Sidstnævnte relationer verificeres umiddelbart i hvert af de tre tilfælde:

$$A \leq \min(B,C), \quad \min(B,C) < A < \max(B,C), \quad \max(B,C) \leq A.$$

Det betragtede lattice har et naturligt *dualt* lattice, der fremkommer ved at erstatte relationen "$\subseteq$" med "$\supseteq$". Ifølge sætning 37 er sidstnævnte relation nemlig den samme som "$|$". Ved den følgende definition passer sprogbrugen bedst med det duale lattice med relation "$|$".

Definition. Lad R være en Dedekindring, og $\mathfrak{a}$ og $\mathfrak{b}$ brudne idealer $\neq (0)$. Da kaldes $\mathfrak{a}+\mathfrak{b}$ og $\mathfrak{a}\cap\mathfrak{b}$ henholdsvis *største fælles divisor* og *mindste fælles multiplum* for $\mathfrak{a}$ og $\mathfrak{b}$.

Sætning 38. *Lad R være en Dedekindring. Lad der være givet forskellige primidealer $\mathfrak{p}_1,\ldots,\mathfrak{p}_n \neq (0)$ og eksponenter $\alpha_1,\ldots,\alpha_n \in \mathbb{N}_0$. Da findes et $a \in R$, så at*

$$n_{\mathfrak{p}_\nu}((a)) = \alpha_\nu \quad \textit{for} \quad 1 \leq \nu \leq n.$$

Bevis. For hvert $\nu \in \{1,\ldots,n\}$ vælges et $a_\nu \in R$, så at

$$a_\nu \in {\mathfrak{p}_1}^{\alpha_1+1}\cdots{\mathfrak{p}_\nu}^{\alpha_\nu}\cdots{\mathfrak{p}_n}^{\alpha_n+1} \setminus {\mathfrak{p}_1}^{\alpha_1+1}\cdots{\mathfrak{p}_\nu}^{\alpha_\nu+1}\cdots{\mathfrak{p}_n}^{\alpha_n+1}.$$

Da er

$$n_{\mathfrak{p}_\nu}((a_\nu)) = \alpha_\nu \quad \text{og} \quad n_{\mathfrak{p}_\mu}((a_\nu)) \geq \alpha_\mu + 1 \quad \text{for} \quad \mu \neq \nu.$$

Sæt $a = a_1 + \cdots + a_n$. Da

$$a_\nu \in {\mathfrak{p}_1}^{\alpha_1}\cdots{\mathfrak{p}_n}^{\alpha_n} \quad \text{for} \quad \nu \in \{1,\ldots,n\},$$

gælder

$$a \in {\mathfrak{p}_1}^{\alpha_1}\cdots{\mathfrak{p}_n}^{\alpha_n} \Rightarrow n_{\mathfrak{p}_\nu}((a)) \geq \alpha_\nu \quad \text{for} \quad 1 \leq \nu \leq n.$$

På den anden side er

$$n_{\mathfrak{p}_\nu}((a_\nu)) = \alpha_\nu \quad \text{og} \quad n_{\mathfrak{p}_\nu}((a_\mu)) \geq \alpha_\nu + 1 \quad \text{for} \quad \mu \neq \nu,$$

hvorfor

$$a = a_1 + \cdots + a_n \equiv a_\nu \not\equiv 0 \pmod{{\mathfrak{p}_\nu}^{\alpha_\nu+1}}.$$

Dette viser, at $n_{\mathfrak{p}_\nu}((a)) \leq \alpha_\nu$ for $1 \leq \nu \leq n$. □

Definition. Lad R være en Dedekindring. To hele idealer $\mathfrak{a}$ og $\mathfrak{b}$ ($\neq (0)$) kaldes *indbyrdes primiske*, hvis $\mathfrak{a}+\mathfrak{b} = R$, dvs. største fælles divisor for $\mathfrak{a}$ og $\mathfrak{b}$ er $R = (1)$.

Sætning 39. *Lad R være en Dedekindring og $\mathfrak{a}$ og $\mathfrak{b}$ hele idealer $\neq (0)$. Såfremt $\mathfrak{a} \subseteq \mathfrak{b}$ findes et element $d \in \mathfrak{b}$, så at $\mathfrak{b} = \mathfrak{a} + (d)$.*

Bevis. Da $\mathfrak{a} \subseteq \mathfrak{b}$, er $n_{\mathfrak{p}}(\mathfrak{a}) \geq n_{\mathfrak{p}}(\mathfrak{b})$. Ifølge sætning 38 findes et $d \in R$, så at $n_{\mathfrak{p}}((d)) = n_{\mathfrak{p}}(\mathfrak{b})$ for alle $\mathfrak{p}$, for hvilke $n_{\mathfrak{p}}(\mathfrak{a}) > 0$. Det er klart, at $n_{\mathfrak{p}}((d)) \geq n_{\mathfrak{p}}(\mathfrak{b})$ for alle $\mathfrak{p}$, hvorfor $d \in \mathfrak{b}$ følge sætning 37. På den anden side er

$$n_{\mathfrak{p}}(\mathfrak{a} + (d)) = \min(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}((d))) = n_{\mathfrak{p}}(\mathfrak{b})$$

for alle $\mathfrak{p}$. □

Korollar 1. *Lad R være en Dedekindring og $\mathfrak{a} \neq (0)$ et helt ideal i R. Da er $R/\mathfrak{a}$ PIR (= principal ideal ring).*

Bevis. Lad $\varphi : R \to R/\mathfrak{a}$ være den naturlige homomorfi, og lad I være et vilkårligt ideal i $R/\mathfrak{a}$. Da er $J = \varphi^{-1}(I)$ et ideal i R, og $\mathfrak{a} \subseteq J \subseteq R$. Der findes derfor ifølge sætning 39 et $d \in J$, så at $J = \mathfrak{a} + (d)$. Følgelig er $I = \varphi(J) = (\varphi(d))$ et hovedideal. □

Korollar 2. *Lad R være en Dedekindring. Ethvert helt ideal $\mathfrak{a}$ er frembragt af højst to elementer. Mere præcist: For ethvert helt ideal $\mathfrak{a} \neq (0)$ og ethvert $a \in \mathfrak{a} \setminus \{0\}$ findes et $b \in \mathfrak{a}$, så at $\mathfrak{a} = (a) + (b) = (a, b)$.*

Bevis. Da $(a) \subseteq \mathfrak{a}$ og $(a) \neq (0)$, findes ifølge sætning 39 et $b \in \mathfrak{b}$, så at $(a) + (b) = \mathfrak{a}$. □

Korollar 3. *Lad R være en Dedekindring og $\mathfrak{a}$ og $\mathfrak{b}$ fra (0) forskellige hele idealer i R. Da findes et helt ideal $\mathfrak{c}$, så at*

$$\mathfrak{a} + \mathfrak{c} = R \quad \textit{og} \quad \mathfrak{bc} \quad \textit{er et hovedideal.}$$

Bevis. Da $\mathfrak{ab} \subseteq \mathfrak{b}$, findes ifølge sætning 39 et $d \in \mathfrak{b} \setminus \{0\}$, så at $\mathfrak{b} = (d) + \mathfrak{ab}$. Da $(d) \subseteq \mathfrak{b}$ vil $\mathfrak{b} \,|\, (d)$, dvs. der findes et helt ideal $\mathfrak{c}$, så at $(d) = \mathfrak{bc}$. Med dette valg af $\mathfrak{c}$ er $\mathfrak{bc} = (d)$ et hovedideal, og yderligere gælder

$$\mathfrak{b} = \mathfrak{bc} + \mathfrak{ab} = (\mathfrak{a} + \mathfrak{c})\mathfrak{b},$$

hvorfor $\mathfrak{a} + \mathfrak{c} = R$. □

Med henblik på en senere anvendelse betragtes i det følgende spørgsmålet om løsbarhed af simultane kongruenser i en Dedekindring. Vi begynder med én kongruens:

Sætning 40. *Lad R være en Dedekindring, og betragt kongruensen*

$$ax \equiv b \pmod{\mathfrak{a}},$$

hvor $a, b \in R$ og $\mathfrak{a} \neq (0)$ er et helt ideal i R. Da gælder:

Kongruensen har en løsning $x \in R \Leftrightarrow (\mathfrak{a} + (a)) \,|\, (b) \Leftrightarrow (b) \subseteq \mathfrak{a} + (a) \Leftrightarrow b \in \mathfrak{a} + (a)$.

Bevis. Da de tre sidste betingelser i sætningen er ækvivalente (jf sætning 37), er det nok at bemærke, at $ax \equiv b \pmod{\mathfrak{a}} \Leftrightarrow b - ax \in \mathfrak{a} \Leftrightarrow b \in \mathfrak{a} + (a)$. □

Sætning 41. *(Den kinesiske restklassesætning). Lad R være en Dedekindring, og lad $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $n \in \mathbb{N}$, være fra (0) forskellige hele idealer i R. Da har systemet af kongruenser:*

$$\begin{aligned} x &\equiv x_1 \pmod{\mathfrak{a}_1} \\ x &\equiv x_2 \pmod{\mathfrak{a}_2} \\ &\vdots \\ x &\equiv x_n \pmod{\mathfrak{a}_n} \end{aligned}$$

for givne $x_1, x_2, \ldots, x_n \in R$ en løsning $x \in R \Leftrightarrow \forall i, j \in \{1, \ldots, n\} : x_i \equiv x_j \pmod{\mathfrak{a}_i + \mathfrak{a}_j}$.

Bevis. $\Rightarrow$: For hvert par (i, j) har delsystemet

$$\begin{aligned} x &\equiv x_i \pmod{\mathfrak{a}_i} \\ x &\equiv x_j \pmod{\mathfrak{a}_j} \end{aligned}$$

en løsning $x \in R$. Følgelig er

$$x_i \equiv x \equiv x_j \pmod{\mathfrak{a}_i + \mathfrak{a}_j}.$$

$\Leftarrow$: Denne implikation vises ved induktion efter n. For $n = 1$ er påstanden klar, da $x = x_1$ er en løsning.

Antag dernæst, at implikationen er opfyldt for ethvert system bestående af $n-1$ kongruenser. Da findes specielt et $x' \in R$, så at

$$x' \equiv x_i \pmod{\mathfrak{a}_i} \quad \text{for} \quad 1 \leq i \leq n-1.$$

Af sætningens antagelse fås da, at

$$x' \equiv x_i \equiv x_n \pmod{\mathfrak{a}_i + \mathfrak{a}_n} \quad \text{for} \quad 1 \leq i \leq n-1,$$

hvorfor

$$x' - x_n \in \bigcap_{i=1}^{n-1} (\mathfrak{a}_i + \mathfrak{a}_n).$$

Da R er en Dedekindring, gælder den distributive regel for "$+$" mht. "$\cap$", hvorfor

$$x' - x_n \in \bigcap_{i=1}^{n-1} (\mathfrak{a}_i + \mathfrak{a}_n) = \mathfrak{a}_n + \bigcap_{i=1}^{n-1} \mathfrak{a}_i.$$

Der findes derfor $a \in \bigcap_1^{n-1} \mathfrak{a}_i$ og $a_n \in \mathfrak{a}_n$, så at $x' - x_n = a + a_n$. Sættes nu $x = x_n + a_n = x' - a$, er

$$x' - x = a \in \bigcap_{i=1}^{n-1} \mathfrak{a}_i,$$

hvorfor

$$x \equiv x' \equiv x_i \pmod{\mathfrak{a}_i} \quad \text{for} \quad 1 \leq i \leq n-1.$$

Da endvidere

$$x = x_n + a_n \equiv x_n \pmod{\mathfrak{a}_n},$$

er $x \in R$ en løsning til systemet af n kongruenser. □

Bemærkning. I det vigtige specialtilfælde, hvor $\mathfrak{a}_i + \mathfrak{a}_j = R$ for alle (i, j), $i \neq j$, dvs. $\mathfrak{a}_i$'erne er parvis indbyrdes primiske, er betingelsen for løsbarhed automatisk opfyldt.

Sætning 42. *Lad R være en Dedekindring, og lad $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, være fra (0) forskellige hele idealer i R. Antag, at $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $1 \leq i < j \leq n$, og sæt $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Da er*

$$R/\mathfrak{a} \simeq R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n,$$

hvor ringen på højre side er direkte sum af restklasseringene $R/\mathfrak{a}_\nu$.

Bevis. For $a \in R$ betegner $\overline{a}$ og $\overline{a}^{(\nu)}$ restklasserne modulo $\mathfrak{a}$ og modulo $\mathfrak{a}_\nu$. Vi betragter afbildningen

$$\varphi : R/\mathfrak{a} \to R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n$$

defineret ved $\varphi(\overline{a}) = (\overline{a}^{(1)}, \ldots, \overline{a}^{(n)})$, idet det bemærkes, at inklusionerne $\mathfrak{a} \subseteq \mathfrak{a}_\nu$ sikrer, at φ er veldefineret, dvs. uafhængig af repræsentanten a for $\overline{a}$.

Efter sin konstruktion er φ en ringhomomorfi. Da $\mathfrak{a} + \mathfrak{b} = R \Rightarrow \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$ (der gælder altid $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a} \cdot \mathfrak{b}$) fås, at

$$\overline{a} \in \ker \varphi \Leftrightarrow a \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a} \Leftrightarrow \overline{a} = \overline{0},$$

dvs. φ er injektiv.

Lad $(\overline{x_1}^{(1)}, \ldots, \overline{x_n}^{(n)})$ være et vilkårligt element i $R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n$. Da $\mathfrak{a}_\nu$'erne er parvis indbyrdes primiske, viser den kinesiske restklassesætning, at systemet af kongruenser:

$$\begin{aligned} x &\equiv x_1 \pmod{\mathfrak{a}_1} \\ &\vdots \\ x &\equiv x_n \pmod{\mathfrak{a}_n} \end{aligned}$$

har en løsning $x \in R$. Følgelig er

$$\varphi(\overline{x}) = (\overline{x}^{(1)}, \ldots, \overline{x}^{(n)}) = (\overline{x_1}^{(1)}, \ldots, \overline{x_n}^{(n)}),$$

dvs. φ er surjektiv. □

Definition. Lad R være en Dedekindring og $\mathfrak{a} \neq (0)$ et helt ideal i R. En restklasse $\overline{a} \pmod{\mathfrak{a}}$ kaldes en *primisk restklasse* modulo $\mathfrak{a}$, såfremt $(a) + \mathfrak{a} = R$. Alternativt betyder dette, at $n_\mathfrak{p}((a)) = 0$ for alle $\mathfrak{p} \mid \mathfrak{a}$.

Bemærkning. Da

$$\overline{a} = \overline{b} \Leftrightarrow a \equiv b \pmod{\mathfrak{a}} \Leftrightarrow a - b \in \mathfrak{a} \Rightarrow a \in (b) + \mathfrak{a} \Rightarrow (a) + \mathfrak{a} \subseteq (b) + \mathfrak{a},$$

gælder $(a) + \mathfrak{a} = R \Rightarrow (b) + \mathfrak{a} = R$, dvs. begrebet primisk restklasse er veldefineret.

Sætning 43. *Lad R være en Dedekindring og $\mathfrak{a} \neq (0)$ et helt ideal i R. Da er $\overline{a}$ en primisk restklasse modulo $\mathfrak{a} \Leftrightarrow \overline{a}$ er et invertibelt element i $(R/\mathfrak{a}, \cdot)$. Alternativt udtrykt: de primiske restklasser modulo $\mathfrak{a}$ udgør en multiplikativ gruppe, nemlig gruppen $(R/\mathfrak{a})^\times$ af invertible elementer i $(R/\mathfrak{a}, \cdot)$.*

Bevis. $\Leftarrow$: Såfremt $\overline{a}$ er en primisk restklasse modulo $\mathfrak{a}$, er $(a) + \mathfrak{a} = R$. Ifølge sætning 40 har kongruensen

$$(*) \qquad ax \equiv 1 \pmod{\mathfrak{a}}$$

derfor en løsning $x = b \in R$, dvs. $\overline{b}$ er invers til $\overline{a}$.

$\Rightarrow$: Såfremt $\overline{a}$ er invertibel, findes en restklasse $\overline{b}$, så at $\overline{a}\overline{b} = \overline{1}$, dvs. kongruensen (*) har en løsning $x = b \in R$. Ifølge sætning 40 gælder derfor

$$1 \in (a) + \mathfrak{a} \Rightarrow (a) + \mathfrak{a} = R.$$

Den resterende del af sætningen følger nu af det viste. □

Sætning 44. *Lad R være en Dedekindring, og lad $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, være fra (0) forskellige hele idealer i R. Antag, at $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $1 \leq i < j \leq n$, og sæt $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Da er den primiske restklassegruppe modulo $\mathfrak{a}$ isomorf med det direkte produkt af de primiske restklassegrupper modulo $\mathfrak{a}_\nu$, $1 \leq \nu \leq n$.*

Bevis. Ved den naturlige isomorfi

$$\varphi : R/\mathfrak{a} \to R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n$$

er $\overline{a}$ en primisk restklasse modulo $\mathfrak{a} \Leftrightarrow \overline{a}$ er invertibelt i $R/\mathfrak{a} \Leftrightarrow \overline{a}^{(\nu)}$ er invertibelt i $R/\mathfrak{a}_\nu$ for $1 \leq \nu \leq n \Leftrightarrow \overline{a}^{(\nu)}$ er en primisk restklasse modulo $\mathfrak{a}_\nu$ for $1 \leq \nu \leq n$. □

I kraft af sætningerne 42 og 44 er det ved undersøgelse af $R/\mathfrak{a}$ tilstrækkeligt at se på $R/\mathfrak{p}^n$, hvor $\mathfrak{p}$ er et primideal $\neq (0)$ og $n \in \mathbb{N}$. Med henblik herpå indfører vi følgende

Definition. Lad R være en Dedekindring og $\mathfrak{p} \neq (0)$ et primideal i R. Et element $\pi \in R$ kaldes et *primelement* for $\mathfrak{p}$, såfremt $\mathfrak{p} \,|\, (\pi)$ men $\mathfrak{p}^2 \nmid (\pi)$. Alternativt betyder dette (jf sætning 37), at $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, eller at $n_{\mathfrak{p}}((\pi)) = 1$.

Bemærkning. Man skriver fx $\mathfrak{p}\,|\,\pi$ i stedet for det mere præcise $\mathfrak{p}\,|\,(\pi)$. Da $\mathfrak{p} \supset \mathfrak{p}^2$ (egenskab D for Dedekindring), findes der et primelement π for ethvert $\mathfrak{p} \neq (0)$. Det ses endvidere, at

$$n_{\mathfrak{p}}((\pi^\nu)) = n_{\mathfrak{p}}((\pi)^\nu) = \nu n_{\mathfrak{p}}((\pi)) = \nu \quad \text{for} \quad \nu \in \mathbb{Z}.$$

Sætning 45. *Lad R være en Dedekindring og $\mathfrak{p} \neq (0)$ et primideal i R. Lad π være et primelement for $\mathfrak{p}$, og lad $\{\alpha_i \mid i \in I\}$ være et repræsentantsystem for restklasserne modulo $\mathfrak{p}$. For $n \in \mathbb{N}$ kan restklasserne modulo $\mathfrak{p}^n$ på en og kun en måde repræsenteres ved*

$$(*) \qquad \alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_{n-1}}\pi^{n-1}, \quad \textit{hvor} \quad i_\nu \in I \quad \textit{for} \quad 0 \leq \nu < n.$$

De primiske restklasser modulo $\mathfrak{p}^n$ svarer præcis til repræsentanter (*) med $\alpha_{i_0} \not\equiv 0 \pmod{\mathfrak{p}}$.

Bevis. Lad $\overline{a}$ være en vilkårlig restklasse modulo $\mathfrak{p}^n$. Vi vil først vise, at der findes $i_0, \ldots, i_{n-1} \in I$, så at

$$a \equiv \alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_{n-1}}\pi^{n-1} \pmod{\mathfrak{p}^n}.$$

Bestemmelsen af $i_0, \ldots, i_{n-1} \in I$ sker successivt. Først vælges $i_0 \in I$, så at $a \equiv \alpha_{i_0} \pmod{\mathfrak{p}}$. Såfremt vi allerede har bestemt $i_0, \ldots, i_{\nu-1} \in I$, så at

$$a \equiv \alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_{\nu-1}}\pi^{\nu-1} \pmod{\mathfrak{p}^\nu},$$

ønsker vi at bestemme $i_\nu \in I$, så at

$$a \equiv \alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_{\nu-1}}\pi^{\nu-1} + \alpha_{i_\nu}\pi^\nu \pmod{\mathfrak{p}^{\nu+1}},$$

dvs. α_{i_ν} skal tilfredsstille kongruensen

$$(**) \qquad \pi^\nu x \equiv a - \left(\alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_{\nu-1}}\pi^{\nu-1}\right) = b \pmod{\mathfrak{p}^{\nu+1}},$$

hvor $b \equiv 0 \pmod{\mathfrak{p}^\nu}$ ifølge antagelsen. Da $n_{\mathfrak{p}}((\pi^\nu)+\mathfrak{p}^{\nu+1}) = \min(\nu, \nu+1) = \nu$, er $(\pi^\nu) + \mathfrak{p}^{\nu+1} = \mathfrak{p}^\nu$, hvorfor $((\pi^\nu) + \mathfrak{p}^{\nu+1})\,|\,(b)$. Ifølge sætning 40, har (**) en løsning $x \in R$. Vælges derfor $i_\nu \in I$, så at $\alpha_{i_\nu} \equiv x \pmod{\mathfrak{p}}$, er $\pi^\nu \alpha_{i_\nu} \equiv \pi^\nu x \pmod{\mathfrak{p}^{\nu+1}}$, så at α_{i_ν} ligeledes er en løsning til kongruensen (**). Eksistensen af en fremstilling (*) er hermed godtgjort.

For at vise entydigheden antages, at

$$\alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_{n-1}}\pi^{n-1} \equiv \alpha_{j_0} + \alpha_{j_1}\pi + \cdots + \alpha_{j_{n-1}}\pi^{n-1} \pmod{\mathfrak{p}^n}.$$

Da er specielt $\alpha_{i_0} \equiv \alpha_{j_0} \pmod{\mathfrak{p}}$, altså $i_0 = j_0$. Da π er et primelement for $\mathfrak{p}$, følger heraf, at

$$\alpha_{i_1} + \cdots + \alpha_{i_{n-1}}\pi^{n-2} \equiv \alpha_{j_1} + \cdots + \alpha_{j_{n-1}}\pi^{n-2} \pmod{\mathfrak{p}^{n-1}}.$$

Da er specielt $\alpha_{i_1} \equiv \alpha_{j_1} \pmod{\mathfrak{p}}$, altså $i_1 = j_1$. Fortsat anvendelse af dette argument viser entydigheden af en fremstilling (*).

Da

$$(a) + \mathfrak{p}^n = R \Leftrightarrow (a) + \mathfrak{p} = R \Leftrightarrow (\alpha_{i_0}) + \mathfrak{p} = R \Leftrightarrow \alpha_{i_0} \not\equiv 0 \pmod{\mathfrak{p}},$$

følger påstanden om de primiske restklasser modulo $\mathfrak{p}^n$. □

Valuationer med henblik på Dedekindringe.

Definition. Lad K være et legeme. En afbildning $|| : K \to \mathbb{R}_+ \cup \{0\}$ kaldes en *(multiplikativ) valuation*, såfremt:

$1'$. $|0| = 0$, $|x| > 0$ for $x \in K \setminus \{0\}$.

$2'$. $|xy| = |x||y|$ for $x, y \in K$.

$3'$. $|x + y| \leq |x| + |y|$ for $x, y \in K$.

Valuationen kaldes *ikke-arkimedisk*, såfremt $3'$ gælder i den stærkere form

$3''$. $|x + y| \leq \max(|x|, |y|)$ for $x, y \in K$.

En afbildning $\nu : K \to \mathbb{R} \cup \{\infty\}$ kaldes en *additiv (ikke-arkimedisk) valuation*, såfremt:

1. $\nu(0) = \infty$, $\nu(x) \in \mathbb{R}$ for $x \in K \setminus \{0\}$.
2. $\nu(xy) = \nu(x) + \nu(y)$ for $x, y \in K$.
3. $\nu(x + y) \geq \min(\nu(x), \nu(y))$ for $x, y \in K$.

Bemærkning. Ved afbildningen $-\log_a : \mathbb{R}_+ \to \mathbb{R}$ svarer en multiplikativ ikke-arkimedisk valuation til en additiv valuation.

Lad (K, ν) være et legeme forsynet med en additiv valuation. Man definerer da

$$V = \{x \in K \mid \nu(x) \geq 0\}, \quad \mathfrak{m} = \{x \in K \mid \nu(x) > 0\}.$$

Det fremgår umiddelbart, at V er et integritetsområde, og at $\mathfrak{m}$ er et ideal i V. Endvidere ses, at

$$U = V \setminus \mathfrak{m} = \{x \in K \mid \nu(x) = 0\}$$

er gruppen af invertible elementer i V. Heraf følger, at $\mathfrak{m} = V \setminus U$ er et maksimalt ideal i V, og at $\mathfrak{m}$ indeholder ethvert ægte ideal i V. Følgelig er $\mathfrak{m}$ det eneste maksimale ideal i V.

V kaldes *valuationsringen* for (K, ν) og $\mathfrak{m}$ det tilhørende maksimale ideal.

Valuationen ν kaldes *diskret*, såfremt værdimængden $\nu(K^\times)$ er en diskret undergruppe $\neq \{0\}$ af $(\mathbb{R}, +)$. En diskret valuation ν kaldes *normeret*, hvis $\nu(K^\times) = \mathbb{Z}$.

To valuationer ν_1 og ν_2 kaldes *ækvivalente*, hvis de tilsvarende valuationsringe er ens. Ensbetydende betingelser er, at de tilhørende maksimale idealer er ens, eller at ν_1 og ν_2 er proportionale.

Lad nu R være en Dedekindring med brøklegeme K, og lad $\mathfrak{p}$ være et primideal $\neq (0)$ i R. For $a \in K$ defineres i kraft af sætning 36:

$$n_{\mathfrak{p}}(a) = \begin{cases} n_{\mathfrak{p}}((a)) & \text{for} \quad a \neq 0 \\ \infty \quad \text{for} & a = 0. \end{cases}$$

Det følger umiddelbart, at $n_{\mathfrak{p}}$ er en normeret (diskret) valuation på K. Vi betegner den tilhørende valuationsring $V_{\mathfrak{p}}$ og det tilhørende maksimale ideal $\mathfrak{m}_{\mathfrak{p}}$ og sætter $U_{\mathfrak{p}} = V_{\mathfrak{p}} \setminus \mathfrak{m}_{\mathfrak{p}}$.

Vi anfører uden bevis to vigtige sætninger, som tilsammen giver en karakterisering af Dedekindringe ved hjælp af valuationer.

Sætning 46. *Lad R være en Dedekindring med brøklegeme K. Da er*

$$(*) \qquad \{n_{\mathfrak{p}} \mid \mathfrak{p} \text{ primideal } \neq (0) \text{ i } R\}$$

samtlige normerede valuationer på K med $V_{\mathfrak{p}} \supseteq R$. Der gælder endvidere

$$\bigcap_{\mathfrak{p}} V_{\mathfrak{p}} = R, \quad \bigcap_{\mathfrak{p}} \mathfrak{m}_{\mathfrak{p}} = (0),$$

$$\forall x \in K^\times : x \in U_{\mathfrak{p}} \quad \text{for næsten alle} \quad \mathfrak{p}.$$

Valuationerne i (*) er indbyrdes inækvivalente og tilfredsstiller følgende betingelse (den stærke approximationssætning):

Givet endeligt mange af valuationerne i (*): $\{n_{\mathfrak{p}_1}, \ldots, n_{\mathfrak{p}_n}\}$, et naturligt tal N og n elementer $a_1, \ldots a_n \in K$. Da findes et element $a \in K$, så at

$$n_{\mathfrak{p}_\nu}(a - a_\nu) \geq N \quad \textit{for} \quad 1 \leq \nu \leq n,$$

og

$$n_{\mathfrak{p}}(a) \geq 0 \quad \textit{for} \quad \mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

Sætning 47. *Lad K være et legeme og $\{n_i \mid i \in I\}$ et system af inækvivalente normerede valuationer på K, som opfylder følgende to betingelser:*

(i) $\forall x \in K^\times : x \in U_i$ for næsten alle $i \in I$.

(ii) Den stærke approximationssætning gælder.

Da er $R = \cap_{i \in I} V_i$ en Dedekindring, og $\{R \cap \mathfrak{m}_i \mid i \in I\}$ samtlige fra (0) forskellige primidealer i R.

Ved hjælp af sætningerne 46 og 47 kan man konstruere en række Dedekindringe. Endvidere kan man med udgangspunkt i den omtalte valuationsteoretiske karakterisering af Dedekindringe vise sætning 17 (udvidelser af Dedekindringe) uden at måtte forudsætte, at udvidelsen er separabel.

Der henvises til E. Artin: Theory of Algebraic Numbers, Göttingen 1959.

Opgaver:

Opgave 1. Lad $K = \overline{\mathbb{Q}}$ være legemet af alle algebraiske tal, og lad $R = \overline{\mathbb{Z}}$ være den hele afslutning af $\mathbb{Z}$ mht. K.

Vis, at ringen R består af alle hele algebraiske tal.

Vis, at ringen R ikke er noethersk.

Vink: Vis fx, at

$$(\sqrt{2}) \subset (\sqrt[4]{2}) \subset (\sqrt[8]{2}) \subset \dots ,$$

hvor idealerne er hovedidealer i R.

Opgave 2. Lad R være et integritetsområde, og lad $\mathfrak{a}_1, \dots , \mathfrak{a}_n$, $n \in \mathbb{N}$, være fra (0) forskellige idealer i R. Betragt systemer af kongruenser:

$$\begin{aligned} x &\equiv x_1 \pmod{\mathfrak{a}_1} \\ x &\equiv x_2 \pmod{\mathfrak{a}_2} \\ &\vdots \\ x &\equiv x_n \pmod{\mathfrak{a}_n} \end{aligned}$$

hvor $x_1, x_2, \dots , x_n \in R$ er givne.

1) Vis, at en nødvendig betingelse for løsning af systemet, er at $x_i \equiv x_j \pmod{\mathfrak{a}_i + \mathfrak{a}_j}$ for $1 \leq i < j \leq n$.

2) Vis, at betingelsen i 1) også er tilstrækkelig for løsbarhed af et vilkårligt system, hvis ethvert system af tre kongruenser, som opfylder betingelsen i 1), er løsbart. I bekræftende fald siges den kinesiske restklassesætning at gælde i ringen R.

Vink: Vis, at løsbarhed af ethvert system af tre kongruenser, som opfylder betingelsen i 1), medfører, at idealerne i R udgør et distributivt lattice, dvs.

$$\mathfrak{a}_1 + (\mathfrak{a}_2 \cap \mathfrak{a}_3) = (\mathfrak{a}_1 + \mathfrak{a}_2) \cap (\mathfrak{a}_1 + \mathfrak{a}_3).$$

Opgave 3. Lad R være et integritetsområde, og lad $\mathfrak{a}_1, \dots , \mathfrak{a}_n$, $n \in \mathbb{N}$, være fra (0) forskellige idealer i R. Antag, at idealerne $\mathfrak{a}_i$ er parvist *comaximale*,

dvs. $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $1 \leq i < j \leq n$. Vis, at ethvert system af kongruenser:

$$\begin{aligned} x &\equiv x_1 \pmod{\mathfrak{a}_1} \\ x &\equiv x_2 \pmod{\mathfrak{a}_2} \\ &\vdots \\ x &\equiv x_n \pmod{\mathfrak{a}_n} \end{aligned}$$

for givne $x_1, x_2, \ldots, x_n \in R$ har en løsning $x \in R$.

Opgave 4. Betragt ringen $R = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$. Vis, at den kinesiske restklassesætning ikke gælder i R.

Opgave 5. Betragt polynomiumsringen $R = K[x, y]$ over et legeme K. Vis, at den kinesiske restklassesætning ikke gælder i R.

Opgave 6. Betragt ringen $R = \overline{Z}$ fra opgave 1. Vis, at den kinesiske restklassesætning gælder i R.

3. Klassiske Dedekindringe

I det følgende betragtes situationen

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & K \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & O_K \end{array}$$

hvor K er et algebraisk tallegeme med $[K:\mathbb{Q}] = n \in \mathbb{N}$, og O_K (efter tysk: *Ordnung*) betegner ringen af hele algebraiske tal i K. Da $\mathbb{Z}$ er en Dedekindring, følger det af sætning 17 (udvidelsessætningen), at O_K er en Dedekindring. Vi vil kalde en sådan en *klassisk* Dedekindring.

Det fremgår af en tidligere bemærkning, at ethvert brudent ideal $\mathfrak{a} \neq (0)$ i K mht. O_K, altså specielt O_K selv, er en fri $\mathbb{Z}$-modul af rang $n = [K:\mathbb{Q}]$.

Definition. Ved *diskriminanten* d af K forstås diskriminanten $D(\omega)$ af en $\mathbb{Z}$-basis for O_K.

Bemærkning 1. For to $\mathbb{Z}$-baser ω og ω' for O_K er $\underline{\omega}' = C\underline{\omega}$, hvor basisskiftmatricen C er invertibel i matrixringen $\mathrm{Mat}_n(\mathbb{Z})$, dvs. $\det C \in \mathbb{Z}$ er invertibel i $\mathbb{Z}$. Følgelig er $\det C = \pm 1$, så at $D(\omega') = (\det C)^2 D(\omega) = D(\omega)$, hvorfor diskriminanten d for K er veldefineret. Da en $\mathbb{Z}$-basis ω for O_K tillige er en $\mathbb{Q}$-basis for K, er $d \neq 0$ ifølge sætning 8 eller sætning 9.

Bemærkning 2. Det vil ofte forekomme, at vi betragter et algebraisk tallegeme K af grad $n = [K:\mathbb{Q}]$ og diskriminant d, og hvori der er valgt et frembringerelement ϑ (jf sætning 15), så at $K = \mathbb{Q}(\vartheta)$, samt en $\mathbb{Z}$-basis $\omega = (\omega_1, \ldots, \omega_n)$ for O_K. Vi betegner da med $\vartheta^{(1)} = \vartheta, \ldots, \vartheta^{(n)}$ de konjugerede til ϑ inden for $\mathbb{C}$, dvs. rødderne i minimalpolynomiet f_ϑ mht $\mathbb{Q}$. Disse er indbyrdes forskellige ifølge sætning 12 (korollar). Lad endvidere K^* være $K(\vartheta^{(1)}, \ldots, \vartheta^{(n)})$, dvs. K^* er spaltningslegemet for f_ϑ inden for $\mathbb{C}$. Det er en vigtig omstændighed, at K^* kun afhænger af K, dvs. er uafhængig af den valgte frembringer ϑ. Dette skyldes, at K^* er det mindste dellegeme af $\mathbb{C}$, som indeholder K og tillige ethvert $\alpha \in \mathbb{C}$, som er konjugeret til et element i K. K^* kaldes *det normale hylster* for K inden for $\mathbb{C}$. Lad $G = \mathrm{Gal}(K^*/\mathbb{Q})$. Da er et element $\sigma \in G$ bestemt ved den permutation af $(\vartheta^{(1)}, \ldots, \vartheta^{(n)})$, som det bevirker. Derfor er G en undergruppe i den symmetriske gruppe S_n, og følgelig gælder

$$n = [K:\mathbb{Q}] \leq [K^*:\mathbb{Q}] = |G| \leq |S_n| = n!.$$

(Jf eksempel 11, hvor $[K:\mathbb{Q}] = 3$ og $|G| = 3!$, og eksempel 12, hvor $[K:\mathbb{Q}] = \varphi(n)$ og $|G| = \varphi(n)$.)

Det bemærkes, at G opererer *transitivt* på $(\vartheta^{(1)}, \ldots, \vartheta^{(n)})$, dvs.

$$I = \{\nu \in \{1, \ldots, n\} \mid \vartheta^{(\nu)} = \sigma(\vartheta) \quad \text{for et} \quad \sigma \in G\}$$

har $|I| = n$. Thi, hvis $|I| < n$, bestemmer

$$f(x) = \prod_{i \in I}(x - \vartheta^{(i)})$$

et egentligt polynomium $f \in \mathbb{Q}[x]$ med ϑ som rod og af grad $\partial f = |I| < n$, hvilket er en modstrid.

Vi betragter

$$(*) \qquad K^{(\nu)} = K(\vartheta^{(\nu)}) \quad \text{for} \quad 1 \leq \nu \leq n.$$

Disse legemer kaldes de med K *konjugerede legemer* inden for $\mathbb{C}$. På grund af transitiviteten af G er begrebet konjugeret legeme uafhængigt af den valgte frembringer ϑ for K. Dette giver nu anledning til at indføre følgende vigtige *invarianter* for K:

r_1 = antallet af reelle legemer blandt (*),

r_2 = antallet af par af komplekst konjugerede (ikke reelle) legemer blandt (*).

Bemærk, at da $f_\vartheta \in \mathbb{Q}[x]$, er r_1 antallet af reelle rødder i f_ϑ og r_2 antallet af par af komplekst konjugerede (ikke reelle) rødder i f_ϑ. Følgelig gælder:

$$r_1 + 2r_2 = n = [K : \mathbb{Q}].$$

Det bemærkes også, at da $\omega = (\omega_1, \ldots, \omega_n)$ er en $\mathbb{Z}$-basis for O_K er $\omega^{(\nu)} = (\omega_1^{(\nu)}, \ldots, \omega_n^{(\nu)})$ en $\mathbb{Z}$-basis for $O_{K^{(\nu)}}$. Dette følger af, at $\sigma(O_K) = O_{K^{(\nu)}}$, når $\sigma \in G$ opfylder $\sigma(\vartheta) = \vartheta^{(\nu)}$.

Sætning 48. *(Stickelberger). For ethvert algebraisk tallegeme K er diskriminanten $d \equiv 0, 1 \pmod 4$.*

Bevis. Det bemærkes først, at det følger af sætning 7, at ethvert $\alpha \in O_K$ har $S(\alpha) = S_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ og $N(\alpha) = N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Idet $\omega = (\omega_1, \ldots, \omega_n)$ er en vilkårlig $\mathbb{Z}$-basis for O_K, er specielt hvert ω_r og dermed hvert $\omega_r\omega_s$ i O_K, og derfor er

$$d = \det(S(\omega_r\omega_s)) \in \mathbb{Z}.$$

For at indse kongruensen (som skyldes Stickelberger) benyttes en variant af en tidligere omskrivning af diskriminanten

$$\begin{aligned} d =& \det(S(\omega_r\omega_s) = (\det(\omega_r^{(\nu)}))^2 \\ =& \left(\sum_{(\nu_1,\dots,\nu_n) \text{ lige}} \omega_1^{(\nu_1)} \cdots \omega_n^{(\nu_n)} - \sum_{(\nu_1,\dots,\nu_n) \text{ ulige}} \omega_1^{(\nu_1)} \cdots \omega_n^{(\nu_n)} \right)^2 \\ =& (A-B)^2 \\ =& (A+B)^2 - 4AB. \end{aligned}$$

Det fremgår af ovenstående udtryk, at A og B og dermed $A+B$ og AB er hele algebraiske tal (dvs. hele mht $\mathbb{Z}$).

Lad nu $K = \mathbb{Q}(\vartheta)$, og lad $K^* = \mathbb{Q}(\vartheta^{(1)}, \dots, \vartheta^{(n)})$, hvor $\vartheta^{(1)} = \vartheta, \dots, \vartheta^{(n)}$ er de konjugerede til ϑ. Da er K^* en galois udvidelse af $\mathbb{Q}$. Ethvert $\sigma \in \mathrm{Gal}(K^*/\mathbb{Q})$ giver da anledning til en permutation af $(\vartheta^{(1)}, \dots, \vartheta^{(n)})$, og dermed til den samme permutation af $(\omega_r^{(1)}, \dots, \omega_r^{(n)})$ for hvert $r \in \{1, \dots, n\}$, og derfor er enten $(\sigma(A), \sigma(B)) = (A, B)$ (hvis σ er lige) eller $(\sigma(A), \sigma(B)) = (B, A)$ (hvis σ er ulige). Følgelig er

$$\sigma(A+B) = A+B \quad \text{og} \quad \sigma(AB) = AB \quad \text{for} \quad \sigma \in \mathrm{Gal}(K^*/\mathbb{Q}).$$

Af Galoisteoriens hovedsætning følger da, at $A+B,\ AB \in \mathbb{Q}$. Da $A+B,\ AB$ tillige var hele mht. $\mathbb{Z}$, og $\mathbb{Z}$ er helt afsluttet, er $A+B,\ AB \in \mathbb{Z}$. Heraf fås nu

$$d = (A+B)^2 - 4AB \equiv (A+B)^2 \equiv 0, 1 \pmod 4,$$

hvilket er den ønskede kongruens. □

Sætning 49. *Ethvert kvadratisk tallegeme er af formen $K = \mathbb{Q}(\sqrt{D})$, hvor $D \in \mathbb{Z} \setminus \{0, 1\}$ og er kvadratfrit. Den tilhørende ring O_K af hele tal er givet ved*

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{D} & \textit{for} \quad D \equiv 2, 3 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2} & \textit{for} \quad D \equiv 1 \pmod 4 \end{cases}$$

Diskriminanten for $K = \mathbb{Q}(\sqrt{D})$ er givet ved

$$d = \begin{cases} 4D & \textit{for} \quad D \equiv 2, 3 \pmod 4 \\ D & \textit{for} \quad D \equiv 1 \pmod 4 \end{cases}$$

Bevis. Såfremt $[K:\mathbb{Q}]=2$, er $K=\mathbb{Q}(\vartheta)$, hvor

$$a_2\vartheta^2+a_1\vartheta+a_0=0 \quad \text{med} \quad a_\nu\in\mathbb{Z} \quad \text{og} \quad a_2\neq 0,$$

dvs.

$$\vartheta=\frac{1}{2a_2}\left(-a_1\pm\sqrt{a_1^2-4a_2a_0}\right).$$

Altså er nødvendigvis $K=\mathbb{Q}(\sqrt{D})$, hvor $D=a_1^2-4a_2a_0$. Det er klart, at vi kan se bort fra tilfældene $D=0,1$ og at vi uden indskrænkning kan antage, at D er kvadratfrit.

Betragt omvendt et sådant D. Det er klart, at $\sqrt{D}$ har grad ≤ 2 over $\mathbb{Q}$. Antag (indirekte), at der findes et D, for hvilket graden af $\sqrt{D}$ er 1. Da er $\sqrt{D}=p/q$, hvor $p,q\in\mathbb{Z}\setminus\{0\}$. Altså $p^2=Dq^2$. Da $\mathbb{Z}$ er UFD, og D er kvadratfrit, følger heraf $D=1$, hvilket er en modstrid.

For at bestemme O_K bemærkes, at $1,\sqrt{D}\in O_K$ for alle D, idet de tilhørende minimalpolynomier $x-1$ og x^2-D begge tilhører $\mathbb{Z}[x]$. Når $D\equiv 1 \pmod 4$ er endvidere $\frac{1}{2}(1+\sqrt{D})\in O_K$, idet minimalpolynomiet $x^2-x+\frac{1}{4}(1-D)\in\mathbb{Z}[x]$. Vi skelner nu mellem to tilfælde:

For $D\equiv 2,3 \pmod 4$ er $\mathbb{Z}+\mathbb{Z}\sqrt{D}\subseteq O_K$, og

$$D(1,\sqrt{D})=\det\begin{pmatrix} S(1) & S(\sqrt{D}) \\ S(\sqrt{D}) & S(D)\end{pmatrix}=\det\begin{pmatrix}2 & 0\\ 0 & 2D\end{pmatrix}=4D.$$

Idet $\omega=(\omega_1,\omega_2)$ er en $\mathbb{Z}$-basis for O_K gælder

$$\begin{pmatrix}1\\ \sqrt{D}\end{pmatrix}=\begin{pmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix},$$

hvor $c_{rs}\in\mathbb{Z}$. Følgelig er

$$4D=D(1,\sqrt{D})=(\det(c_{rs}))^2 d.$$

Da D er kvadratfrit, er derfor $(\det(c_{rs}))^2=1,4$. Men hvis $(\det(c_{rs}))^2=4$, er $d=D\equiv 2,3 \pmod 4$ i strid med Stickelbergers sætning. Altså er $(\det(c_{rs}))=\pm 1$, dvs. $(1,\sqrt{D})$ er en $\mathbb{Z}$-basis for O_K, og $d=4D$.

For $D\equiv 1 \pmod 4$ er $\mathbb{Z}+\mathbb{Z}\frac{1}{2}(1+\sqrt{D})\subseteq O_K$, og

$$D(1,\tfrac{1+\sqrt{D}}{2})=\det\begin{pmatrix} S(1) & S(\frac{1+\sqrt{D}}{2}) \\ S(\frac{1+\sqrt{D}}{2}) & S(\frac{1+D+2\sqrt{D}}{4})\end{pmatrix}=\det\begin{pmatrix}2 & 1\\ 1 & \frac{1+D}{2}\end{pmatrix}=D.$$

Da D er kvadratfrit viser argumentet ovenfor, at $(1, \frac{1}{2}(1+\sqrt{D}))$ er en $\mathbb{Z}$-basis for O_K, og at $d = D$. □

I det følgende betragtes pånyen en vilkårlig klassisk Dedekindring O_K, hvor $[K : \mathbb{Q}] = n \in \mathbb{N}$. Vi indfører nogle fundamentale begreber og viser en række vigtige sætninger. Derefter illustreres teorien for de kvadratiske tallegemer.

Sætning 50. *Lad $\mathfrak{a} \neq (0)$ være et helt ideal i O_K. Da er $|O_K/\mathfrak{a}| < \infty$.*

Bevis. Vælg $\alpha \in \mathfrak{a} \setminus \{0\}$. Da er $N_{K/\mathbb{Q}}(\alpha) = \alpha\alpha'$, hvor

$$\alpha' = N_{K/\mathbb{Q}}(\alpha)/\alpha = \alpha^{(2)} \cdots \alpha^{(n)}$$

er i K og helt algebraisk, altså $\alpha' \in O_K$. Derfor er $0 \neq N_{K/\mathbb{Q}}(\alpha) \in \mathfrak{a} \cap \mathbb{Z}$, dvs. der findes et element $a \in \mathfrak{a} \cap \mathbb{N}$. Lad nu $(\omega_1, \ldots, \omega_n)$ være en $\mathbb{Z}$-basis for O_K, og lad

$$\beta = \sum_1^n m_i\omega_i, \quad \text{hvor} \quad m_i \in \mathbb{Z},$$

være et vilkårligt element i O_K. Skriv

$$m_i = aq_i + r_i, \quad \text{hvor} \quad q_i,\ r_i \in \mathbb{Z} \quad \text{og} \quad 0 \leq r_i < a.$$

Da er

$$\beta = \sum_1^n (aq_i + r_i)\omega_i = \left(\sum_1^n q_i\omega_i\right) a + \sum_1^n r_i\omega_i \equiv \sum_1^n r_i\omega_i \pmod{\mathfrak{a}},$$

hvilket viser, at $|O_K/\mathfrak{a}| \leq a^n$. □

Definition. Lad $\mathfrak{a} \neq (0)$ være et helt ideal i O_K. Da kaldes $|O_K/\mathfrak{a}| \in \mathbb{N}$ *normen* af $\mathfrak{a}$. Den betegnes $N(\mathfrak{a})$.

Sætning 51. *Lad $\mathfrak{a}$ og $\mathfrak{b}$ være fra (0) forskellige hele idealer i O_K. Da gælder*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Bevis. Lad

$$\mathfrak{a} = {\mathfrak{p}_1}^{n_1} \cdots {\mathfrak{p}_r}^{n_r},$$

hvor $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ er indbyrdes forskellige primidealer og $n_1, \ldots, n_r \in \mathbb{N}$. Det fremgår af sætning 42, at

$$N(\mathfrak{a}) = N({\mathfrak{p}_1}^{n_1}) \cdots N({\mathfrak{p}_r}^{n_r}),$$

og af sætning 45, at

$$N({\mathfrak{p}_i}^{n_i}) = N(\mathfrak{p}_i)^{n_i},$$

således at

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{n_1} \cdots N(\mathfrak{p}_r)^{n_r}.$$

Heraf følger resultatet umiddelbart. □

Sætning 52. *(Elementardivisorsætningen.) Lad G være en fri abelsk gruppe af rang $n \in \mathbb{N}$, og lad H være en undergruppe i G. Da er H en fri abelsk gruppe af rang $m \leq n$, og der findes en basis $(\omega_1, \ldots, \omega_n)$ for G og en basis $(\varphi_1, \ldots, \varphi_m)$ for H, så at*

$$\varphi_j = \epsilon_j \omega_j \quad \textit{hvor} \quad \epsilon_j \in \mathbb{N} \quad \textit{for} \quad 1 \leq j \leq m,$$

og hvor yderligere

$$\epsilon_j \,|\, \epsilon_{j+1} \quad \textit{for} \quad 1 \leq j < m.$$

Bevis. At H er en fri abelsk gruppe af rang $m \leq n$ er tidligere vist (jf sætning 22). Lad ω' og φ' være vilkårlige baser for G og H. Da er

$$\begin{pmatrix} \varphi'_1 \\ \vdots \\ \varphi'_m \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix} = A \begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix},$$

hvor $a_{rs} \in \mathbb{Z}$. Ved et samtidigt basisskift for G og H erstattes matricen A af MAN, hvor M og N er basisskiftmatricer for G og H. Ifølge et tidligere ræsonnement (jf bemærkningen til definitionen af diskriminant for K) er M og N derfor heltalsmatricer af størrelse henholdsvis $m \times m$ og $n \times n$ og af determinant ± 1.

Specielt kan M vælges som produkt af *elementære* heltalsmatricer af størrelse $m \times m$, der enkeltvis bevirker, at to rækker ombyttes eller et heltalsmultiplum af én række adderes til en anden række. Tilsvarende kan N vælges som produkt af heltalsmatricer af størrelse $n \times n$, der enkeltvis bevirker at to søjler ombyttes eller et heltalsmultiplum af én søjle adderes til en anden søjle.

Herved kan opnås, at a_{11} erstattes af $\gcd(a_{rs} \mid 1 \leq r \leq m, 1 \leq s \leq n)$, hvorefter de øvrige elementer i første række og første søjle kan erstattes af 0'er. Derpå opereres på tilsvarende måde på delmatricen, hvor første række og første søjle tænkes slettet. Når denne diagonaliseringsproces er tilendebragt, er A blevet erstattet af en matrix af den ønskede diagonalform og med de angivne delelighedsbetingelser. □

Sætning 53. *Lad $\mathfrak{a} \neq (0)$ være et helt ideal i O_K, og lad $\mathfrak{a}$ og O_K have $\mathbb{Z}$-baser φ og ω. Da gælder*

$$D(\varphi) = N(\mathfrak{a})^2 d.$$

Hvis specielt $\mathfrak{a} = (\alpha) = \alpha O_K$ med $\alpha \in O_K$, gælder

$$N(\mathfrak{a}) = |N(\alpha)|.$$

Bevis. Ved første del af sætningen kan det uden indskrænkning antages, at baserne er valgt som i elementardivisorsætningen (med $m = n$). Da er

$$D(\varphi) = (\det(\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n)))^2 D(\omega) = (\epsilon_1 \cdots \epsilon_n)^2 d.$$

På den anden side følger det, at

$$N(\mathfrak{a}) = |O_K/\mathfrak{a}| = \epsilon_1 \cdots \epsilon_n,$$

idet restklasserne i $O_K/\mathfrak{a}$ præcis repræsenteres ved

$$\{r_1\omega_1 + \cdots + r_n\omega_n \mid 0 \leq r_i < \epsilon_i \quad \text{for} \quad 1 \leq i \leq n\}.$$

Ved anden del af sætningen fås benyttes en vilkårlig $\mathbb{Z}$-basis ω for O_K og for $\mathfrak{a} = (\alpha)$ $\mathbb{Z}$-basen $(\varphi) = \alpha(\omega) = A(\omega)$, hvor A er en $n \times n$-matrix over $\mathbb{Z}$. Da er

$$N(\mathfrak{a})^2 d = D(\varphi) = (\det A)^2 d = N(\alpha)^2 d$$

ifølge første del af sætningen samt transformationsformlen for diskriminanter og definitionen af $N(\alpha)$ i kapitel 1. Dette giver det ønskede. □

Sætning 54. *Lad $\mathfrak{p} \neq (0)$ være et primideal i O_K. Da findes præcist et primtal p, så at $\mathfrak{p} \mid pO_K$. For dette gælder $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Endvidere er*

$$N(\mathfrak{p}) = p^f, \quad \textit{hvor} \quad 1 \leq f \leq n = [K : \mathbb{Q}].$$

Bevis. Antag (indirekte), at $\mathfrak{p} \mid p_1 O_K$ og $\mathfrak{p} \mid p_2 O_K$, hvor p_1 og p_2 er forskellige primtal. Da gælder også $\mathfrak{p} \mid p_1 O_K + p_2 O_K = O_K$, hvilket er en modstrid. Dette viser entydigheden af p.

Da $\mathfrak{p}$ er et maksimalt ideal, er $O_K/\mathfrak{p}$ et legeme, som ifølge sætning 50 er endeligt. Altså er (jf eksempel 13) $O_K/\mathfrak{p} \simeq \mathbb{F}_{p^f}$, hvor p er et primtal og $f \in \mathbb{N}$. Da karakteristikken af $O_K/\mathfrak{p}$ er p, vil $p \in O_K$ ved den naturlige homomorfi $O_K \to O_K/\mathfrak{p}$ blive afbildet i $\overline{0}$, dvs. $p \in \mathfrak{p}$. Dette kan også udtrykkes ved $pO_k \subseteq \mathfrak{p}$ eller $\mathfrak{p} \,|\, pO_K$. Dette viser eksistensen af p.

Da $pO_K \subseteq \mathfrak{p}$, er

$$p^f = N(\mathfrak{p}) = |O_K/\mathfrak{p}| \leq |O_K/(pO_K)| = N(pO_K) = |N(p)| = p^n.$$

Heraf følger uligheden $f \leq n$. □

Definition. Primtallet p kaldes det til $\mathfrak{p} \neq (0)$ *hørende* primtal, og f kaldes *graden* af $\mathfrak{p}$.

Sætning 55. *Lad p være et primtal, og lad*

$$(p) = pO_K = {\mathfrak{p}_1}^{e_1} \cdots {\mathfrak{p}_r}^{e_r}$$

være primidealopløsningen af (p). Da er

$$\sum_{i=1}^{r} e_i f_i = n = [K : \mathbb{Q}],$$

hvor f_i er graden af $\mathfrak{p}_i$.

Bevis. Udregning af normer giver

$$p^n = N((p)) = N({\mathfrak{p}_1}^{e_1} \cdots {\mathfrak{p}_r}^{e_r}) = \prod_{i=1}^{r} p^{e_i f_i} = p^{\sum_{i=1}^{r} e_i f_i},$$

hvilket viser den ønskede formel. □

Definition. Eksponenten e_i for $\mathfrak{p}_i$ i primidealopløsningen af $(p) = pO_K$ kaldes *forgreningsindex* for $\mathfrak{p}_i$.

Sætning 56. *Lad $\mathfrak{a} \neq (0)$ være et helt ideal i O_K, og lad $\Phi(\mathfrak{a})$ betegne antallet af primiske restklasser modulo $\mathfrak{a}$. Da gælder*

$$\Phi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p} \,|\, \mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right).$$

Bevis. For $\mathfrak{a} = \mathfrak{p}^m, m \in \mathbb{N}$, fremgår det af sætning 45, at

$$\Phi(\mathfrak{a}) = (N(\mathfrak{p}) - 1)N(\mathfrak{p})^{m-1} = N(\mathfrak{p})^m \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

dvs. formlen er vist i dette tilfælde. For $\mathfrak{a} = {\mathfrak{p}_1}^{m_1} \cdots {\mathfrak{p}_r}^{m_r}$ følger heraf og af sætningerne 44 og 51, at

$$\begin{aligned}\Phi(\mathfrak{a}) =& \Phi({\mathfrak{p}_1}^{m_1}) \cdots \Phi({\mathfrak{p}_r}^{m_r}) \\ =& N(\mathfrak{p}_1)^{m_1} \left(1 - \frac{1}{N(\mathfrak{p}_1)}\right) \cdots N(\mathfrak{p}_r)^{m_r} \left(1 - \frac{1}{N(\mathfrak{p}_r)}\right) \\ =& N(\mathfrak{a}) \prod_{\mathfrak{p} \mid \mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right).\end{aligned}$$

Dette viser den angivne formel. □

Sætning 57. *For ethvert helt ideal $\mathfrak{a} \neq (0)$ gælder*

$$\sum_{\mathfrak{b} \mid \mathfrak{a}} \Phi(\mathfrak{b}) = N(\mathfrak{a}).$$

Bevis. Sæt

$$F(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} \Phi(\mathfrak{b}),$$

og antag, at

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2, \quad \text{hvor} \quad \mathfrak{a}_1 + \mathfrak{a}_2 = O_K.$$

Da er

$$\begin{aligned}F(\mathfrak{a}) =& \sum_{\mathfrak{b} \mid \mathfrak{a}} \Phi(\mathfrak{b}) = \sum_{\mathfrak{b}_1 \mid \mathfrak{a}_1 \wedge \mathfrak{b}_2 \mid \mathfrak{a}_2} \Phi(\mathfrak{b}_1\mathfrak{b}_2) \\ =& \sum_{\mathfrak{b}_1 \mid \mathfrak{a}_1 \wedge \mathfrak{b}_2 \mid \mathfrak{a}_2} \Phi(\mathfrak{b}_1)\Phi(\mathfrak{b}_2) \\ =& \sum_{\mathfrak{b}_1 \mid \mathfrak{a}_1} \Phi(\mathfrak{b}_1) \sum_{\mathfrak{b}_2 \mid \mathfrak{a}_2} \Phi(\mathfrak{b}_2) \\ =& F(\mathfrak{a}_1)F(\mathfrak{a}_2).\end{aligned}$$

Dette viser, at F er *multiplikativ*. Da også N er multiplikativ (endda *stærkt*), er det herefter tilstrækkeligt at vise sætningen for $\mathfrak{a} = \mathfrak{p}^m$. Her finder vi

$$\begin{aligned} F(\mathfrak{p}^m) =& \Phi((1)) + \Phi(\mathfrak{p}) + \cdots + \Phi(\mathfrak{p}^m) \\ =& 1 + (N(\mathfrak{p}) - 1) + \cdots + (N(\mathfrak{p}^m) - N(\mathfrak{p}^{m-1})) \\ =& N(\mathfrak{p}^m), \end{aligned}$$

hvormed sætningen er vist. □

Bemærkning. For $K = \mathbb{Q}$ er $\Phi((n)) = \varphi(n)$ for $n \in \mathbb{N}$, hvor φ er Eulers funktion (jf eksempel 4). Formlerne i sætningerne 56 og 57 generaliserer derfor de velkendte formler

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right),$$

og

$$\sum_{m \mid n} \varphi(m) = n.$$

Primidealer i kvadratiske tallegemer. Vi indleder med nogle velkendte begreber og resultater.

Definition. Lad p være et ulige primtal. Da defineres *Legendre symbolet*

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{1, -1, 0\}$$

ved

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{hvis} \quad \text{hvis } x^2 \equiv a \not\equiv 0 \pmod{p} \text{ har en løsning } x \in \mathbb{Z} \\ -1 & \text{hvis} \quad x^2 \equiv a \pmod{p} \text{ ikke har nogen løsning } x \in \mathbb{Z} \\ 0 & \text{hvis} \quad a \equiv 0 \pmod{p} \end{cases}$$

Man kalder $a \in \mathbb{Z}$ *kvadratisk rest* $\pmod{p}$, hvis $(\frac{a}{p}) = 1$, og *kvadratisk ikke rest* $\pmod{p}$, hvis $(\frac{a}{p}) = -1$.

Vi anfører følgende fundamentale sætninger uden bevis:

Sætning 58. *(Eulers kriterium). For ethvert ulige primtal p og ethvert $a \in \mathbb{Z}$ er*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Korollar. *For ethvert ulige primtal p er Legendre symbolet (stærkt) multiplikativt:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \textit{for} \quad a, b \in \mathbb{Z}.$$

Sætning 59. *(Reciprocitetssætningen). Idet p og q er forskellige ulige primtal gælder:*

(i) $$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)} = \begin{cases} 1, & \textit{hvis} \quad p \equiv 1 \pmod 4 \\ -1, & \textit{hvis} \quad p \equiv -1 \pmod 4, \end{cases}$$

(ii) $$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)} = \begin{cases} 1, & \textit{hvis} \quad p \equiv \pm 1 \pmod 8 \\ -1, & \textit{hvis} \quad p \equiv \pm 3 \pmod 8, \end{cases}$$

(iii) $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}.$$

Bemærkning. Resultaterne (i) og (ii) kaldes henholdvis 1. og 2. *supplement* til reciprocitetssætningen, medens (iii) er selve *reciprocitetssætningen*. Det bemærkes, at (i) følger direkte af Eulers kriterium. Den øvrige del af sætningen er først vist af Gauss i *Disquisitiones Arithmeticae*, 1801.

Sætning 60. *Lad K være et kvadratisk tallegeme med diskriminant d, og lad p være et ulige primtal. Da har $(p) = pO_K$ følgende dekomposition i primidealer:*

(i) $(p) = \mathfrak{p}_1\mathfrak{p}_2$ *med* $\mathfrak{p}_1 \neq \mathfrak{p}_2$ *((p) er opløst)* $\Leftrightarrow (\frac{d}{p}) = 1$;

(ii) *(p) er primideal i O_K ((p) er træg)* $\Leftrightarrow (\frac{d}{p}) = -1$;

(iii) $(p) = \mathfrak{p}^2$ *((p) er forgrenet)* $\Leftrightarrow (\frac{d}{p}) = 0$.

Bevis. Vi viser først implikationerne " $\Rightarrow$ ".

(i) (p) opløst $\Rightarrow (\frac{d}{p}) = 1$. Med betegnelserne fra sætning 55 er i dette tilfælde: $r = 2$, $e_i = f_i = 1$ for $1 \leq i \leq 2$, dvs. $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$. Da $\mathfrak{p}_i \,|\, pO_K$ vil $\mathfrak{p}_i \nmid mO_K$ for $1 \leq m < p$ ifølge sætning 54. Dette viser, at elementerne i $\{0, 1, \ldots, p-1\}$ repræsenterer forskellige restklasser modulo $\mathfrak{p}_i$, og eftersom

$$|O_K/\mathfrak{p}_i| = N(\mathfrak{p}_i) = p = |\{0, 1, \ldots, p-1\}|,$$

er $\{0, 1, \ldots, p-1\}$ et fuldstændigt repræsentantsystem for $O_K/\mathfrak{p}_i$ for $1 \leq i \leq 2$. Lad $K = \mathbb{Q}(\sqrt{D})$, hvor $D = d$ eller $D = d/4$ har den i sætning 49 angivne betydning. Da $\sqrt{D} \in O_K$, findes et $s \in \{0, 1, \ldots, p-1\}$, så at

$$\sqrt{D} \equiv s \pmod{\mathfrak{p}_1} \Rightarrow D \equiv s^2 \pmod{\mathfrak{p}_1} \Rightarrow D \equiv s^2 \pmod{p},$$

og derfor er $(\frac{d}{p}) = (\frac{D}{p}) \in \{0, 1\}$. Såfremt $(\frac{d}{p}) = 0$, dvs. $D \equiv 0 \pmod{p}$, er

$$(\sqrt{D})^2 \equiv 0 \pmod{\mathfrak{p}_i} \Rightarrow \sqrt{D} \equiv 0 \pmod{\mathfrak{p}_i} \Rightarrow \sqrt{D} \equiv 0 \pmod{\mathfrak{p}_1\mathfrak{p}_2},$$

dvs. $\sqrt{D}/p \in O_K$. Da $p > 2$, strider dette imidlertid mod beskrivelsen af O_K i sætning 49, og vi har dermed vist, at $(\frac{d}{p}) = 1$.

(ii) (p) træg $\Rightarrow (\frac{d}{p}) = -1$. Antag (indirekte), at $(\frac{d}{p}) = (\frac{D}{p}) \in \{0, 1\}$. Da findes et $s \in \mathbb{Z}$, så at

$$D \equiv s^2 \pmod{p} \Rightarrow (\sqrt{D} + s)(\sqrt{D} - s) \equiv 0 \pmod{(p)}.$$

Da (p) er et primideal i O_K, er derfor enten $(\sqrt{D} + s)/p \in O_K$ eller $(\sqrt{D} - s)/p \in O_K$. Da $p > 2$, strider dette imidlertid mod beskrivelsen af O_K i sætning 49, og vi har dermed vist, at $(\frac{d}{p}) = -1$.

(iii) (p) forgrenet $\Rightarrow (\frac{d}{p}) = 0$. Med betegnelserne fra sætning 55 er i dette tilfælde: $r = 1$, $e = 2$, $f = 1$, dvs. $N(\mathfrak{p}) = p$. Som i tilfælde *(i)* er $\{0, 1, \ldots, p-1\}$ et fuldstændigt repræsentantsystem for $O_K/\mathfrak{p}$. Lad $K = \mathbb{Q}(\sqrt{D})$, hvor $D = d$ eller $D = d/4$ har den i sætning 49 angivne betydning. Da $\sqrt{D} \in O_K$, findes et $s \in \{0, 1, \ldots, p-1\}$, så at

$$\sqrt{D} \equiv s \pmod{\mathfrak{p}} \Rightarrow D \equiv s^2 \pmod{\mathfrak{p}} \Rightarrow D \equiv s^2 \pmod{p},$$

og da $(p) = \mathfrak{p}^2$, er derfor

$$(*) \qquad (\sqrt{D} + s)(\sqrt{D} - s) \equiv 0 \pmod{\mathfrak{p}^2}.$$

Da $p > 2$, gælder $p \nmid (\sqrt{D} \pm s)$, og af (*) følger derfor, at

$$\sqrt{D} + s \equiv \sqrt{D} - s \equiv 0 \pmod{\mathfrak{p}} \Rightarrow 2\sqrt{D} \equiv 0 \pmod{\mathfrak{p}}.$$

Dette viser, at $4D \equiv 0 \pmod{p}$, hvoraf

$$\left(\frac{d}{p}\right) = \left(\frac{D}{p}\right) = \left(\frac{4D}{p}\right) = 0.$$

Eftersom $[K:\mathbb{Q}] = 2 = \sum_{i=1}^{r} e_i f_i$ kun har de tre løsninger, der er omtalt under (i), (ii) og (iii), vil de tre tilfælde: (p) opløst, træg og forgrenet, udtømme alle muligheder for dekomposition af (p). Derfor følger implikationerne " $\Leftarrow$ " for (i), (ii) og (iii) automatisk. □

Sætning 61. *Lad K være et kvadratisk tallegeme med diskriminant d. Da har $(2) = 2O_K$ følgende dekomposition i primidealer:*

(i) $(2) = \mathfrak{p}_1\mathfrak{p}_2$ *med* $\mathfrak{p}_1 \neq \mathfrak{p}_2$ *((2) er opløst)* $\Leftrightarrow d \equiv 1 \pmod 8$*;*

(ii) *(2) er primideal i O_K ((2) er træg)* $\Leftrightarrow d \equiv 5 \pmod 8$*;*

(iii) $(2) = \mathfrak{p}^2$ *((2) er forgrenet)* $\Leftrightarrow d \equiv 0 \pmod 4$*.*

Bevis. Vi viser først implikationerne " $\Rightarrow$ ".

(i) (2) opløst $\Rightarrow d \equiv 1 \pmod 8$. Med betegnelserne fra sætning 55 er i dette tilfælde: $r = 2$, $e_i = f_i = 1$ for $1 \leq i \leq 2$, dvs. $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 2$. Det er derfor klart, at $\{0,1\}$ er et fuldstændigt repræsentantsystem for $O_K/\mathfrak{p}_i$ for $1 \leq i \leq 2$. Lad $K = \mathbb{Q}(\sqrt{D})$, hvor $D = d$ eller $D = d/4$ har den i sætning 49 angivne betydning. Da $\sqrt{D} \in O_K$, findes $s_i \in \{0,1\}$, så at

$$\sqrt{D} \equiv s_i \pmod{\mathfrak{p}_i} \Rightarrow D \equiv s_i^2 \pmod{\mathfrak{p}_i} \Rightarrow D \equiv s_i^2 \pmod 2,$$

hvorfor $s_1 = s_2 = s$. Derfor er

$$\sqrt{D} \equiv s \pmod{\mathfrak{p}_i} \text{ for } 1 \leq i \leq 2 \Rightarrow \sqrt{D} \equiv s \pmod{(2)}.$$

Heraf fås $s = 1$, da $\frac{1}{2}\sqrt{D} \notin O_K$ ifølge sætning 49. Altså er $\frac{1}{2}(\sqrt{D}-1) \in O_K$, hvorfor $d = D \equiv 1 \pmod 4$. Betragt dernæst $\frac{1}{2}(1+\sqrt{D}) \in O_K$. Som ovenfor findes et $s \in \{0,1\}$, så at

$$\begin{aligned} \tfrac{1}{2}(1+\sqrt{D}) \equiv s \pmod{\mathfrak{p}_1} &\Rightarrow 1+\sqrt{D} \equiv 2s \pmod{2\mathfrak{p}_1} \\ &\Rightarrow \sqrt{D} \equiv 2s-1 \pmod{2\mathfrak{p}_1}. \end{aligned}$$

Endvidere har vi

$$\sqrt{D} \equiv 1 \equiv -(2s-1) \pmod{(2)}.$$

Tilsammen fås

$$D - (2s-1)^2 = (\sqrt{D} - (2s-1))(\sqrt{D} + (2s-1)) \equiv 0 \pmod{4\mathfrak{p}_1},$$

hvoraf $D \equiv (2s-1)^2 = 4s(s-1)+1 \equiv 1 \pmod 8$.

(ii) (2) træg $\Rightarrow d \equiv 5 \pmod 8$. Beviset føres indirekte, idet vi ifølge sætning 49 da skal udelukke tilfældene 1) $d = 4D \equiv 0 \pmod 4$ og 2) $d = D \equiv 1 \pmod 8$.

I tilfælde 1) er $D \equiv 2, 3 \pmod 4$. Hvis $D \equiv 2 \pmod 4$ er

$$D \equiv 0 \pmod 2 \Rightarrow (\sqrt{D})^2 \equiv 0 \pmod{(2)},$$

altså $\sqrt{D} \equiv 0 \pmod{(2)}$, da (2) er et primideal i O_K. Men dette er en modstrid, da

$$\tfrac{1}{2}\sqrt{D} \notin O_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}.$$

Hvis $D \equiv 3 \pmod 4$ er

$$1 + D \equiv 0 \pmod 2 \Rightarrow (1+\sqrt{D})^2 = 1 + D + 2\sqrt{D} \equiv 0 \pmod{(2)},$$

altså $1 + \sqrt{D} \equiv 0 \pmod{(2)}$, da (2) er et primideal i O_K. Men dette er en modstrid, da

$$\tfrac{1}{2}(1+\sqrt{D}) \notin O_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}.$$

I tilfælde 2) er $D \equiv 1 \pmod 8$. Da er

$$(1+\sqrt{D})(1-\sqrt{D}) = 1 - D \equiv 0 \pmod{(2)^3},$$

hvorfor

$$1 + \sqrt{D} \equiv 0 \pmod{(2)^2} \quad \text{eller} \quad 1 - \sqrt{D} \equiv 0 \pmod{(2)^2}.$$

Men dette er en modstrid, da

$$\tfrac{1}{4}(1 \pm \sqrt{D}) \notin O_K = \mathbb{Z} + \mathbb{Z}\tfrac{1}{2}(1+\sqrt{D}).$$

(iii) (2) forgrenet $\Rightarrow d \equiv 0 \pmod 4$. Med betegnelserne fra sætning 55 er i dette tilfælde: $r = 1$, $e = 2$, $f = 1$, dvs. $N(\mathfrak{p}) = 2$. Som i tilfælde *(i)* er det klart, at $\{0, 1\}$ et fuldstændigt repræsentantsystem for $O_K/\mathfrak{p}$. Antag (indirekte), at $d \not\equiv 0 \pmod 4$. Ifølge sætning 49 er da $d = D \equiv 1 \pmod 4$, og $O_K = \mathbb{Z} + \mathbb{Z}\frac{1}{2}(1+\sqrt{D})$. Specielt er $\frac{1}{2}(1+\sqrt{D}) \in O_K$, og der findes derfor et $s \in \{0, 1\}$, så at

(*) $$\tfrac{1}{2}(1+\sqrt{D}) \equiv s \pmod{\mathfrak{p}}.$$

Lad $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ være $\mathbb{Q}$-automorfien givet ved $\sigma(a+b\sqrt{D}) = a - b\sqrt{D}$ for $a, b \in \mathbb{Q}$. Det er klart, at σ afbilder et helt ideal på et helt ideal og et primideal $\neq (0)$ på et primideal $\neq (0)$, samt at $N(\sigma(\mathfrak{a})) = N(\mathfrak{a})$, når $\mathfrak{a} \neq (0)$ er et helt ideal. Da der kun findes ét primideal med norm 2, nemlig $\mathfrak{p}$, gælder derfor $\sigma(\mathfrak{p}) = \mathfrak{p}$. Anvendes σ på (*), fås følgelig

$$(**) \qquad \tfrac{1}{2}(1-\sqrt{D}) \equiv s \pmod{\mathfrak{p}}.$$

Af (*) og (**) følger nu

$$1 = \tfrac{1}{2}(1+\sqrt{D}) + \tfrac{1}{2}(1-\sqrt{D}) \equiv 2s \equiv 0 \pmod{\mathfrak{p}},$$

hvilket er en modstrid.

Eftersom $[K:\mathbb{Q}] = 2 = \sum_{i=1}^{r} e_i f_i$ kun har de tre løsninger, der er omtalt under (i), (ii) og (iii), vil de tre tilfælde: (2) opløst, træg og forgrenet, udtømme alle muligheder for dekomposition af (2). Derfor følger implikationerne " $\Leftarrow$ " for (i), (ii) og (iii) automatisk. □

Definition. For $a \equiv 0, 1 \pmod 4$ sættes:

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{for} \quad a \equiv 1 \pmod 8 \\ -1 & \text{for} \quad a \equiv 5 \pmod 8 \\ 0 & \text{for} \quad a \equiv 0 \pmod 4. \end{cases}$$

Med denne definition kan sætningerne 60 og 61 nu sammenfattes til:

Sætning 62. *Lad $K = \mathbb{Q}(\sqrt{D})$ være et kvadratisk tallegeme med diskriminant d, og lad p være et primtal. Da har $(p) = pO_K$ følgende dekomposition i primidealer:*

(i) $(p) = \mathfrak{p}_1\mathfrak{p}_2$ *med* $\mathfrak{p}_1 \neq \mathfrak{p}_2$ *((p) er opløst)* $\Leftrightarrow (\frac{d}{p}) = 1$;

(ii) *(p) er primideal i O_K ((p) er træg)* $\Leftrightarrow (\frac{d}{p}) = -1$;

(iii) $(p) = \mathfrak{p}^2$ *((p) er forgrenet)* $\Leftrightarrow (\frac{d}{p}) = 0$.

Øvelse. Heri præciseres primidealdekompositionen i sætning 62. Vis, at der for et ulige primtal p gælder:

$$(p) = \begin{cases} (p, s+\sqrt{D})(p, s-\sqrt{D}), & \text{når} \quad D \equiv s^2 \not\equiv 0 \pmod p \\ (p, \sqrt{D})^2, & \text{når} \quad D \equiv 0 \pmod p. \end{cases}$$

Vis, at der for primtallet 2 gælder:

$$(2) = \begin{cases} (2, \frac{1}{2}(1+\sqrt{D}))(2, \frac{1}{2}(1-\sqrt{D})), & \text{når} \quad d = D \equiv 1 \pmod 8 \\ (2, 1+\sqrt{D})^2, & \text{når} \quad \frac{d}{4} = D \equiv 3 \pmod 4 \\ (2, \sqrt{D})^2, & \text{når} \quad \frac{d}{4} = D \equiv 2 \pmod 4. \end{cases}$$

Eksempel 16. For tallegemet $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ (det *gaussiske* tallegeme) er $D = -1 \equiv 3 \pmod 4$. Ifølge sætning 49 er $O_K = \mathbb{Z} + \mathbb{Z}i$ og $d = -4$. Da

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2 = \left(\frac{-1}{p}\right),$$

når p er et ulige primtal, følger det af sætningerne 59 og 62, at dekompositionen af (p) i primidealer er:

(i) $(p) = \mathfrak{p}_1\mathfrak{p}_2$, når $p \equiv 1 \pmod 4$,

(ii) (p) er et primideal i O_K, når $p \equiv -1 \pmod 4$,

(iii) $(2) = \mathfrak{p}^2$.

Formler for $\mathfrak{p}_1$, $\mathfrak{p}_2$ og $\mathfrak{p}$ er givet i øvelsen efter sætning 62.

Eksempel 17. For tallegemet $K = \mathbb{Q}(\sqrt{2})$ er $D = 2 \equiv 2 \pmod 4$. Ifølge sætning 49 er $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ og $d = 8$. Da

$$\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right),$$

når p er et ulige primtal, følger det af sætningerne 59 og 62, at dekompositionen af (p) i primidealer er:

(i) $(p) = \mathfrak{p}_1\mathfrak{p}_2$, når $p \equiv \pm 1 \pmod 8$,

(ii) (p) er et primideal i O_K, når $p \equiv \pm 3 \pmod 8$,

(iii) $(2) = \mathfrak{p}^2$.

Formler for $\mathfrak{p}_1$, $\mathfrak{p}_2$ og $\mathfrak{p}$ er givet i øvelsen efter sætning 62.

Eksempel 18. For tallegemet $K = \mathbb{Q}(\sqrt{-3})$ (det *eisensteinske* tallegeme) er $D = -3 \equiv 1 \pmod 4$. Ifølge sætning 49 er $O_K = \mathbb{Z} + \mathbb{Z}\frac{1}{2}(1+\sqrt{-3})$ og $d = -3$. Ifølge sætning 59 gælder for et primtal $p > 3$:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$
$$= \begin{cases} 1, & \text{når } p \equiv 1 \pmod 3 \\ -1, & \text{når } p \equiv -1 \pmod 3). \end{cases}$$

Det følger nu af sætning 62, at dekompositionen af (p) i primidealer er:

(i) $(p) = \mathfrak{p}_1\mathfrak{p}_2$, når $p \equiv 1 \pmod 3$,

(ii) (p) er et primideal i O_K, når $p \equiv -1 \pmod 3$,

(iii) $(3) = \mathfrak{p}^2$.

Formler for $\mathfrak{p}_1$, $\mathfrak{p}_2$ og $\mathfrak{p}$ er givet i øvelsen efter sætning 62.

Eksempel 19. For tallegemet $K = \mathbb{Q}(\sqrt{-5})$ er $D = -5 \equiv 3 \pmod 4$. Ifølge sætning 49 er $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ og $d = -20$. Ifølge sætning 59 gælder for et primtal $p \neq 2, 5$:

$$\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right),$$

hvor

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{når } p \equiv 1 \pmod 4 \\ -1, & \text{når } p \equiv -1 \pmod 4), \end{cases}$$
$$\left(\frac{p}{5}\right) = \begin{cases} 1, & \text{når } p \equiv \pm 1 \pmod 5 \\ -1, & \text{når } p \equiv \pm 2 \pmod 5). \end{cases}$$

Ifølge den kinesiske restklassesætning for $\mathbb{Z}$ er derfor

$$\left(\frac{-20}{p}\right) = \begin{cases} 1, & \text{når } p \equiv 1, 3, 7, 9, \pmod{20} \\ -1, & \text{når } p \equiv 11, 13, 17, 19 \pmod{20}. \end{cases}$$

Det følger nu af sætning 62, at dekompositionen af (p) i primidealer er:

(i) $(p) = \mathfrak{p}_1\mathfrak{p}_2$, når $p \equiv 1, 3, 7, 9 \pmod{20}$,

(ii) (p) er et primideal i O_K, når $p \equiv 11, 13, 17, 19 \pmod{20}$,

(*iii*) $(p) = \mathfrak{p}^2$, når $p = 2, 5$.

Formler for $\mathfrak{p}_1$, $\mathfrak{p}_2$ og $\mathfrak{p}$ er givet i øvelsen efter sætning 62. Fx er primidealdekompositionen for (2) og (3):

$$\begin{aligned}(2) =&(2, 1+\sqrt{-5})^2 = \mathfrak{p}^2,\\ (3) =&(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = \mathfrak{p}_3\mathfrak{p}_3',\end{aligned}$$

hvorfor (6) har primidealfaktoriseringen $(6) = \mathfrak{p}^2\mathfrak{p}_3\mathfrak{p}_3'$. Da

$$\mathfrak{p}\mathfrak{p}_3 = (6, 2(1+\sqrt{-5}), 3(1+\sqrt{-5}), (1+\sqrt{-5})^2) = (1+\sqrt{-5}),$$

og

$$\mathfrak{p}\mathfrak{p}_3' = (6, 2(1-\sqrt{-5}), 3(1+\sqrt{-5}), 6) = (1-\sqrt{-5}),$$

har vi en idealteoretisk forklaring på, at

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

ikke har entydig faktorisering i primelementer.

Minkowski's sætninger. Den russiske matematiker H. Minkowski (1864–1909) er grundlæggeren af den såkaldte *geometriske talteori*, der har centrale anvendelser i algebraisk talteori.

Definition. Lad $(\underline{e}_1, \ldots, \underline{e}_l)$, $1 \leq l \leq n$, være et lineært uafhængigt sæt af vektorer i $\mathbb{R}^n$. Da kaldes

$$\Lambda = \mathbb{Z}\underline{e}_1 + \cdots + \mathbb{Z}\underline{e}_l,$$

et l-dimensionalt *(punkt)gitter* i $\mathbb{R}^n$. Specielt kaldes Λ et *fuldt* gitter, hvis $l = \operatorname{rang}_{\mathbb{Z}}\Lambda = n$. Ved *gitterdeterminanten* $d(\Lambda)$ forstås

$$d(\Lambda) = v(\{x_1\underline{e}_1 + \cdots + x_l\underline{e}_l \mid x_\lambda \in [0,1[\}),$$

hvor v er det l-dimensionale normerede Lebesquemål.

Bemærkning. Da basisskiftmatricen mellem to $\mathbb{Z}$-baser for et l-dimensionalt gitter er en $l \times l$-heltalsmatrix af determinant ± 1, er gitterdeterminanten uafhængig af basis.

Sætning 63. *Lad Λ være et fuldt gitter i $\mathbb{R}^n$, og lad $\mathcal{S} \subseteq \mathbb{R}^n$ være Lebesguemålelig med $v(\mathcal{S}) > d(\Lambda)$. Da findes to forskellige punkter $\underline{x}_1, \underline{x}_2 \in \mathcal{S}$ med $\underline{x}_1 \equiv \underline{x}_2$ (mod Λ).*

Bevis. Lad $(\underline{e}_1, \ldots, \underline{e}_n)$ være en basis for Λ, og sæt

$$\mathcal{P} = \{x_1\underline{e}_1 + \cdots + x_n\underline{e}_n \mid x_\nu \in [0,1[\}.$$

Lad endvidere

$$\mathcal{P}_{\underline{x}} = \mathcal{P} + \underline{x} \quad \text{for} \quad \underline{x} \in \Lambda$$

være parallelepidet $\mathcal{P}$ translateret med vektoren $\underline{x}$. Af disse definitioner følger umiddelbart, at

$$\bigcup_{\underline{x}\in\Lambda} \mathcal{P}_{\underline{x}} = \mathbb{R}^n,$$

hvor foreningen er disjunkt. Med andre ord: $\mathcal{P}$ er et *fundamentalområde* for gruppen $(\Lambda, +)$ virkende på $\mathbb{R}^n$. Heraf fås, at

$$\mathcal{S} = \mathcal{S} \cap \mathbb{R}^n = \mathcal{S} \cap \bigcup_{\underline{x}\in\Lambda} \mathcal{P}_{\underline{x}} = \bigcup_{\underline{x}\in\Lambda} \mathcal{S} \cap \mathcal{P}_{\underline{x}},$$

hvor foreningen ligeledes er disjunkt. Derfor gælder

$$v(\mathcal{S}) = \sum_{\underline{x}\in\Lambda} v(\mathcal{S} \cap \mathcal{P}_{\underline{x}}).$$

Antag nu (indirekte), at der ikke findes to forskellige $\underline{x}_1, \underline{x}_2 \in \mathcal{S}$ med $\underline{x}_1 \equiv \underline{x}_2$ (mod Λ). Da er

$$\mathcal{T} = \bigcup_{\underline{x}\in\Lambda} (\mathcal{S} \cap \mathcal{P}_{\underline{x}} - \underline{x}),$$

ligeledes en disjunkt forening. Heraf og af det givne fås da

$$v(\mathcal{T}) = \sum_{\underline{x}\in\Lambda} v(\mathcal{S} \cap \mathcal{P}_{\underline{x}} - \underline{x}) = \sum_{\underline{x}\in\Lambda} v(\mathcal{S} \cap \mathcal{P}_{\underline{x}}) = v(\mathcal{S}) > d(\Lambda) = v(\mathcal{P}).$$

Men dette er en modstrid, da $\mathcal{T} \subseteq \mathcal{P}$. □

Sætning 64. *(Minkowski's gitterpunktsætning). Lad Λ være et fuldt gitter i $\mathbb{R}^n$, og lad $\mathcal{S} \subseteq \mathbb{R}^n$ være symmetrisk om $\underline{0}$ og konveks og med $v(\mathcal{S}) > 2^n d(\Lambda)$. Da findes et fra $\underline{0}$ forskelligt gitterpunkt fra Λ i $\mathcal{S}$.*

Bevis. For mængden $\frac{1}{2}\mathcal{S}$, hvor der multipliceres ud fra $\underline{0}$, gælder

$$v(\tfrac{1}{2}\mathcal{S}) = 2^{-n} v(\mathcal{S}) > d(\Lambda).$$

Ifølge sætning 63 indeholder $\frac{1}{2}\mathcal{S}$ derfor to forskellige punkter $\underline{x}_1, \underline{x}_2$ med $\underline{x}_1 \equiv \underline{x}_2 \pmod{\Lambda}$. Da $\mathcal{S}$ og dermed $\frac{1}{2}\mathcal{S}$ er symmetrisk om $\underline{0}$ og konveks, gælder derfor

$$\tfrac{1}{2}(\underline{x}_1 - \underline{x}_2) = \tfrac{1}{2}(\underline{x}_1 + (-\underline{x}_2)) \in \tfrac{1}{2}\mathcal{S} \setminus \underline{0},$$

dvs.

$$\underline{0} \neq \underline{x} = \underline{x}_1 - \underline{x}_2 \in \mathcal{S} \cap \Lambda.$$

Dette viser sætningen. □

Sætning 65. *(Minkowski's linearformsætning: det reelle tilfælde). Lad*

$$L_r(\underline{x}) = a_{r1}x_1 + \cdots + a_{rn}x_n \quad \textit{for} \quad 1 \leq r \leq n$$

være reelle linearformer (dvs. $a_{rs} \in \mathbb{R}$) med $\Delta = \det(a_{rs}) \neq 0$. Lad $c_1, \ldots, c_n$ i $\mathbb{R}_+$ opfylde uligheden

$$c_1 \cdots c_n \geq |\Delta|.$$

Da findes et gitterpunkt $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus \{\underline{0}\}$, så at

$$(*) \qquad |L_r(\underline{x})| \leq c_r \quad \textit{for} \quad 1 \leq r \leq n.$$

Såfremt $n > 1$, kan betingelsen (*) skærpes derved, at " $\leq$ " erstattes af " $<$ " for alle $r \in \{1, \ldots, n\}$ pånær ét.

Bevis. Lad $\epsilon > 0$ være givet. Betragt mængden

$$\mathcal{S}_\epsilon = \{\underline{\xi} \in \mathbb{R}^n \mid |\xi_1| < c_1 + \epsilon,\ |\xi_2| < c_2, \ldots, |\xi_n| < c_n\}.$$

Det bemærkes, at $\mathcal{S}_\epsilon$ er symmetrisk om $\underline{0}$ og konveks, samt at

$$v(\mathcal{S}_\epsilon) = 2^n(c_1 + \epsilon)c_2 \cdots c_n > 2^n|\Delta|.$$

Lad

$$\Lambda = \{(L_1(\underline{x}), \ldots, L_n(\underline{x})) \mid \underline{x} \in \mathbb{Z}^n\} = f(\mathbb{Z}^n),$$

hvor $f : \mathbb{R}^n \to \mathbb{R}^n$ er den lineære afbildning som mht. den naturlige basis har afbildningsmatricen (a_{rs}). Da $\mathbb{Z}^n$ er et fuldt gitter i $\mathbb{R}^n$ med gitterdeterminant 1, er $\Lambda = f(\mathbb{Z}^n)$ et fuldt gitter med $d(\Lambda) = |\det(a_{rs})| = |\Delta|$. Ifølge Minkowski's gitterpunktsætning findes derfor et

$$(**) \qquad \underline{x}_\epsilon \in \mathbb{Z}^n \setminus \{\underline{0}\}, \quad \text{så at} \quad f(\underline{x}_\epsilon) \in \Lambda \cap \mathcal{S}_\epsilon.$$

Det bemærkes, at $\mathcal{S}_\epsilon$ aftager med ϵ, og at fx $\mathcal{S}_1$, som er begrænset, kun indeholder endeligt mange gitterpunkter fra Λ. Derfor følger af (**), at der findes et $\underline{x} \in \mathbb{Z}^n \setminus \{\underline{0}\}$ (uafhængigt af ϵ), så at

$$\underline{0} \neq f(\underline{x}) \in \bigcap_{\epsilon>0} (\Lambda \cap \mathcal{S}_\epsilon) = \Lambda \cap \bigcap_{\epsilon>0} \mathcal{S}_\epsilon.$$

Da

$$\bigcap_{\epsilon>0} \mathcal{S}_\epsilon = \{\underline{\xi} \in \mathbb{R}^n \mid |\xi_1| \leq c_1,\ |\xi_2| < c_2, \ldots, |\xi_n| < c_n\}.$$

har vi vist sætningen i den skærpede formulering (med det specielle $r = 1$). □

Sætning 66. *(Minkowski's linearformsætning: det komplekse tilfælde). Lad*

$$L_r(\underline{x}) = a_{r1}x_1 + \cdots + a_{rn}x_n \quad \textit{for} \quad 1 \leq r \leq n$$

være komplekse linearformer (dvs. $a_{rs} \in \mathbb{C}$) med $\Delta = \det(a_{rs}) \neq 0$ og af følgende specielle form: af de $n = r_1 + 2r_2$ linearformer er de r_1 første $L_1, \ldots L_{r_1}$ alle reelle, medens de $2r_2$ sidste er parvis (komplekst) konjugerede, dvs. $L_{r_1+2j-1} = \overline{L_{r_1+2j}}$ for $1 \leq j \leq r_2$. Lad $c_1, \ldots, c_n \in \mathbb{R}_+$, hvor $c_{r_1+2j-1} = c_{r_1+2j}$ for $1 \leq j \leq r_2$, opfylde uligheden

$$c_1 \cdots c_n \geq |\Delta|.$$

Da findes et gitterpunkt $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus \{\underline{0}\}$, så at

$$(*) \qquad |L_r(\underline{x})| \leq c_r \quad \textit{for} \quad 1 \leq r \leq n.$$

For $r_2 > 0$ kan betingelsen (*) skærpes derved, at "$\leq$" erstattes af "$<$" for alle $r \in \{1, \ldots, n\}$. For $r_2 = 0$ kan betingelsen (*) skærpes som i sætning 65.

Bevis. Vi sætter

$$\begin{aligned} L'_i &= L_i \quad \text{for} \quad 1 \leq i \leq r_1, \\ L'_{r_1+2j-1} &= \tfrac{1}{2}(L_{r_1+2j-1} + L_{r_1+2j}) = \Re L_{r_1+2j-1} \quad \text{for} \quad 1 \leq j \leq r_2, \\ L'_{r_1+2j} &= \tfrac{1}{2i}(L_{r_1+2j-1} - L_{r_1+2j}) = \Im L_{r_1+2j-1} \quad \text{for} \quad 1 \leq j \leq r_2. \end{aligned}$$

Udtrykt ved matricer er sammenhængen

$$\begin{pmatrix} L'_1 \\ \vdots \\ L'_{r_1} \\ L'_{r_1+1} \\ L'_{r_1+2} \\ \vdots \\ L'_{n-1} \\ L'_n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \ldots & 0 & \frac{1}{2} & \frac{1}{2} & \ldots & 0 & 0 \\ 0 & \ldots & 0 & \frac{1}{2i} & -\frac{1}{2i} & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 & 0 & \ldots & \frac{1}{2} & \frac{1}{2} \\ 0 & \ldots & 0 & 0 & 0 & \ldots & \frac{1}{2i} & -\frac{1}{2i} \end{pmatrix} \begin{pmatrix} L_1 \\ \vdots \\ L_{r_1} \\ L_{r_1+1} \\ L_{r_1+2} \\ \vdots \\ L_{n-1} \\ L_n \end{pmatrix}.$$

Af blokstrukturen af denne matrix følger, at $L'_r, 1 \leq r \leq n$, er et system af reelle linearformer af determinant Δ', hvor

$$\Delta' = (-\tfrac{1}{2i})^{r_2} \Delta,$$

og derfor

$$|\Delta'| = 2^{-r_2} |\Delta|.$$

Sætter vi yderligere

$$\begin{aligned} c'_i &= c_i \quad \text{for} \quad 1 \leq i \leq r_1, \\ c'_{r_1+2j-1} = c'_{r_1+2j} &= \tfrac{1}{\sqrt{2}} c_{r_1+2j-1} = \tfrac{1}{\sqrt{2}} c_{r_1+2j} \quad \text{for} \quad 1 \leq j \leq r_2, \end{aligned}$$

har vi derfor

$$c'_1 \cdots c'_n = 2^{-r_2} c_1 \cdots c_n \geq 2^{-r_2} |\Delta| = |\Delta'|.$$

Ifølge sætning 65 findes derfor et gitterpunkt $\underline{x} \in \mathbb{Z}^n \setminus \{\underline{0}\}$, så at

$$|L'_r(\underline{x})| \leq c'_r \quad \text{for} \quad 1 \leq r \leq n,$$

og hvor lighedstegn kun er fornødent for et r. For dette gitterpunkt $\underline{x}$ er da

$$|L_i(\underline{x})| \leq c_i \quad \text{for} \quad 1 \leq i \leq r_1.$$

Endvidere gælder

$$\begin{aligned} |L_{r_1+2j-1}(x)|^2 =& |L'_{r_1+2j-1}(x)|^2 + |L'_{r_1+2j}(x)|^2 \\ \leq& 2 \cdot \tfrac{1}{2} {c_{r_1+2j-1}}^2 = {c_{r_1+2j-1}}^2 \quad \text{for} \quad 1 \leq j \leq r_2, \end{aligned}$$

dvs.

$$|L_{r_1+2j-1}(x)| \leq c_{r_1+2j-1} \quad \text{for} \quad 1 \leq j \leq r_2.$$

Analogt fås

$$|L_{r_1+2j}(x)| \leq c_{r_1+2j} \quad \text{for} \quad 1 \leq j \leq r_2.$$

For $r_2 > 0$ følger skærpelsen som anført ved i sætning 65 at vælge " $<$ " for $1 \leq r < n$. □

Sætning 67. *(Dedekind's diskriminantsætning). Lad $K \neq \mathbb{Q}$ være et algebraisk tallegeme. For diskriminanten d for K gælder da $|d| > 1$.*

Bevis. Lad $[K : \mathbb{Q}] = n > 1$, og lad $K = \mathbb{Q}(\vartheta)$, hvor ϑ er et primitivt element med konjugerede:

$$\vartheta^{(1)}, \ldots, \vartheta^{(r_1)}, \vartheta^{(r_1+1)} = \overline{\vartheta^{(r_1+2)}}, \ldots, \vartheta^{(n-1)} = \overline{\vartheta^{(n)}},$$

hvor de første r_1 konjugerede er reelle, medens de øvrige er ikke reelle men parvis komplekst konjugerede. Lad $K^{(r)} = \mathbb{Q}(\vartheta^{(r)})$ for $1 \leq r \leq n$. Da har $O_{K^{(r)}}$ (jf bemærkning 2, side 3.1) $\mathbb{Z}$-baser $(\omega_s^{(r)} = f_s(\vartheta^{(r)}) \mid 1 \leq s \leq n)$, hvor $f_s \in \mathbb{Q}[x]$ for $1 \leq s \leq n$. Specielt gælder:

$$\omega_s^{(i)} \in \mathbb{R} \quad \text{for} \quad 1 \leq s \leq n,\ 1 \leq i \leq r_1,$$

og

$$\omega_s^{(r_1+2j-1)} = \overline{\omega_s^{(r_1+2j)}} \quad \text{for} \quad 1 \leq s \leq n,\ 1 \leq j \leq r_2.$$

Endvidere er alle $\omega_s^{(r)}$ hele algebraiske tal. Vi betragter systemet af linearformer

$$L_r(\underline{x}) = \sum_{s=1}^{n} \omega_s^{(r)} x_s \quad \text{for} \quad 1 \leq r \leq n$$

med determinant

$$\Delta = \det(\omega_s^{(r)}).$$

Ifølge tidligere beregninger gælder

$$\Delta^2 = d \neq 0,$$

hvor d er diskriminanten for legemet K. Vi vælger nu konstanter $c_1, \ldots, c_n \in \mathbb{R}_+$, hvor $c_{r_1+2j-1} = c_{r_1+2j}$ for $1 \leq j \leq r_2$, og med

$$c_1 \cdots c_n = \sqrt{|d|}.$$

Ifølge sætning 66 findes et gitterpunkt $\underline{x} \in \mathbb{Z}^n \setminus \{\underline{0}\}$, så at

$$|L_r(\underline{x})| \leq c_r \quad \text{for} \quad 1 \leq r \leq n$$

og med den i sætningen angivne skærpelse.

Antag nu (indirekte), at $|d| = 1$. Da var

$$\left| N_{K^{(1)}/\mathbb{Q}} \left(\sum_{s=1}^{n} \omega_s^{(1)} x_s \right) \right| = \left| \prod_{r=1}^{n} \left(\sum_{s=1}^{n} \omega_s^{(r)} x_s \right) \right| = \prod_{r=1}^{n} |L_r(\underline{x})| < c_1 \cdots c_n = 1.$$

Da $\sum_{s=1}^{n} \omega_s^{(1)} x_s$ er et helt algebraisk tal gælder også

$$N_{K^{(1)}/\mathbb{Q}} \left(\sum_{s=1}^{n} \omega_s^{(1)} x_s \right) \in \mathbb{Z}.$$

Tilsammen fås derfor

$$N_{K^{(1)}/\mathbb{Q}} \left(\sum_{s=1}^{n} \omega_s^{(1)} x_s \right) = 0,$$

hvorfor

$$\sum_{s=1}^{n} \omega_s^{(1)} x_s = 0.$$

Men dette er en modstrid, da $(\omega_s^{(1)} \mid 1 \leq s \leq n)$ er en $\mathbb{Z}$-basis for $O_{K^{(1)}}$, og $\underline{x} \neq \underline{0}$. □

Bemærkning. På grund af Stickelberger's sætning kan uligheden i sætningen umiddelbart skærpes til $|d| \geq 3$, jf i øvrigt opgave 2. Ifølge en berømt sætning af Dedekind er primtallet p forgrenet, hvis og kun hvis $p \,|\, d$. Ethvert algebraisk tallegeme $K \neq \mathbb{Q}$ har derfor mindst et (men endeligt mange) forgrenet primtal.

Klassegruppe og klassetal. Lad R være en Dedekindring med brøklegeme K.

Definition. Ved *klassegruppen* $\mathrm{Cl}(R)$ forstås kvotientgruppen mellem gruppen af brudne idealer ($\neq (0)$) og undergruppen af brudne hovedidealer ($\neq (0)$). Ved *klassetallet* h for R forstås $h = h(R) = |\mathrm{Cl}(R)|$.

Bemærkning 1. I forbindelse med ovenstående definition af klassegruppe siges to fra (0) forskellige brudne idealer $\mathfrak{a}, \mathfrak{b}$ i K mht. R at være *ækvivalente*, hvis de repræsenterer samme element i klassegruppen, dvs.:

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists \alpha \in K \setminus \{0\}, \quad \text{så at} \quad \mathfrak{a} = (\alpha)\mathfrak{b}.$$

Ækvivalensklasserne af brudne idealer kaldes *idealklasser*. Det bemærkes, at enhver idealklasse C indeholder et helt ideal. Thi er $\mathfrak{b} \in C$ og $d \in R \setminus \{0\}$ en fællesnævner for $\mathfrak{b}$, så er $\mathfrak{a} = (d)\mathfrak{b}$ et helt ideal. Da $\mathfrak{a} \sim \mathfrak{b}$ og $\mathfrak{b} \in C$, er $\mathfrak{a} \in C$. Bemærk også, at $\mathfrak{a}$ og $\mathfrak{b}$ tilhører inverse idealklasser C og $C^{-1} \Leftrightarrow \mathfrak{a}\mathfrak{b} = (\alpha) \sim (1)$.

Bemærkning 2. Det er vist (R. Fossum), at enhver abelsk gruppe kan forekomme som $\mathrm{Cl}(R)$ for en passende Dedekindring.

Sætning 68. *Lad R være en Dedekindring. Da er følgende egenskaber ækvivalente:*

(i) $h = 1$.

(ii) Ethvert brudent ideal er et hovedideal.

(iii) R er PID.

(iv) R er UFD.

Bevis. $(i) \Leftrightarrow (ii)$ følger direkte af definitionen. $(ii) \Leftrightarrow (iii)$ er klar. $(iii) \Leftrightarrow (iv)$ følger af sætning 35. □

I det følgende er K et algebraisk tallegeme og $R = O_K$ en klassisk Dedekindring. Vi skriver da også

$$\mathrm{Cl}(K) = \mathrm{Cl}(O_K) \quad \text{og} \quad h(K) = h(O_K) = h.$$

Sætning 69. *Lad $K \neq \mathbb{Q}$ være et algebraisk tallegeme med diskriminant d. Da gælder følgende tre endelighedsbetingelser:*

(i) Enhver idealklasse C indeholder et helt ideal $\mathfrak{a}$, som opfylder uligheden

$$N(\mathfrak{a}) < \sqrt{|d|}.$$

(ii) For ethvert $M \in \mathbb{R}_+$ findes kun endeligt mange hele idealer i O_K med $N(\mathfrak{a}) < M$.

(iii) Klassegruppen Cl(K) er endelig.

Bevis. (i): Lad C være en vilkårlig idealklasse. Da indeholder den inverse idealklasse C^{-1} ifølge bemærkning 1 et helt ideal $\mathfrak{b}$. Lad $\omega = (\omega_1, \ldots, \omega_n)$ være en $\mathbb{Z}$-basis for $\mathfrak{b}$, og betragt systemet af linearformer

$$L_r(\underline{x}) = \sum_{s=1}^{n} \omega_s^{(r)} x_s \quad \text{for} \quad 1 \leq r \leq n.$$

For dette systems determinant Δ gælder da (jf sætning 53)

$$\Delta^2 = \det(\omega_s^{(r)})^2 = D(\omega) = N(\mathfrak{b})^2 d \neq 0.$$

Systemet er derfor af den i sætning 66 betragtede art, og for $c_1 = \cdots = c_n = \sqrt[n]{|\Delta|}$ er også alle betingelser for $c_1, \ldots, c_n$ opfyldt. Sætningen (i den skærpede version) giver da, at der findes et gitterpunkt $\underline{x} \in \mathbb{Z}^n \setminus \{\underline{0}\}$, så at

$$\left| N_{K/\mathbb{Q}} \left(\sum_{s=1}^{n} \omega_s x_s \right) \right| = \left| \prod_{r=1}^{n} \left(\sum_{s=1}^{n} \omega_s^{(r)} x_s \right) \right| = \prod_{r=1}^{n} |L_r(\underline{x})| < c_1 \cdots c_n = |\Delta|.$$

Da $\beta = \sum_{s=1}^{n} \omega_s x_s \in \mathfrak{b}$ og $\beta \neq 0$, er $(0) \neq (\beta) \subseteq \mathfrak{b}$. Altså gælder $\mathfrak{b} \,|\, (\beta)$, dvs. der findes et helt ideal $\mathfrak{a} \neq (0)$, så at $(\beta) = \mathfrak{a}\mathfrak{b}$. Vi har nu

$$N(\mathfrak{a})N(\mathfrak{b}) = N((\beta)) = |N(\beta)| < |\Delta| = N(\mathfrak{b})\sqrt{|d|},$$

hvoraf

$$N(\mathfrak{a}) < \sqrt{|d|}.$$

Da $\mathfrak{b} \in C^{-1}$ og $\mathfrak{ab} = (\beta) \sim (1)$, er $\mathfrak{a} \in C$. Dette viser (i).

(ii): Antag, at $\mathfrak{a} \neq (0)$ er et helt ideal med $N(\mathfrak{a}) < M$. Lad

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})}.$$

Da er

$$N(\mathfrak{a}) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{n_{\mathfrak{p}}(\mathfrak{a})} < M.$$

Da $N(\mathfrak{p}) = p^f$, hvor p er et primtal og $f \in \mathbb{N}$, er

$$p \leq p^f \leq p^{f n_{\mathfrak{p}}(\mathfrak{a})} = N(\mathfrak{p})^{n_{\mathfrak{p}}(\mathfrak{a})} < M \quad \text{hvis} \quad \mathfrak{p} \,|\, \mathfrak{a}.$$

Denne ulighed viser, at der kun kan forekomme primtal $p < M$ og dermed kun endeligt mange mulige primidealer $\mathfrak{p}$ og for hvert af disse kun eksponenter $n_{\mathfrak{p}} \leq \frac{\log M}{\log p}$. Dette viser (ii).

(iii) følger umiddelbart af (i) og (ii). □

Korollar 1. *Såfremt ethvert primideal $\mathfrak{p}$ i R med $N(\mathfrak{p}) < \sqrt{|d|}$ er et hovedideal, da er h=1.*

Bevis. Det givne medfører, at ethvert helt ideal $\mathfrak{a}$ med $N(\mathfrak{a}) < \sqrt{|d|}$ er et hovedideal. Resultatet følger derfor af sætning 69 (i). □

Korollar 2. *For et kvadratisk tallegeme K gælder følgende: Såfremt $(\frac{d}{p}) = -1$ for ethvert primtal $p < \sqrt{|d|}$, da er $h = 1$.*

Bevis. Af sætning 62 følger, at ethvert primideal $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{|d|}$ har formen (p), hvor $p < \sqrt{|d|}$ er et primtal. Korollar 1 giver derfor resultatet. □

Eksempel 20. Legemet $K = \mathbb{Q}(\sqrt{-1})$ har $D = -1 \equiv 3 \pmod 4$. Ifølge sætning 49 er $d = -4$, dvs. $\sqrt{|d|} = 2$. Det eneste hele ideal $\mathfrak{a}$ med $N(\mathfrak{a}) < 2$ er $\mathfrak{a} = (1)$, hvorfor $h = 1$ ifølge sætning 69 (i) (eller korollar 1).

Eksempel 21. Legemet $K = \mathbb{Q}(\sqrt{-2})$ har $D = -2 \equiv 2 \pmod 4$. Ifølge sætning 49 er $d = -8$, dvs. $\sqrt{|d|} < 3$. De eneste primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{|d|}$ har derfor $N(\mathfrak{p}) = 2$. Da $2 \,|\, d(= -8)$, er (2) forgrenet, hvorfor der kun er ét primideal $\mathfrak{p}_2 \,|\, (2)$, og for dette er $N(\mathfrak{p}_2) = 2$. Da $N((\sqrt{-2})) = |N(\sqrt{-2})| = 2$, er $\mathfrak{p}_2 = (\sqrt{-2})$. Ifølge sætning 69 (korollar 1) er da $h = 1$.

Eksempel 22. Legemet $K = \mathbb{Q}(\sqrt{-3})$ har $D = -3 \equiv 1 \pmod 4$. Ifølge sætning 49 er $d = -3$, dvs. $\sqrt{|d|} < 2$. Det eneste hele ideal $\mathfrak{a}$ med $N(\mathfrak{a}) < 2$ er $\mathfrak{a} = (1)$, hvorfor $h = 1$ ifølge sætning 69 (i) (eller korollar 1).

Eksempel 23. Legemet $K = \mathbb{Q}(\sqrt{-7})$ har $D = -7 \equiv 1 \pmod 4$. Ifølge sætning 49 er $d = -7$, dvs. $\sqrt{|d|} < 3$. De eneste primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{|d|}$ har derfor $N(\mathfrak{p}) = 2$. Da $-7 \equiv 1 \pmod 8$ er $(\frac{-7}{2}) = 1$, hvorfor $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ er opløst. Der findes derfor netop to primidealer $\mathfrak{p}_2$ og $\mathfrak{p}_2'$ med norm $< \sqrt{|d|}$, og for disse er $N(\mathfrak{p}_2) = N(\mathfrak{p}_2') = 2$. Da $N((\frac{1}{2}(1+\sqrt{-7}))) = |N(\frac{1}{2}(1+\sqrt{-7}))| = 2$ er fx $\mathfrak{p}_2 = ((\frac{1}{2}(1 + \sqrt{-7})) \sim (1)$. Men da er også $\mathfrak{p}_2' \sim (\mathfrak{p}_2)^{-1} \sim (1)$. Ifølge sætning 69 (korollar 1) er da $h = 1$.

Eksempel 24. Legemet $K = \mathbb{Q}(\sqrt{-11})$ har $D = -11 \equiv 1 \pmod 4$. Ifølge sætning 49 er $d = -11$, dvs. $\sqrt{|d|} < 4$. De eneste primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{|d|}$ har derfor $N(\mathfrak{p}) = 2, 3$. Da $-11 \equiv 5 \pmod 8$ er $(\frac{-11}{2}) = -1$, er (2) træg, dvs. der findes intet primideal $\mathfrak{p}$ med $N(\mathfrak{p}) = 2$. Da $(\frac{-11}{3}) = (\frac{1}{3}) = 1$, er $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ opløst. Der findes derfor netop to primidealer $\mathfrak{p}_3$ og $\mathfrak{p}_3'$ med norm $< \sqrt{|d|}$, og for disse er $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. Da $N((\frac{1}{2}(1 + \sqrt{-11}))) = |N(\frac{1}{2}(1 + \sqrt{-11}))| = 3$ er fx $\mathfrak{p}_3 = ((\frac{1}{2}(1 + \sqrt{-11})) \sim (1)$. Men da er også $\mathfrak{p}_3' \sim (\mathfrak{p}_3)^{-1} \sim (1)$. Ifølge sætning 69 (korollar 1) er da $h = 1$.

Eksempel 25. Legemet $K = \mathbb{Q}(\sqrt{-19})$ har $D = -19 \equiv 1 \pmod 4$. Ifølge sætning 49 er $d = -19$, dvs. $\sqrt{|d|} < 5$. Da

$$-19 \equiv 5 \pmod 8 \Leftrightarrow \left(\frac{-19}{2}\right) = -1,$$

og

$$\left(\frac{-19}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

er $h = 1$ ifølge sætning 69 (korollar 2).

Eksempel 26. Legemet $K = \mathbb{Q}(\sqrt{-5})$ har $D = -5 \equiv 3 \pmod 4$. Ifølge sætning 49 er $d = -20$, dvs. $\sqrt{|d|} < 5$. De eneste primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{|d|}$ har derfor $N(\mathfrak{p}) = 2, 3, 4$. Det fremgår af eksempel 19, at de omhandlede primidealer er

$$\mathfrak{p}_2 = (2, 1 + \sqrt{-5}) \text{ med } {\mathfrak{p}_2}^2 = (2) \text{ og } N(\mathfrak{p}_2) = 2,$$
$$\mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \mathfrak{p}_3' = (3, 1 - \sqrt{-5}) \text{ med } \mathfrak{p}_3\mathfrak{p}_3' = (3) \text{ og } N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3.$$

Da $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ og $N(a + b\sqrt{-5}) = a^2 + 5b^2$, findes der ingen elementer i O_K af norm 2 eller 3. Intet af de tre primidealer er derfor hovedideal. De eneste hele idealer $\mathfrak{a}$ med $N(\mathfrak{a}) < \sqrt{|d|} < 5$ er nu

$$(*) \qquad (1), \quad \mathfrak{p}_2, \quad \mathfrak{p}_3, \quad \mathfrak{p}_3', \quad {\mathfrak{p}_2}^2 = (2).$$

Af udregninger i eksempel 19 fremgår, at

$$\mathfrak{p}_2\mathfrak{p}_3 = (1 + \sqrt{-5}) \sim (1), \quad \mathfrak{p}_2\mathfrak{p}_3' = (1 - \sqrt{-5}) \sim (1).$$

For idealerne i (*) gælder derfor følgende relationer:

$$\mathfrak{p}_3 \sim {\mathfrak{p}_2}^{-1} \sim \mathfrak{p}_2, \quad \mathfrak{p}_3' \sim {\mathfrak{p}_2}^{-1} \sim \mathfrak{p}_2, \quad {\mathfrak{p}_2}^2 \sim (1).$$

Dette viser ifølge sætning 69, at $h = 2$, idet idealklasserne er repræsenteret ved (1) og $\mathfrak{p}_2$. Heraf følger, at klassegruppen $\mathrm{Cl}(K) \simeq C_2$.

Eksempel 27. Legemet $K = \mathbb{Q}(\sqrt{2})$ har $D = 2 \equiv 2 \pmod 4$. Ifølge sætning 49 er $d = 8$, dvs. $\sqrt{|d|} < 3$. De eneste primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{|d|}$ har derfor $N(\mathfrak{p}) = 2$. Da $2 \,|\, d(= 8)$, er (2) forgrenet, hvorfor der kun er ét primideal $\mathfrak{p}_2 \,|\, (2)$, og for dette er $N(\mathfrak{p}_2) = 2$. Da $N((\sqrt{2})) = |N(\sqrt{2})| = 2$, er $\mathfrak{p}_2 = (\sqrt{2})$. Ifølge sætning 69 (korollar 1) er da $h = 1$.

Eksempel 28. Legemet $K = \mathbb{Q}(\sqrt{-13})$ har $D = -13 \equiv 3 \pmod 4$. Ifølge sætning 49 er $d = -52$, dvs. $\sqrt{|d|} < 8$. Primtallene $< \sqrt{|d|}$ er derfor 2, 3, 5, 7. For disse gælder ifølge sætning 62:

$$\left(\frac{d}{2}\right) = 0, \quad \text{dvs.} \quad (2) = {\mathfrak{p}_2}^2, \ N(\mathfrak{p}_2) = 2;$$

$$\left(\frac{d}{3}\right) = \left(\frac{-52}{3}\right) = \left(\frac{-1}{3}\right) = -1, \quad \text{dvs.} \quad (3) \quad \text{er primideal;}$$

$$\left(\frac{d}{5}\right) = \left(\frac{-52}{5}\right) = \left(\frac{-2}{5}\right) = -1, \quad \text{dvs.} \quad (5) \quad \text{er primideal;}$$

$$\left(\frac{d}{7}\right) = \left(\frac{-52}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \text{dvs.} \quad (7) = \mathfrak{p}_7\mathfrak{p}_7', \ N(\mathfrak{p}_7) = N(\mathfrak{p}_7') = 7.$$

De eneste idealer med norm 14 er da $\mathfrak{p}_2\mathfrak{p}_7$ og $\mathfrak{p}_2\mathfrak{p}_7'$, og da idealet $(1+\sqrt{-13})$ har norm 14, er fx $\mathfrak{p}_2\mathfrak{p}_7 = (1+\sqrt{-13}) \sim (1)$. Da tillige $\mathfrak{p}_2{}^2 = (2) \sim (1)$, og $\mathfrak{p}_7\mathfrak{p}_7' = (7) \sim (1)$, følger det, at $\mathfrak{p}_7 \sim \mathfrak{p}_7' \sim \mathfrak{p}_2$.

Da $O_K = \mathbb{Z}+\mathbb{Z}\sqrt{-13}$ og $N(a+b\sqrt{-13}) = a^2+13b^2$, findes der intet element i O_K af norm 2, hvorfor $\mathfrak{p}_2 \not\sim (1)$. Dette viser ifølge sætning 69, at $h = 2$, idet idealklasserne er repræsenteret ved (1) og $\mathfrak{p}_2$. Heraf følger, at klassegruppen $\mathrm{Cl}(K) \simeq C_2$.

Mordell's ligning. I dette afsnit gives eksempler på løsning af diophantiske ligninger (heltalsligninger) ved brug af algebraisk talteori.

Sætning 70. *Den diophantiske ligning*

$$x^3 = y^2 + 2$$

har kun løsningerne $(x, y) = (3, \pm 5) \in \mathbb{Z}^2$.

Bevis. Det er klart, at $(x, y) = (3, \pm 5)$ er løsninger til ligningen. Antag omvendt, at $(x, y) \in \mathbb{Z}^2$ er en løsning. Det bemærkes først, at x og y begge må være ulige. Thi ellers var begge lige, og dermed var $x^3 \equiv 0 \pmod 8$, men $y^2 + 2 \equiv 2 \pmod 4$, modstrid! Vi vil benytte ringen $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{-2}$ for $K = \mathbb{Q}(\sqrt{-2})$, som har klassetal 1 ifølge eksempel 21. Vi har da

$$(*) \qquad x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Lad $a \in O_K$ være (en) største fælles divisor for $y + \sqrt{-2}$ og $y - \sqrt{-2}$. Da gælder:

$$a \,|\, x^3 \Rightarrow N(a) \,|\, N(x^3) = x^6 \Rightarrow N(a) \text{ ulige},$$

og

$$a \,|\, y + \sqrt{-2} - (y - \sqrt{-2}) = 2\sqrt{-2} \Rightarrow N(a) \,|\, N(2\sqrt{-2}) = 8.$$

Følgelig er $N(a) = \pm 1$, dvs. a er en enhed i O_K. Dette viser, at faktorerne $y+\sqrt{-2}$ og $y-\sqrt{-2}$ i (*) er indbyrdes primiske. Da O_K er PID og dermed UFD, og de eneste enheder i O_K er $1 = 1^3$ og $-1 = (-1)^3$, følger det derfor

af (*), at $y+\sqrt{-2}$ og $y-\sqrt{-2}$ begge er 3'de potenser af elementer i O_K. Specielt er altså

$$y+\sqrt{-2}=(u+v\sqrt{-2})^3, \quad \text{hvor} \quad u,v\in\mathbb{Z},$$

dvs.

$$\begin{aligned} y &= u^3-6uv^2, \\ 1 &= 3u^2v-2v^3=v(3u^2-2v^2). \end{aligned}$$

Heraf fås $v=3u^2-2=\pm 1$, altså $v=1, u=\pm 1$. Dette giver $y=\mp 5, x=3$. □

Sætning 71. *Den diophantiske ligning*

$$x^3=y^2+13$$

har kun løsningerne $(x,y)=(17,\pm 70)\in\mathbb{Z}^2$.

Bevis. Det er klart, at $(x,y)=(17,\pm 70)$ er løsninger til ligningen. Antag omvendt, at $(x,y)\in\mathbb{Z}^2$ er en løsning. Det bemærkes først, at x er ulige og y lige. Thi ellers var x lige og y ulige, og dermed var $x^3\equiv 0 \pmod 8$, men $y^2+13\equiv 6 \pmod 8$, modstrid! Vi vil benytte ringen $O_K=\mathbb{Z}+\mathbb{Z}\sqrt{-13}$ for $K=\mathbb{Q}(\sqrt{-13})$, som har klassetal 2 ifølge eksempel 28. Vi har da

$$(*) \qquad x^3=(y+\sqrt{-13})(y-\sqrt{-13}),$$

og svarende hertil idealligningen

$$(**) \qquad (x)^3=(y+\sqrt{-13})(y-\sqrt{-13}),$$

Lad $\mathfrak{a}$ være største fælles divisor for idealerne $(y+\sqrt{-13})$ og $(y-\sqrt{-13})$. Da gælder:

$$\mathfrak{a}\,|\,(x^3)\Rightarrow N(\mathfrak{a})\,|\,N((x^3))=x^6\Rightarrow N(\mathfrak{a}) \text{ ulige},$$

og

$$\begin{aligned} \mathfrak{a}\supseteq(y+\sqrt{-13})\wedge\mathfrak{a}\supseteq(y-\sqrt{-13})&\Rightarrow\mathfrak{a}\supseteq(2\sqrt{-13}) \\ &\Rightarrow N(\mathfrak{a})\,|\,N((2\sqrt{-13}))=4\cdot 13. \end{aligned}$$

Følgelig er $N(\mathfrak{a}) = 1, 13$. Ifølge sætning 62 er (13) forgrenet, dvs. der findes kun et ideal $\mathfrak{p}_{13}$ af norm 13. Imidlertid er $N((\sqrt{-13})) = 13$, hvorfor $\mathfrak{p}_{13} = (\sqrt{-13})$ er det eneste ideal af norm 13. Såfremt $N(\mathfrak{a}) = 13$, er derfor $\mathfrak{a} = (\sqrt{-13})$, men da ville venstre side af (*) være delelig med 13^3 og højre side delelig med 13 men ikke med 13^2, modstrid! Derfor er $\mathfrak{a} = (1)$, altså idealerne $(y + \sqrt{-13})$ og $(y - \sqrt{-13})$ i (**) indbyrdes primiske. Da O_K er en Dedekindring følger det derfor af (**), at $(y + \sqrt{-13})$ og $(y - \sqrt{-13})$ begge er 3'de potenser af hele idealer i O_K. Specielt er altså

$$(y + \sqrt{-13}) = \mathfrak{b}^3, \quad \text{hvor} \quad \mathfrak{b} \quad \text{er et helt ideal i} \quad O_K.$$

Da klassetallet for O_K er 2, er $\mathfrak{b}^2 \sim (1)$, hvorfor

$$\mathfrak{b} \sim \mathfrak{b}^3 = (y + \sqrt{-13}) \sim (1),$$

dvs. $\mathfrak{b}$ er selv et hovedideal. Lad $\mathfrak{b} = (u + v\sqrt{-13})$, hvor $u, v \in \mathbb{Z}$. Da er

$$(y + \sqrt{-13}) = (u + v\sqrt{-13})^3.$$

Da de eneste enheder i O_K er $1 = 1^3$ og $-1 = (-1)^3$, følger heraf (efter evt. fortegnsskift for u og v), at

$$y + \sqrt{-13} = (u + v\sqrt{-13})^3.$$

Denne ligning er ensbetydende med

$$\begin{aligned} y &= u^3 - 39uv^2, \\ 1 &= 3u^2v - 13v^3 = v(3u^2 - 13v^2). \end{aligned}$$

Heraf fås $v = 3u^2 - 13 = \pm 1$, altså $v = -1, u = \pm 2$. Dette giver $y = \mp 70, x = 17$. □

Historisk note. Den diophantiske ligning

$$y^2 = x^3 + t, \quad t \in \mathbb{Z} \setminus \{0\},$$

der nu sædvanligvis kaldes *Mordell's ligning* efter den engelske matematiker L. J. Mordell, har en historie, der går tilbage til Bachet (1621). Bachet observerede løsningen $(x, y) = (3, 5)$ for $t = -2$ (jf sætning 70), og Fermat stillede engelske matematikere den opgave at vise, at dette er den eneste løsning i

naturlige tal. Det kan til den anvendte metode bemærkes, at den fungerer, når klassetallet $h = h(\mathbb{Q}(\sqrt{t}))$ ikke er deleligt med 3. Situationen kompliceres dog for $t > 0$ af tilstedeværelsen af uendeligt mange enheder.

Det bør endelig nævnes, at den engelske matematiker A. Baker (1968) har vist, at Mordell's ligning for ethvert t kun har endeligt mange løsninger, idet disse tilfredsstiller uligheden

$$(*) \qquad \max(|x|, |y|) < \exp(10^{10}|t|^{10^4}).$$

Baker's metode giver således en *effektiv* løsning af Mordell's ligning. Baker har senere forbedret vurderingen i (*) væsentligt og derved været i stand til at løse ligningen fuldstændigt for numeriske værdier af t.

Imaginært kvadratiske tallegemer med klassetal 1. Vi viser først

Sætning 72. *Lad $K = \mathbb{Q}(\sqrt{D})$, hvor $D < 0$ og kvadratfri, og lad h være klassetallet for K. Hvis klassetallet $h = 1$, da gælder:*

$$D = -1, -2, -7 \quad \textit{eller} \quad D = -p, \quad \textit{hvor} \quad p \equiv 3 \pmod 8 \quad \textit{er et primtal.}$$

Bevis. 1. Lad $D \equiv 2, 3 \pmod 4$. Ifølge sætning 49 er $d = 4D$, og $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}$. Da er $(\frac{d}{2}) = 0$, og ifølge sætning 62 er derfor $(2) = \mathfrak{p}_2{}^2$, hvor $N(\mathfrak{p}_2) = 2$. Da $N(a + b\sqrt{D}) = a^2 - Db^2$, findes intet element i O_K af norm 2, når $-D > 2$. For $-D > 2$ er derfor $\mathfrak{p}_2 \not\sim (1)$, altså $h > 1$. Da $h = 1$, er de eneste muligheder $D = -1, -2$. For disse værdier af D er $h = 1$ ifølge eksemplerne 20-21.

2. Lad $D \equiv 1 \pmod 4$. Ifølge sætning 49 er $d = D$, og $O_K = \mathbb{Z} + \mathbb{Z}\frac{1}{2}(1 + \sqrt{D})$.

Betragt først tilfældet $D = d \equiv 1 \pmod 8$. Da er $(\frac{d}{2}) = 1$, og ifølge sætning 62 er derfor $(2) = \mathfrak{p}_2\mathfrak{p}_2{}'$, hvor $N(\mathfrak{p}_2) = N(\mathfrak{p}_2{}') = 2$. Da

$$N\left(a + b\frac{1+\sqrt{D}}{2}\right) = a^2 + ab + \frac{1-D}{4}b^2 = a^2 + ab + b^2 + \frac{-3-D}{4}b^2,$$

findes intet element i O_K af norm 2, når $-D > 7$. For $-D > 7$ er derfor $\mathfrak{p}_2 \not\sim (1)$, altså $h > 1$. Da $h = 1$, er den eneste mulighed $D = -7$. For $D = -7$ er er $h = 1$ ifølge eksempel 23.

Betragt dernæst tilfældet $D = d \equiv 5 \pmod 8$, og antag (indirekte), at $-D = -d = p_1 \cdots p_r$, hvor $r > 1$, og $p_1 < \cdots < p_r$ er primdivisorerne i $-D$. Da er $(\frac{d}{p_1}) = 0$, og ifølge sætning 62 er derfor $(p_1) = \mathfrak{p}^2$, hvor $N(\mathfrak{p}) = p_1$. Da $h = 1$ er

$$\mathfrak{p} = \left(a + b\frac{1+\sqrt{D}}{2}\right), \quad \text{hvor} \quad a, b \in \mathbb{Z}.$$

Men da gælder

$$-\frac{D}{5} \geq \frac{-D}{p_2 \cdots p_r} = p_1 = a^2 + ab + b^2 + \frac{-3-D}{4}b^2.$$

Da $b \neq 0$ (ellers var $p_1 = a^2$), er derfor

$$-\frac{D}{5} \geq 1 + \frac{-3-D}{4} = \frac{1-D}{4} > -\frac{D}{4},$$

hvilket er en modstrid. Altså er $D = -p$, hvor $p \equiv 3 \pmod 8$ er et primtal. □

Som supplement til den foregående sætning viser vi dernæst

Sætning 73. *(Rabinowitsch) Lad $K = \mathbb{Q}(\sqrt{-p})$, hvor $p \equiv 3 \pmod 8$ er et primtal > 3. Lad h være klassetallet for K, og lad $f_q(x) = x^2 + x + q$, hvor $q = \frac{p+1}{4}$. Da gælder:*

$$h = 1 \Leftrightarrow f_q(x) \text{ har primtalsværdi for } \quad x = 0, \ldots, q-2.$$

Bevis. Det bemærkes først, at

$$(*) \quad q = f_q(0) \leq f_q(x) \leq f_q(q-2) = (q-1)^2 + 1 = \left(\frac{p-3}{4}\right)^2 + 1 < \left(\frac{p}{4}\right)^2$$

for $0 \leq x \leq q-2$. Det ses iøvrigt, at

$$f_q(q-1) = q^2 \quad \text{og} \quad f_q(q) = (q+1)^2 - 1$$

ikke er primtal for $q \geq 3$.

$\Rightarrow$: Da $O_K = \mathbb{Z} + \mathbb{Z}\frac{1}{2}(1+\sqrt{-p})$ gælder for $\alpha = x + \frac{1}{2}(1+\sqrt{-p}) \in O_K$, at

$$N(\alpha) = \alpha\overline{\alpha} = f_q(x).$$

Ifølge (*) er derfor

$$(**) \qquad N(\alpha) < (\tfrac{p}{4})^2 \quad \text{for} \quad 0 \le x \le q-2.$$

Vi påstår, at α er et primelement. Antag (indirekte), at $\alpha = \alpha_1\alpha_2$, hvor $\alpha_i \in O_K$ ikke er en enhed for $i = 1, 2$. For $i = 1, 2$ er da

$$\alpha_i = a_i + b_i\frac{1+\sqrt{-p}}{2},\ a_i, b_i \in \mathbb{Z}.$$

Her er $b_i \neq 0$ for $i = 1, 2$, thi hvis $b_i = 0$ var $\alpha_i = a_i$ og $|a_i| \ge 2$, hvorfor $\alpha/\alpha_i \notin O_K$, modstrid! For $i = 1, 2$ er følgelig

$$N(\alpha_i) = a_i^2 + a_ib_i + b_i^2 + \frac{p-3}{4}b_i^2 \ge 1 + \frac{p-3}{4} = \frac{p+1}{4} > \frac{p}{4},$$

altså $N(\alpha) = N(\alpha_1)N(\alpha_2) > (\frac{p}{4})^2$, i modstrid med (**). Altså er α og dermed også $\overline{\alpha}$ primelementer i O_K. Da O_K er UFD, er $f_q(x) = \alpha\overline{\alpha}$ derfor essentielt den eneste faktorisering af $f_q(x)$ inden for O_K. Da

$$(***) \qquad f_q(x) \ge q \ge 3 \quad \text{for} \quad 0 \le x \le q-2,$$

er $f_q(x)$ derfor et primtal.

$\Leftarrow$: Ifølge sætning 69 korollar 2 er det tilstrækkeligt at vise, at $(\frac{d}{l}) = -1$ for alle primtal $l < \sqrt{|d|}$. Det observeres, at

$$\sqrt{|d|} = \sqrt{p} = \sqrt{4q-1} \le q-2 \Leftrightarrow q > 7.$$

1°. Vi behandler først specialtilfældene $q \le 7$, dvs. $p = 4q-1 \le 27$. De eneste primtal $p \equiv 3 \pmod 8$ med $3 < p \le 27$ er $p = 11, 19$ svarende til $q = 3, 5$. Ifølge eksemplerne 24-25 er $h = 1$ i begge tilfælde. På den anden side er

$$f_3(x) = x^2 + x + 3, \quad \text{altså} \quad f_3(0) = 3,\ f_3(1) = 5,$$

og

$$f_5(x) = x^2 + x + 5, \quad \text{altså} \quad f_5(0) = 5,\ f_5(1) = 7,\ f_5(2) = 11,\ f_5(3) = 17,$$

hvorfor betingelsen om primtalsværdier er opfyldt.

2°. For $q > 7$ er det ifølge (***) tilstrækkeligt at vise, at

$$\left(\frac{d}{l}\right) = \left(\frac{-p}{l}\right) = -1 \quad \text{for alle primtal} \quad l < q-2.$$

Antag (indirekte), at der findes et primtal $l < q-2$ med $(\frac{d}{l}) = 0, 1$ Da findes et primideal $\mathfrak{p}$ med $\mathfrak{p} \,|\, (l)$ og med $N(\mathfrak{p}) = l$. De l restklasser i $O_K/\mathfrak{p}$ er derfor repræsenteret ved

$$\left\{ x + \frac{1+\sqrt{-p}}{2} \mid 0 \le x < l < q-2 \right\}.$$

Specielt findes der derfor et $x \in [0, l[$, så at

$$x + \frac{1+\sqrt{-p}}{2} \equiv 0 \pmod{\mathfrak{p}} \Rightarrow f_q(x) = N\left(x + \frac{1+\sqrt{-p}}{2}\right) \equiv 0 \pmod{l},$$

idet vi benytter, at $\mathfrak{p} \cap \mathbb{Z} = l\mathbb{Z}$ jf sætning 54. Da $f_q(x)$ er et primtal må der derfor gælde $f_q(x) = l$. Men dette er en modstrid, da $l < q-2 < q \le f_q(x)$. □

Historisk note. At polynomierne $f_q(x)$ fremstiller primtal for $0 \le x \le q-2$ for $q = 3, 5, 11, 17, 41$ (svarende til $p = 11, 19, 43, 67, 163$) blev observeret af L. Euler (1707-1783). C. F. Gauss (1777-1855) undersøgte i *Disquisitiones Arithmeticae* (1801) klassetal for kvadratiske former i to variable af given diskriminant og heltalskoefficienter. Han fandt, at klassetallet for negativ diskriminant d er lig 1 i 9 tilfælde, nemlig for $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ og tilsyneladende ikke i andre tilfælde. Sammenhængen mellem Eulers og Gauss' observationer blev klarlagt med ovennævnte sætning af G. Rabinowitsch (1913).

At der kun er endeligt mange imaginært kvadratiske tallegemer $\mathbb{Q}(\sqrt{D})$, med klassetal 1, blev vist af H. Heilbronn (1934), der viste, at $h(\mathbb{Q}(\sqrt{D})) \to \infty$ for $-D \to \infty$. Samme år viste H. Heilbronn og E. H. Linnfoot, at der udover de ni kendte imaginært kvadratiske tallegemer med klassetal 1 højst var ét til, og at $-D > 5 \cdot 10^9$ for et sådant. Dette berømte problem blev løst af K. Heegner (1952), A. Baker (1966) og H. M. Stark (1967), der alle viste, at der kun findes ni sådanne tallegemer. Der henvises til H. M. Stark, *On the Problem of Unique Factorization in Complex Quadratic Fields*, (41-56). Proceedings of Symposia in Pure Mathematics, Volume XII, Number Theory, AMS 1969.

Euklidiske ringe. I det følgende er R et integritetsområde.

Definition. En *euklidisk funktion* f på R er en afbildning $f : R \to \mathbb{N}_0$ med følgende egenskab:

$$\forall a, b \in R,\ b \neq 0,\ \exists q, r \in R \quad \text{med} \quad a = bq + r \quad \text{og} \quad f(r) < f(b).$$

Ringen R kaldes *euklidisk*, hvis der findes en euklidisk funktion f på R.

Sætning 74. *Lad f være en euklidisk funktion på R. Da gælder:*

(i) $f(0) < f(b)$ *for ethvert* $b \in R \setminus \{0\}$.

(ii) $\forall b \in R : f(b) = min_{x \in R \setminus \{0\}} f(x) \Rightarrow b$ *er en enhed i* R.

Bevis. (i). Vi kan gerne antage, at $f(b) = \min_{x \in R \setminus \{0\}} f(x)$. For ethvert $a \in R$ findes da $q, r \in R$, så at $a = bq + r$ og $f(r) < f(b)$. Pga. minimaliteten af $f(b)$ er $r = 0$.

(ii). Argumentet i (i) viser, at b er divisor i ethvert $a \in R$. □

Sætning 75. *R euklidisk $\Rightarrow$ R er PID.*

Bevis. Lad $\mathfrak{a} \neq (0)$ være et vilkårligt ideal i R, og lad $b \neq 0$ være et element i $\mathfrak{a}$, for hvilket $f(b) = \min_{x \in \mathfrak{a} \setminus \{0\}} f(x)$. For et vilkårligt $a \in \mathfrak{a}$ findes da $q, r \in R$ med $a = bq + r$ og $f(r) < f(b)$. Da $a, b \in \mathfrak{a}$, er $r \in \mathfrak{a}$, og pga. minimaliteten af $f(b)$ er derfor $r = 0$. Men dette viser, at $a = bq \in bR$, dvs. $\mathfrak{a} = bR$ er et hovedideal. □

Definition. To euklidiske funktioner f og g på R kaldes *ækvivalente*, hvis der findes en ordensbevarende bijektion $\varphi : f(R) \to g(R)$, så at $g = \varphi \circ f$.

Sætning 76. *Lad R være en euklidisk ring, og lad $\{f_\alpha \mid \alpha \in I\}$ være familien af samtlige euklidiske funktioner på R. Da er $f = inf\, f_\alpha$ defineret ved*

$$f(x) = inf_{\alpha \in I} f_\alpha(x) = min_{\alpha \in I} f_\alpha(x) \quad for \quad x \in R,$$

ligeledes en euklidisk funktion på R.

Bevis. Givet $a, b \in R$, $b \neq 0$. Da findes et $\alpha_0 \in I$, så at $f(b) = f_{\alpha_0}(b)$. Da f_{α_0} er euklidisk på R findes $q, r \in R$, så at $a = bq + r$ og $f_{\alpha_0}(r) < f_{\alpha_0}(b)$. Der gælder da

$$f(r) = \min_{\alpha \in I} f_\alpha(r) \leq f_{\alpha_0}(r) < f_{\alpha_0}(b) = f(b),$$

hvormed påstanden er bevist. □

Definition. Funktionen f i sætning 76 kaldes *den minimale euklidiske funktion* på en euklidisk ring R.

Eksempel 29. Ringen $R = \mathbb{Z}$ er euklidisk med sædvanlig absolutværdi $|\ |$ som euklidisk funktion. Denne euklidiske funktion er ikke minimal. Derimod ses det let, at

$$f : n \mapsto \begin{cases} 0, & \text{når} \quad n = 0 \\ \left[\frac{\log |n|}{\log 2}\right] + 1, & \text{når} \quad n \neq 0 \end{cases}$$

er den minimale euklidiske funktion. Bemærk, at $f(n)$ for $n > 0$ er antallet af binære cifre i $|n|$. Alternativt betyder dette, at

$$f^{-1}(0) = \{0\},\ f^{-1}(1) = \{-1, 1\},\ f^{-1}(2) = \{\pm 2, \pm 3\},$$
$$f^{-1}(3) = \{\pm 4, \pm 5, \pm 6, \pm 7\}, \ldots .$$

Eksempel 30. Polymiumsringen $R = k[x]$ over et vilkårligt kommutativt legeme k er euklidisk, idet

$$f : F(x) \mapsto \begin{cases} 0, & \text{når} \quad F \quad \text{er nulpolynomiet} \\ (\partial F) + 1 & \text{ellers} \end{cases}$$

er en euklidisk funktion. Denne funktion er faktisk den minimale euklidiske funktion.

Sætning 77. *(Motzkin) Lad R være et integritetsområde, og definér ved induktion*

$$R_0 = \{0\},$$
$$R_n{}' = \{b \in R \mid \textit{ hver restklasse modulo } b \textit{ indeholder et } r \in \bigcup_{\nu<n} R_\nu\},$$
$$R_n = R_n{}' \setminus \bigcup_{\nu<n} R_\nu, \quad n \geq 1.$$

Da er R euklidisk, hvis og kun hvis

$$R = \bigcup_{n=0}^{\infty} R_n.$$

I bekræftende fald er $f : R \to \mathbb{N}_0$ defineret ved

$$f(x) = n \Leftrightarrow x \in R_n, \quad \textit{dvs.} \quad f^{-1}(n) = R_n,$$

den minimale euklidiske funktion på R.

Bevis. 1°. Antag, at $R = \cup_{n=0}^{\infty} R_n$. Vi vil først vise, at $f : R \to \mathbb{N}_0$ er en euklidisk funktion. For $a, b \in R$ med $b \neq 0$ er $f(b) = n > 0$. Da er $b \in R_n \subseteq {R_n}'$, hvorfor der findes et $r \in \cup_{\nu<n} R_\nu$, så at $a \equiv r \pmod{b}$. Men dette betyder, at der findes et $q \in R$, så at $a = bq + r$. Da $f(r) < n = f(b)$, viser dette, at f er euklidisk.

Lad $\tilde{f}$ være den minimale euklidiske funktion på R, og antag (indirekte), at $f \neq \tilde{f}$, dvs. $f > \tilde{f}$. Lad $\tilde{R}_n = \tilde{f}^{-1}(n)$ for $n \in \mathbb{N}_0$, og sæt $\tilde{R}'_n = \cup_{\nu \leq n} \tilde{R}_\nu$. Da findes et $n_0 \in \mathbb{N}$, så at

$${R_\nu}' = \tilde{R}'_\nu, \ 0 \leq \nu < n_0, \ {R_{n_0}}' \subset \tilde{R}'_{n_0}.$$

For $b \in \tilde{R}'_{n_0} \setminus {R_{n_0}}'$ og ethvert $a \in R$ findes (da $\tilde{f}$ er euklidisk) $q, r \in R$ med $a = bq + r$ og $\tilde{f}(r) < \tilde{f}(b) = n$. Men da $\tilde{f}(r) = f(r)$ opfylder b betingelsen for at tilhøre ${R_n}'$, og dette er en modstrid, da $f(b) > n$.

2°. Antag, at R er euklidisk med minimal euklidisk funktion $\tilde{f}$, og definer $\tilde{R}_n$ og $\tilde{R}'_n$ som ovenfor. Det samme argument som før viser, at ${R_n}' = \tilde{R}'_n$ og dermed at $R_n = \tilde{R}_n$ for $n \in \mathbb{N}_0$. Men dette giver umiddelbart

$$\bigcup_{n=0}^{\infty} R_n = \bigcup_{n=0}^{\infty} \tilde{R}_n = R,$$

som ønsket. □

Bemærkning. Ved at anvende sætning 77 på $R = \mathbb{Z}$ og $R = k[x]$, hvor k er et (kommutativt) legeme, finder man umiddelbart de i eksemplerne 29 og 30 anførte minimale euklidiske funktioner.

Sætning 78. *Lad $K = \mathbb{Q}(\sqrt{D})$, hvor $D < 0$ og kvadratfri, være et imaginært kvadratisk tallegeme, og lad $R = O_K$. Da er R euklidisk, hvis og kun hvis $D = -1, -2, -3, -7, -11$. I alle disse tilfælde er normen $N : O_K \to \mathbb{N}_0$ en euklidisk funktion (men i intet tilfælde den minimale).*

Bevis. For $D \equiv 2, 3 \pmod 4$ er $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}$, og for $x = a + b\sqrt{D} \in O_K$ er $N(x) = a^2 - Db^2$. For $-D > 2$ (dvs. $-D \geq 5$) gælder derfor

$$\{x \in O_K \mid N(x) < 4\} = \{0, 1, -1\} \quad \text{og} \quad N(0) = 0,\ N(\pm 1) = 1.$$

For $D \equiv 1 \pmod 4$ er $O_K = \mathbb{Z} + \mathbb{Z}\frac{1}{2}(1+\sqrt{D})$, og for $x = a + b\frac{1}{2}(1+\sqrt{D}) \in O_K$ er $N(x) = a^2 + ab + b^2 + \frac{1}{4}(-3-D)b^2$. For $-D > 11$ (dvs. $-D \geq 15$) gælder derfor

$$\{x \in O_K \mid N(x) < 4\} = \{0, 1, -1\} \quad \text{og} \quad N(0) = 0,\ N(\pm 1) = 1.$$

For $D \neq -1, -2, -3, -7, -11$ er derfor

$$R_0 = \{0\},\ R_1{}' = \{0, 1, -1\},\ R_2{}' = R_1{}', \ldots, R_n{}' = R_1{}', \ldots,$$

dvs.

$$R_0 = \{0\},\ R_1 = \{1, -1\},\ R_n = \emptyset \text{ for } n > 1.$$

Altså er

$$\bigcup_{n=0}^{\infty} R_n = \{0, 1, -1\} \neq R,$$

hvorfor $R = O_K$ ikke er euklidisk for $D \neq -1, -2, -3, -7, -11$.

For at fuldføre beviset for sætningen, skal vi derfor blot vise, at normen N er en euklidisk funktion i disse fem tilfælde. Vi skal altså vise:

(*) $$\forall a, b \in O_K, b \neq 0, \exists q \in O_K \text{ med} \quad N(a - bq) < N(b).$$

På grund af multiplikativiteten af N gælder

$$N(a - bq) < N(b) \Leftrightarrow N(a/b - q) < 1 \Leftrightarrow |a/b - q| < 1,$$

hvorfor (*) er en konsekvens af følgende:

(**) $$\forall z \in \mathbb{C}\ \exists q \in O_K \quad \text{med} \quad |z - q| < 1.$$

Betegner $\mathrm{dist}(z, O_K)$ den mindste afstand fra $z \in \mathbb{C}$ til et punkt i O_K er det en elementær geometrisk opgave at indse, at

$$\max_{z\in\mathbb{C}} \mathrm{dist}(z, O_K) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \quad D = -1 \\ \frac{\sqrt{3}}{2} & \text{for} \quad D = -2 \\ \frac{1}{\sqrt{3}} & \text{for} \quad D = -3 \\ \frac{2}{\sqrt{7}} & \text{for} \quad D = -7 \\ \frac{3}{\sqrt{11}} & \text{for} \quad D = -11 \end{cases}$$

Da alle disse maksimale afstande er < 1, er (**) og dermed (*) opfyldt i de fem tilfælde. □

Sætning 79. *Lad $K = \mathbb{Q}(\sqrt{D})$, hvor $D > 1$ og kvadratfri, være et reelt kvadratisk tallegeme, og lad $R = O_K$. Da er $|N| : O_K \to \mathbb{N}_0$ en euklidisk funktion på R, hvis og kun hvis $D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.*

Bevis. Et fuldstændigt bevis for denne sætning er overordentligt kompliceret (jf. V. Ennola: *On the first inhomogeneous minimum of binary quadratic forms and Euclid's algorithm in real quadratic fields*, Ann. Univ. Turku (1958), 9-58).

Vi vil derfor nøjes med at vise resultatet for nogle få (små) værdier af D, og vi skal altså vise:
(*)
$\forall a, b \in O_K, b \neq 0, \exists q \in O_K \quad$ med $|N(a-bq)| < |N(b)|$, dvs. $|N(a/b-q)| < 1$.

For $D \equiv 2, 3 \pmod 4$ er $\frac{a}{b} \in K$, dvs. $\frac{a}{b} = r + s\sqrt{D}$ med $r, s \in \mathbb{Q}$, og $q = x + y\sqrt{D}$ med $x, y \in \mathbb{Z}$. Vi skal ifølge (*) vise, at uligheden

$$|N(r - x + (s - y)\sqrt{D})| = |(r - x)^2 - D(s - y)^2| < 1$$

for givet $(r, s) \in \mathbb{Q}^2$ har en heltalsløsning (x, y). Da vi altid kan vælge $x, y \in \mathbb{Z}$, så at $|r - x| \leq \frac{1}{2}$, $|s - y| \leq \frac{1}{2}$, kan vi derfor opnå, at

$$|N(r - x + (s - y)\sqrt{D})| \leq \tfrac{1}{4}D.$$

Da $\frac{1}{4}D < 1$ for $D = 2, 3$, har vi derfor vist, at $|N|$ er en euklidisk funktion på O_K for $D = 2, 3$.

For $D \equiv 1 \pmod 4$ er $\frac{a}{b} \in K$, dvs. $\frac{a}{b} = r + s \cdot \frac{1}{2}(1+\sqrt{D})$ med $r, s \in \mathbb{Q}$, og $q = x + y \cdot \frac{1}{2}(1+\sqrt{D})$ med $x, y \in \mathbb{Z}$. Vi skal ifølge (*) vise, at uligheden

$$|N(r-x+\tfrac{1}{2}(s-y)(1+\sqrt{D}))| = |(r-x)^2+(r-x)(s-y)-\tfrac{1}{4}(D-1)(s-y)^2| < 1$$

for givet $(r,s) \in \mathbb{Q}^2$ har en heltalsløsning (x,y). Da vi altid kan vælge $x, y \in \mathbb{Z}$, så at $|r-x| \leq \frac{1}{2}$, $|s-y| \leq \frac{1}{2}$, og i tilfælde af $|r-x| = \frac{1}{2}$ disponere over fortegnet for $r-x$, så at $(r-x)(s-y) \geq 0$, kan vi derfor opnå, at

$$|N(r-x+(s-y)\tfrac{1}{2}(1+\sqrt{D}))| < \frac{D+3}{16}$$

Da $\frac{1}{16}(D+3) \leq 1$ for $D = 5, 13$, har vi derfor vist, at $|N|$ er en euklidisk funktion på O_K for $D = 5, 13$. □

Historisk note. En meget læseværdig oversigtsartikel om dette emne er Hendrik W. Lenstra, Jr.: *Euclidean Number Fields* 1-3, Mathematical Intelligencer, vol 2 (1979), 6-15, 73-77, 99-103. Heri omtales udførligt cirkeldelingslegemer $K_n = \mathbb{Q}(e^{2\pi i/n})$, hvor $n \in \mathbb{N}$. Da $K_n = K_{2n}$, når n er ulige (da er $\varphi(n) = \varphi(2n)$), kan det antages, at $n \not\equiv 2 \pmod 4$.

Ifølge J. M. Masley og H. L. Montgomery (*Cyclotomic fields with unique factorization*, J. Reine Angew. Math. 286/287 (1976), 248-256) gælder da, at K_n har klassetal 1, hvis og kun hvis $n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$.

Det er endvidere kendt, at O_{K_n} er euklidisk mht. normen (dvs. $|N|$ er en euklidisk funktion), hvis $n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 16, 20, 24$.

Et andet af H.W. Lenstra's mange interessante bidrag til emnet er følgende bemærkelsesværdige resultat:

Lad K være et algebraisk tallegeme, og antag, at O_K har klassetal 1 og har uendeligt mange enheder (dette udelukker netop $\mathbb{Q}$ og de imaginært kvadratiske tallegemer). Forudsat gyldigheden af et antal generaliserede Riemann hypoteser er da O_K euklidisk.

Dirichlet's enhedssætning. Vi betragter et algebraisk tallegeme K af grad $n = [K : \mathbb{Q}]$. Som sædvanligt betegner O_K ringen af hele elementer i K, og $O_K^\times$ betegner mængden af enheder (invertible elementer mht. multiplikationen) i O_K. For normen $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ og sporet $S_{K/\mathbb{Q}} : K \to \mathbb{Q}$ vil vi sædvanligvis benytte de korte skrivemåder N og S. Der mindes om, at $N(\alpha)$, $S(\alpha) \in \mathbb{Z}$, når $\alpha \in O_K$. Diskriminanten for K, betegnes som sædvanligt d.

Sætning 80. *Mængden $O_K^\times$ udgør en multiplikativ gruppe. Endvidere gælder:*

$$O_K^\times = \{\epsilon \in O_K \mid N(\epsilon) = \pm 1\}.$$

Bevis. Den første påstand følger direkte af definitionen på $O_K^\times$. Vi viser formlen for $O_K^\times$ ved at vise hver af de to inklusioner. Da formlen er klar for $n = 1$ antages $n > 1$. $\subseteq$: Såfremt $\epsilon \in O_K^\times$, er $\epsilon^{-1} \in O_K$, hvorfor $N(\epsilon), N(\epsilon^{-1}) \in \mathbb{Z}$. Da $N(\epsilon)N(\epsilon^{-1}) = N(1) = 1$, er derfor $N(\epsilon) = \pm 1$.

$\supseteq$: Betragt omvendt et $\epsilon \in O_K$ med $N(\epsilon) = \pm 1$. Lad de konjugerede for ϵ være $\epsilon^{(1)} = \epsilon, \epsilon^{(2)}, \ldots, \epsilon^{(n)}$, og sæt $\epsilon' = \epsilon^{(2)} \cdots \epsilon^{(n)}$. Da $\epsilon^{(2)}, \ldots, \epsilon^{(n)}$ er hele algebraiske tal, er ϵ' det også. Endvidere er $\epsilon\epsilon' = N(\epsilon) = \pm 1$, altså $\epsilon' = \pm 1/\epsilon \in K$. Da O_K er helt afsluttet i K, er derfor $\epsilon' \in O_K$. Dette viser, at $\epsilon \in O_K^\times$. □

Sætning 81. *(Dirichlet's enhedssætning, 1846). Lad K være et algebraisk tallegeme af grad n, og lad der være r_1 reelle isomorfe indlejringer af K i $\mathbb{C}$ og r_2 par komplekse indlejringer af K i $\mathbb{C}$. Sæt $r = r_1 + r_2 - 1$. Da er enhedsgruppen $O_K^\times$ direkte produkt af endelig cyklisk gruppe (af lige orden) bestående af enhedsrødderne i O_K og en fri abelsk gruppe af rang r.*

Eksempel 31. For $K = \mathbb{Q}$ er $r_1 = 1$, $r_2 = 0$, dvs. $r = 0$. Enhedsgruppen $O_K^\times = \{\pm 1\}$ består af enhedsrødderne i $O_K = \mathbb{Z}$.

Eksempel 32. For et imaginært kvadratisk tallegeme $K = \mathbb{Q}(\sqrt{D})$, hvor $D < 0$ og kvadratfri, er $r_1 = 0$, $r_2 = 1$, dvs. $r = 0$. Enhedsgruppen $O_K^\times$ består af enhedsrødderne i O_K. Der gælder

$$O_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{for} \quad D = -1 \\ \{\pm 1, \frac{1}{2}(\pm 1 \pm \sqrt{-3})\} & \text{for} \quad D = -3 \\ \{\pm 1\} & \text{ellers} \end{cases}$$

Dette følger af beviset for sætning 78 for $D \neq -1, -2, -3, -7, -11$, idet der blev vist, at $\{x \in O_K \mid N(x) < 4\} = \{0, \pm 1\}$. For de resterende fem værdier af D er det efter samme metode let at bestemme $O_K^\times = \{x \in O_K \mid N(x) = 1\}$.

Eksempel 33. For et reelt kvadratisk tallegeme $K = \mathbb{Q}(\sqrt{D})$, hvor $D > 1$ og kvadratfri, er $r_1 = 2$, $r_2 = 0$, dvs. $r = 1$. Da de eneste reelle enhedsrødder

er ± 1 er enhedsgruppen $O_K^\times$ derfor direkte produkt af $\{\pm 1\}$ og en uendelig cyklisk gruppe. For $D \equiv 2, 3 \pmod 4$ er $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}$, hvorfor

$$\begin{aligned} O_K^\times &= \{x + y\sqrt{D} \mid N(x + y\sqrt{D}) = \pm 1,\ x, y \in \mathbb{Z}\} \\ &= \{x + y\sqrt{D} \mid x^2 - Dy^2 = \pm 1,\ x, y \in \mathbb{Z}\}. \end{aligned}$$

Derfor kan enhederne i dette tilfælde fås ud fra løsningerne til den Pellske og ikke Pellske ligning.

Den praktiske bestemmelse af enhederne behandles nærmere i et senere eksempel.

Eksempel 34. For det kubiske tallegeme $K = \mathbb{Q}(\sqrt[3]{2})$, er $r_1 = 1$, $r_2 = 1$, dvs. $r = 1$ (jf eksempel 11). Til senere brug vil vi her vise, at

$$O_K = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}.$$

Lad $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a, b, c \in \mathbb{Q}$ være et vilkårligt element i O_K. Da er α's konjugerede givet ved

$$\alpha^{(2)} = a + b\zeta\sqrt[3]{2} + c\zeta^2\sqrt[3]{4},\ \alpha^{(3)} = a + b\zeta^2\sqrt[3]{2} + c\zeta\sqrt[3]{4},$$

hvor $\zeta = e^{2\pi i/3}$. Da $\zeta + \zeta^2 = -1$ giver en lille udregning, at

$$\begin{aligned} f(x) &= (x - \alpha)(x - \alpha^{(2)})(x - \alpha^{(3)}) \\ (*) \qquad &= x^3 - 3ax^2 + (3a^2 - 6bc)x - (a^3 + 2b^3 + 4c^3 - 6abc). \end{aligned}$$

Da $\alpha \in O_K$, er $f \in \mathbb{Z}[x]$. Specielt er $S(\alpha) = 3a \in \mathbb{Z}$. Da også $\sqrt[3]{2}\alpha,\ \sqrt[3]{4}\alpha \in O_K$, gælder derfor $6b, 6c \in \mathbb{Z}$. Elementet

$$6\alpha = A + B\sqrt[3]{2} + C\sqrt[3]{4} \quad \text{med} \quad A = 6a, B = 6b, C = 6c,$$

har derfor koefficienter $A, B, C \in \mathbb{Z}$, hvor

$$(**) \qquad 6 \,|\, 3A, \quad 6^2 \,|\, 3A^2 - 6BC, \quad 6^3 \,|\, A^3 + 2B^3 + 4C^3 - 6ABC.$$

Af den sidste relation i (**) følger successivt $2 \,|\, A$ (hvad vi allerede vidste), $2 \,|\, B$ og $2 \,|\, C$. Elementet

$$3\alpha = A' + B'\sqrt[3]{2} + C'\sqrt[3]{4} \quad \text{med} \quad A' = 3a, B' = 3b, C' = 3c,$$

har derfor koefficienter $A', B', C' \in \mathbb{Z}$, hvor

$$(***) \qquad 3 \,|\, 3A', \quad 3^2 \,|\, 3A'^2 - 6B'C', \quad 3^3 \,|\, A'^3 + 2B'^3 + 4C'^3 - 6A'B'C'.$$

Hvis $A' \equiv \pm 1 \pmod 3$, følger det af den anden relation i (***), at $B' \equiv -C' \equiv \pm 1 \pmod 3$. Den tredie relation i (***) kan derfor kun være opfyldt (modulo 3), hvis $A' \equiv C' \equiv -B' \pmod 3$. Sættes

$$A' = 3a' + s, \; B' = 3b' - s, \; C' = 3c' + s, \quad \text{hvor} \quad s \in \{\pm 1\},$$

bliver

$$A'^3 \equiv 9a' + s \pmod{27}, \; B'^3 \equiv 9b' - s \pmod{27}, \; C'^3 \equiv 9c' + s \pmod{27},$$

og

$$3A'B'C' \equiv -9(a' - b' + c') - 3s \pmod{27}.$$

Heraf følger imidlertid, at

$$A'^3 + 2B'^3 + 4C'^3 - 6A'B'C' \equiv 27a' + 54c' + 9s \equiv 9s \not\equiv 0 \pmod{27}.$$

Dette viser, at $3 \,|\, A'$. Men da følger af den anden relation i (***), at enten $3 \,|\, B'$ eller $3 \,|\, C'$. Den tredie relation i (***) viser derfor, at både $3 \,|\, B'$ og $3 \,|\, C'$. Dette viser påstanden.

I et senere eksempel vil vi vise, at

$$O_K^\times = \{\pm(\sqrt[3]{2} - 1)^n \mid n \in \mathbb{Z}\}.$$

Eksempel 35. For det kubiske tallegeme $K = \mathbb{Q}(2\cos(2\pi/7))$, er $r_1 = 3$, $r_2 = 0$, dvs. $r = 2$. Dette indses således: Cirkeldelingslegemet $\mathbb{Q}(e^{2\pi i/7})$ har grad 6, og minimalpolynomiet f for $\epsilon = e^{2\pi i/7}$ er givet ved $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, der har nulpunkterne $\epsilon^m, 1 \le m \le 6$. Da

$$\begin{aligned} f(x) &= x^3(x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-3}) \\ &= x^3((x + x^{-1})^3 + (x + x^{-1})^2 - 2(x + x^{-1}) - 1), \end{aligned}$$

har polynomiet $g(x) = x^3 + x^2 - 2x - 1$ nulpunkterne

$$\begin{aligned} &\vartheta^{(1)} = \epsilon + \epsilon^{-1} = 2\cos(2\pi/7), \; \vartheta^{(2)} = \epsilon^2 + \epsilon^{-2} = 2\cos(4\pi/7), \\ &\vartheta^{(3)} = \epsilon^3 + \epsilon^{-3} = 2\cos(6\pi/7). \end{aligned}$$

Da g er irreducibelt i $\mathbb{Q}[x]$, er g derfor minimalpolynomiet for $\vartheta^{(\nu)}$, $1 \leq \nu \leq 3$. Da

$$\vartheta^{(\nu+1)} = {\vartheta^{(\nu)}}^2 - 2, \quad \nu \pmod 3,$$

er $K^{(1)} = K^{(2)} = K^{(3)} = K$, hvor $K^{(\nu)} = \mathbb{Q}(\vartheta^{(\nu)})$. Dette viser, at K er normal over Q, og da $|\mathrm{Gal}K/\mathbb{Q}| = [K : \mathbb{Q}] = 3$ er $\mathrm{Gal}K/\mathbb{Q} \simeq C_3$. Af hensyn til et senere eksempel vil vi bestemme O_K og dermed diskriminanten d for K. Dertil udregnes først diskriminanten

$$D(1, \vartheta^{(1)}, {\vartheta^{(1)}}^2) = \det \begin{pmatrix} S(1) & S(\vartheta^{(1)}) & S({\vartheta^{(1)}}^2) \\ S(\vartheta^{(1)}) & S({\vartheta^{(1)}}^2) & S({\vartheta^{(1)}}^3) \\ S({\vartheta^{(1)}}^2) & S({\vartheta^{(1)}}^3) & S({\vartheta^{(1)}}^4) \end{pmatrix}.$$

Man finder nu

$$\begin{aligned} {\vartheta^{(1)}}^2 &= (\epsilon + \epsilon^{-1})^2 = \epsilon^2 + \epsilon^{-2} + 2 = \vartheta^{(2)} + 2, \\ {\vartheta^{(1)}}^3 &= (\epsilon + \epsilon^{-1})^3 = \epsilon^3 + \epsilon^{-3} + 3(\epsilon + \epsilon^{-1}) = \vartheta^{(3)} + 3\vartheta^{(1)}, \\ {\vartheta^{(1)}}^4 &= (\epsilon + \epsilon^{-1})^4 = \epsilon^4 + \epsilon^{-4} + 4(\epsilon^2 + \epsilon^{-2}) + 6 = \vartheta^{(3)} + 4\vartheta^{(2)} + 6. \end{aligned}$$

Af minimalpolynomiet g for $\vartheta^{(\nu)}$ aflæses (jf sætning 7), at $S(\vartheta^{(\nu)}) = -1$ for $1 \leq \nu \leq 3$. Da $S(1) = [K : \mathbb{Q}] = 3$ fås derfor fra de fundne formler for ${\vartheta^{(1)}}^2, {\vartheta^{(1)}}^3, {\vartheta^{(1)}}^4$:

$$S({\vartheta^{(1)}}^2) = 5, \ S({\vartheta^{(1)}}^3) = -4, \ S({\vartheta^{(1)}}^4) = 13.$$

Altså er

$$D(1, \vartheta^{(1)}, {\vartheta^{(1)}}^2) = \det \begin{pmatrix} 3 & -1 & 5 \\ -1 & 5 & -4 \\ 5 & -4 & 13 \end{pmatrix} = 49 = 7^2.$$

Da $1, \vartheta^{(1)}, {\vartheta^{(1)}}^2 \in O_K$ kan vi skrive

$$\begin{pmatrix} 1 \\ \vartheta^{(1)} \\ {\vartheta^{(1)}}^2 \end{pmatrix} = (c_{rs}) \begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}, \ c_{rs} \in \mathbb{Z},$$

hvor $(\omega_1, \omega_2, \omega_3)$ er en $\mathbb{Z}$-basis for O_K. Ifølge et tidligere resultat (jf side 1.10) er da

$$7^2 = D(1, \vartheta^{(1)}, {\vartheta^{(1)}}^2) = (\det(c_{rs}))^2 d,$$

hvor $d = D(\omega_1, \omega_2, \omega_3)$ er diskriminanten for K. Da $|d| > 1$ ifølge Dedekind's diskriminantsætning, er derfor $(\det(c_{rs}))^2 = 1$. Vi har derfor vist, at $d = 49$ og at $O_K = \mathbb{Z} + \mathbb{Z}\vartheta^{(1)} + \mathbb{Z}{\vartheta^{(1)}}^2$.

I et senere eksempel vil vi vise, at

$$O_K^\times = \{\pm {\vartheta^{(1)}}^{n_1} {\vartheta^{(2)}}^{n_2} \mid n_1,\ n_2 \in \mathbb{Z}\}.$$

I det følgende gøres en række forberedelser til beviset af Dirichlet's enhedssætning.

For det givne algebraiske tallegeme K vælges en frembringer ϑ, således at der for de konjugerede $\vartheta^{(\nu)}$ til ϑ, hvor $\vartheta = \vartheta^{(1)}$, gælder at

$$\vartheta^{(\nu)} \in \mathbb{R} \quad \text{for} \quad 1 \le \nu \le r_1,$$

$$\vartheta^{(\nu)} \in \mathbb{C} \setminus \mathbb{R} \quad \text{og} \quad \vartheta^{(r_1+\nu)} = \overline{\vartheta^{(r_1+r_2+\nu)}} \quad \text{for} \quad 1 \le \nu \le r_2,$$

og hvor $r_1 + 2r_2 = n$. Antallene r_1 og r_2, som ifølge bemærkning 2 kun afhænger af K, vil vi omtale som antallet af reelle indlejringer af K og antallet af par af komplekse indlejringer af K. Idet $K^* = \mathbb{Q}(\vartheta^{(1)}, \ldots, \vartheta^{(n)})$ betegner det normale hylster for K, vælges en gang for alle

$$\sigma_\nu \in \mathrm{Gal}(K^*/\mathbb{Q}) \quad \text{med} \quad \sigma_\nu(\vartheta) = \vartheta^{(\nu)} \quad \text{for} \quad 1 \le \nu \le n.$$

Vi betragter nu afbildningen

$$\varphi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n,$$

der er givet ved

$$\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)).$$

Det er hensigtsmæssigt for

$$x = (x_1, \ldots, x_{r_1+r_2}),\ y = (y_1, \ldots, y_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

at definere

$$\begin{aligned} x + y &= (x_1 + y_1, \ldots, x_{r_1+r_2} + y_{r_1+r_2}), \\ x \cdot y &= (x_1 y_1, \ldots, x_{r_1+r_2} y_{r_1+r_2}), \\ N(x) &= x_1 \cdots x_{r_1} |x_{r_1+1}|^2 \cdots |x_{r_1+r_2}|^2. \end{aligned}$$

Da $\sigma_1, \ldots, \sigma_{r_1+r_2}$ er isomorfier, gælder

$$\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta),\ \varphi(\alpha\beta) = \varphi(\alpha)\cdot\varphi(\beta), \quad \text{for} \quad \alpha, \beta \in K.$$

Endvidere er

$$N(\alpha) = \prod_{\nu=1}^{r_1} \sigma_\nu(\alpha) \prod_{\nu=r_1+1}^{r_1+r_2} |\sigma_\nu(\alpha)|^2 = N(\varphi(\alpha)) \quad \text{for} \quad \alpha \in K.$$

Da hver af afbildningerne $\sigma_\nu,\ 1 \le \nu \le r_1+r_2$, er injektive afbildninger af K, er $\varphi : K \to \mathbb{R}^n$ en injektiv afbildning. Vi vil kalde $\varphi(K)$ *den naturlige indlejring* af K i $\mathbb{R}^n$. Ved *den naturlige* $\mathbb{R}$*-basis* for $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ forstås $(e_1, \ldots, e_n)$, hvor

$$\begin{aligned}
e_1 &= (1, 0, \ldots, 0, 0, 0, \ldots, 0),\\
&\vdots\\
e_{r_1} &= (0, 0, \ldots, 1, 0, 0, \ldots, 0),\\
e_{r_1+1} &= (0, 0, \ldots, 0, 1, 0, \ldots, 0),\\
e_{r_1+2} &= (0, 0, \ldots, 0, i, 0, \ldots, 0),\\
&\vdots\\
e_{n-1} &= (0, 0, \ldots, 0, 0, 0, \ldots, 1),\\
e_n &= (0, 0, \ldots, 0, 0, 0, \ldots, i).
\end{aligned}$$

Lad nu $(\omega_1, \ldots, \omega_n)$ være en $\mathbb{Z}$-basis for O_K. Da er (for $1 \le \nu \le n$):

$$\begin{aligned}
\varphi(\omega_\nu) =& (\sigma_1(\omega_\nu), \ldots, \sigma_{r_1}(\omega_\nu),\\
& \tfrac{1}{2}(\sigma_{r_1+1}(\omega_\nu) + \sigma_{r_1+r_2+1}(\omega_\nu)) + \tfrac{1}{2}(\sigma_{r_1+1}(\omega_\nu) - \sigma_{r_1+r_2+1}(\omega_\nu)),\\
& \ldots, \tfrac{1}{2}(\sigma_{r_1+r_2}(\omega_\nu) + \sigma_{r_1+2r_2}(\omega_\nu)) + \tfrac{1}{2}(\sigma_{r_1+r_2}(\omega_\nu) - \sigma_{r_1+2r_2}(\omega_\nu))),
\end{aligned}$$

dvs.

$$\begin{pmatrix} \varphi(\omega_1) \\ \vdots \\ \varphi(\omega_n) \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \quad \text{med} \quad c_{rs} \in \mathbb{R}.$$

Her er

$$\det(c_{rs}) =$$

$$\begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_{r_1}(\omega_1) & \frac{\sigma_{r_1+1}(\omega_1)+\sigma_{r_1+r_2+1}(\omega_1)}{2} & \frac{\sigma_{r_1+1}(\omega_1)-\sigma_{r_1+r_2+1}(\omega_1)}{2i} & \dots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots \\ \sigma_1(\omega_\nu) & \dots & \sigma_{r_1}(\omega_\nu) & \frac{\sigma_{r_1+1}(\omega_\nu)+\sigma_{r_1+r_2+1}(\omega_\nu)}{2} & \frac{\sigma_{r_1+1}(\omega_\nu)-\sigma_{r_1+r_2+1}(\omega_\nu)}{2i} & \dots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots \\ \sigma_1(\omega_n) & \dots & \sigma_{r_1}(\omega_n) & \frac{\sigma_{r_1+1}(\omega_n)+\sigma_{r_1+r_2+1}(\omega_n)}{2} & \frac{\sigma_{r_1+1}(\omega_n)-\sigma_{r_1+r_2+1}(\omega_n)}{2i} & \dots \end{vmatrix}$$

$$= \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_{r_1}(\omega_1) & \sigma_{r_1+1}(\omega_1) & -\frac{1}{2i}\sigma_{r_1+r_2+1}(\omega_1) & \dots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots \\ \sigma_1(\omega_\nu) & \dots & \sigma_{r_1}(\omega_\nu) & \sigma_{r_1+1}(\omega_\nu) & -\frac{1}{2i}\sigma_{r_1+r_2+1}(\omega_\nu) & \dots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots \\ \sigma_1(\omega_n) & \dots & \sigma_{r_1}(\omega_n) & \sigma_{r_1+1}(\omega_n) & -\frac{1}{2i}\sigma_{r_1+r_2+1}(\omega_n) & \dots \end{vmatrix}$$

$$= (\tfrac{i}{2})^{r_2} \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_{r_1}(\omega_1) & \sigma_{r_1+1}(\omega_1) & \sigma_{r_1+r_2+1}(\omega_1) & \dots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots \\ \sigma_1(\omega_\nu) & \dots & \sigma_{r_1}(\omega_\nu) & \sigma_{r_1+1}(\omega_\nu) & \sigma_{r_1+r_2+1}(\omega_\nu) & \dots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots \\ \sigma_1(\omega_n) & \dots & \sigma_{r_1}(\omega_n) & \sigma_{r_1+1}(\omega_n) & \sigma_{r_1+r_2+1}(\omega_n) & \dots \end{vmatrix}.$$

Heraf følger (jf beviset for Dedekind's diskriminantsætning), at

$$|\det(c_{rs})| = 2^{-r_2}\sqrt{|d|} > 0.$$

Altså er $\Lambda = \varphi(O_K)$ et fuldt gitter i $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ med gitterdeterminant

$$d(\Lambda) = 2^{-r_2}\sqrt{|d|}.$$

Sætning 82. *En delmængde $\Lambda \subseteq \mathbb{R}^n$, $\Lambda \neq \emptyset$, er et gitter $\Leftrightarrow$ Λ har følgende egenskaber:*

(i) Λ er en undergruppe i $(\mathbb{R}^n, +)$.

(ii) Λ *er en diskret delmængde af* $\mathbb{R}^n$.

Bevis. $\Rightarrow$: Lad $\Lambda = \mathbb{Z}\underline{e}_1 + \cdots + \mathbb{Z}\underline{e}_l$, hvor $(\underline{e}_1, \ldots, \underline{e}_l)$ er et lineært uafhængigt sæt i $\mathbb{R}^n$. Begge egenskaber er opfyldt for $l = 0$, idet $\Lambda = \{\underline{0}\}$. Antag derfor, at $1 \leq l \leq n$. Det er klart, at Λ opfylder (i). For at vise (ii) er det tilstrækkeligt at vise, at enhver n-dimensional kugle $\{\underline{y} \in \mathbb{R}^n \mid \|y\| < R\}$ kun indeholder endeligt mange gitterpunkter. Betragt funktionen $f : \mathbb{R}^l \to \mathbb{R}$ givet ved

$$\begin{aligned} f(x_1, \ldots, x_l) =& \|x_1\underline{e}_1 + \cdots + x_l\underline{e}_l\|^2 = (x_1\underline{e}_1 + \cdots + x_l\underline{e}_l) \cdot (x_1\underline{e}_1 + \cdots + x_l\underline{e}_l) \\ =& \sum_{i,j=1}^{l} \underline{e}_i \cdot \underline{e}_j x_i x_j. \end{aligned}$$

Da $S = \{(x_1, \ldots, x_l) \in \mathbb{R}^l \mid {x_1}^2 + \cdots + {x_l}^2 = 1\}$ er en kompakt delmængde af $\mathbb{R}^l$, og

$$f(x_1, \ldots, x_l) = 0 \Leftrightarrow x_1\underline{e}_1 + \cdots + x_l\underline{e}_l = \underline{0} \Leftrightarrow x_1 = \cdots = x_l = 0,$$

er

$$M = \min_{(x_1,\ldots,x_l)\in S} f(x_1, \ldots, x_l) > 0.$$

For $(n_1, \ldots, n_l) \in \mathbb{Z}^l \setminus \{(0, \ldots, 0)\}$ er derfor

$$\begin{aligned} f(n_1, \ldots, n_l) =& ({n_1}^2 + \cdots + {n_l}^2) f\left(\frac{n_1}{\sqrt{{n_1}^2 + \cdots + {n_l}^2}}, \ldots, \frac{n_l}{\sqrt{{n_1}^2 + \cdots + {n_l}^2}}\right) \\ \geq& ({n_1}^2 + \cdots + {n_l}^2)M. \end{aligned}$$

Heraf følger, at der kun er endeligt mange gitterpunkter $n_1\underline{e}_1 + \cdots + n_l\underline{e}_l$ med

$$\|n_1\underline{e}_1 + \cdots + n_l\underline{e}_l)\|^2 = f(n_1, \ldots, n_l) < R^2.$$

$\Leftarrow$: Lad $\Lambda \neq \emptyset$ tilfredsstille (i) og (ii). Lad $L = \mathrm{span}_{\mathbb{R}}\Lambda$ og $l = \dim_{\mathbb{R}} L$. Hvis $l = 0$, er $\Lambda = \{\underline{0}\}$ et gitter (med tom basis). For $l > 0$ vælges l lineært uafhængige vektorer $\underline{e}_1, \ldots, \underline{e}_l \in \Lambda$. Sæt $\Lambda_0 = \mathbb{Z}\underline{e}_1 + \cdots + \mathbb{Z}\underline{e}_l$, og lad

$$\mathcal{P}_0 = \{x_1\underline{e}_1 + \cdots + x_l\underline{e}_l \mid 0 \leq x_i < 1 \quad \text{for} \quad 1 \leq i \leq l\}.$$

Det er klart, at Λ_0 er en undergruppe i Λ, og at undergruppe index

$$j = [\Lambda : \Lambda_0] = |\mathcal{P}_0 \cap \Lambda| < \infty,$$

da $\mathcal{P}_0$ er begrænset, og Λ er diskret. Heraf følger, at $j\Lambda \subseteq \Lambda_0$, altså at $\Lambda \subseteq \frac{1}{j}\Lambda_0$. Af elementardivisorsætningen følger nu, at Λ og $\frac{1}{j}\Lambda_0$ har $\mathbb{Z}$-baser $(\varphi_1, \ldots, \varphi_m)$ og $(\omega_1, \ldots, \omega_l)$, hvor $m \leq l$, og $\phi_i = \epsilon_i \omega_i$, $\epsilon_i \in \mathbb{N}$ for $1 \leq i \leq m$. Da $\dim \operatorname{span}_{\mathbb{R}} \Lambda = \dim \operatorname{span}_{\mathbb{R}} \Lambda_0 = l$, er $m = l$, og $(\varphi_1, \ldots, \varphi_l)$ er en gitterbasis for Λ. □

Sætning 83. *Lad K være et algebraisk tallegeme af grad $n = [K : \mathbb{Q}]$. Da indeholder O_K kun endeligt mange ikke associerede elementer af en given norm.*

Bevis. Lad $m \in \mathbb{N},\ m > 1$, og antag, at $\alpha, \beta \in O_K$ opfylder

$$\alpha \equiv \beta \pmod{mO_K} \quad \text{og} \quad |N(\alpha)| = |N(\beta)| = m.$$

Da $\alpha^{(1)} \cdots \alpha^{(n)} = N(\alpha)$, vil (jf beviset for sætning 80) $\alpha = \alpha^{(1)} \,|\, N(\alpha)$, altså $\alpha \,|\, m = |N(\alpha)|$ (inden for O_K). Tilsvarende gælder $\beta \,|\, m$. På den anden side er $\alpha - \beta = m\gamma$, hvor $\gamma \in O_K$. Altså følger at $\alpha \,|\, \beta$ og $\beta \,|\, \alpha$, dvs. α og β er associerede. Argumentet viser derfor, at der højst er $|O_K/(mO_K)| = m^n$ ikke associerede elementer i O_K af norm $\pm m$. Da der for $m \in \{0, \pm 1\}$ højst er én associeretklasse af elementer af norm m (jf sætning 80), er sætningen bevist. □

Sætning 84. *Lad K være et algebraisk tallegeme af grad $n = [K : \mathbb{Q}]$ og diskriminant d, og lad $\varphi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ være den naturlige indlejring af K. Lad*

$$\mathcal{S} = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |N(x)| = 1\}.$$

Da findes en begrænset delmængde $\mathcal{S}_0 \subseteq \mathcal{S}$, så at

$$\mathcal{S} = \bigcup_{\epsilon \in O_K^\times} \varphi(\epsilon) \cdot \mathcal{S}_0.$$

Bevis. Ifølge sætning 80 gælder

$$\epsilon \in O_K^\times \Leftrightarrow \epsilon \in O_K \quad \text{og} \quad |N(\epsilon)| = 1,$$

og da $N(\varphi(\epsilon)) = N(\epsilon)$, er derfor

$$\varphi(O_K^\times) = \varphi(O_K) \cap \mathcal{S}.$$

Når $\epsilon \in O_K^\times$ følger heraf, at restriktionen til $\mathcal{S}$ af afbildningen af $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ på sig selv givet ved $x \mapsto \varphi(\epsilon) \cdot x$ er en bijektiv afbildning af $\mathcal{S}$. På denne måde opererer enhedsgruppen $O_K^\times$ på fladen $\mathcal{S} \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Betragt nu mængden

$$\mathcal{K} = \left\{x = (x_1, \dots, x_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_1| < c_1, \dots, |x_{r_1+r_2}|^2 < c_{r_1+r_2}\right\},$$

hvor $c_1, \dots, c_{r_1+r_2}$ er positive konstanter. Opfattet som delmængde af $\mathbb{R}^n$ er $\mathcal{K}$ åbenbart konveks og symmetrisk om $\underline{0}$. Endvidere er volumenet af $\mathcal{K}$ givet ved

$$v(\mathcal{K}) = 2c_1 \cdots 2c_{r_1} \pi c_{r_1+1} \cdots \pi c_{r_1+r_2} = 2^{r_1} \pi^{r_2} \prod_1^{r_1+r_2} c_j.$$

Antager vi nu, at $c_1, \dots, c_{r_1+r_2}$ er valgt, så at

$$Q = \prod_1^{r_1+r_2} c_j > (\tfrac{2}{\pi})^{r_2} \sqrt{|d|},$$

da bliver

$$(*) \qquad v(\mathcal{K}) = 2^{r_1} \pi^{r_2} \prod_1^{r_1+r_2} c_j > 2^{r_1+r_2} \sqrt{|d|} = 2^n d(\Lambda),$$

idet $\Lambda = \varphi(O_K)$ ifølge en tidligere beregning har gitterdeterminant $d(\Lambda) = 2^{-r_2}\sqrt{|d|}$.

For hvert $y \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ er $x \mapsto y \cdot x$ en $\mathbb{R}$-lineær afbildning af $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ ind i sig selv af determinant $N(y)$. Dette ses ved at betragte $(y \cdot \underline{e}_1, \dots, y \cdot \underline{e}_n)$. For $y \in \mathcal{S}$ er derfor $y \cdot \Lambda$ et gitter i $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ af determinant $d(y \cdot \Lambda) = d(\Lambda)$.

Ifølge Minkowski's gitterpunktsætning findes ifølge (*) for hvert $y \in \mathcal{S}$ et gitterpunkt $x_y \in \Lambda \setminus \{\underline{0}\}$, så at $y \cdot x_y \in \mathcal{K}$. Der gælder da

$$0 < |N(x_y)| = |N(y)||N(x_y)| = |N(y \cdot x_y)| < \prod_1^{r_1+r_2} c_j = Q.$$

Ifølge sætning 83 findes $\alpha_1, \dots, \alpha_N \in O_K$, så at ethvert $\alpha \in O_K$ med $0 < |N(\alpha)| < Q$ er associeret med et α_ν, $1 \le \nu \le N$. Dette betyder, at hvert x_y er af formen

$$x_y = \varphi(\alpha_\nu \epsilon^{-1}), \quad \text{hvor} \quad 1 \le \nu \le N,\ \epsilon \in O_K^\times.$$

Sætter vi nu

$$\mathcal{S}_0 = \left(\bigcup_{\nu=1}^{N} \varphi({\alpha_\nu}^{-1}) \cdot \mathcal{K} \right) \cap \mathcal{S},$$

er $\mathcal{S}_0$ en begrænset delmængde af $\mathcal{S}$, og for hvert $y \in \mathcal{S}$ findes et x_y og dermed et $\nu \in [1, N]$ og et $\epsilon \in O_K^\times$, så at

$$y \in x_y^{-1} \cdot \mathcal{K} = \varphi({\alpha_\nu}^{-1}) \cdot \varphi(\epsilon) \cdot \mathcal{K}.$$

Dette viser, at

$$\mathcal{S} = \bigcup_{\epsilon \in O_K^\times} \varphi(\epsilon) \cdot \mathcal{S}_0,$$

hvormed sætningen er bevist. □

Vi betragter nu

$$(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid N(x) \neq 0\},$$

dvs. den multiplikative gruppe af invertible elementer (ved $\cdot$) i $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Lad $l : (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \to \mathbb{R}^{r_1+r_2}$ være givet ved

$$l(x) = (l_1(x), \cdots, l_{r_1+r_2}(x)),$$

hvor

$$l_j(x) = \begin{cases} \log|x_j| & \text{for} \quad 1 \leq j \leq r_1 \\ 2\log|x_j| & \text{for} \quad r_1 + 1 \leq j \leq r_1 + r_2 \end{cases}$$

Det er klart, at l er surjektiv, og at l er en homomorfi af $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ på $(\mathbb{R}^{r_1+r_2}, +)$.

Den sammensatte afbildning $L = l \circ \varphi : K^\times \to (\mathbb{R}^{r_1+r_2}, +)$ er da givet ved

$$L(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \ldots, 2\log|\sigma_{r_1+r_2}(\alpha)|).$$

Afbildningen $L = l \circ \varphi : K^\times \to (\mathbb{R}^{r_1+r_2}, +)$, der kaldes *den logaritmiske afbildning*, er ligeledes en homomorfi. Idet $L(\alpha) = (L_1(\alpha), \ldots, L_{r_1+r_2}(\alpha))$ gælder for $\alpha \in K^\times$:

$$\sum_{j=1}^{r_1+r_2} L_j(\alpha) = \log|\sigma_1(\alpha) \cdots \sigma_{r_1}(\alpha)|\sigma_{r_1+1}(\alpha)|^2 \cdots |\sigma_{r_1+r_2}(\alpha)|^2| = \log|N(\alpha)|.$$

For $\epsilon \in O_K^\times$ gælder derfor

$$\sum_{j=1}^{r_1+r_2} L_j(\epsilon) = 0.$$

Vi har derfor vist, at $L(O_K^\times)$ er indeholdt i hyperplanen Π, hvor

$$\Pi = \{(\lambda_1, \dots, \lambda_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \mid \lambda_1 + \cdots + \lambda_{r_1+r_2} = 0\},$$

og at restriktionen af L til $O_K^\times$ er en homomorfi ind i $(\Pi, +)$.

Sætning 85. *Lad K være et algebraisk tallegeme af grad $n = [K : \mathbb{Q}]$, og lad $L : O_K^\times \to \Pi$ være den logaritmiske afbildning. Da gælder:*

(i) Kernen $\ker L$ = mængden af enhedsrødder i $O_K^\times$ = mængden af torsionselementer i $O_K^\times$. Gruppen $(\ker L, \cdot)$ er en endelig cyklisk gruppe af lige orden.

(ii) Billedmængden $L(O_K^\times)$ er et fuldt gitter i Π af dimension $r = r_1 + r_2 - 1$.

Bevis. (i) Det bemærkes først, at de to karakteriseringer af $\ker L$ er ensbetydende, da en enhedsrod og et element af endelig orden i $O_K^\times$ er det samme.

Antag først, at $\epsilon \in O_K^\times$ er en enhedsrod, dvs. der findes et $m \in \mathbb{N}$, så at $\epsilon^m = 1$. Da gælder

$$(\sigma_j(\epsilon))^m = \sigma_j(1) = 1 \Rightarrow |\sigma_j(\epsilon)| = 1 \quad \text{for} \quad 1 \le j \le r_1 + r_2,$$

hvorfor $L(\epsilon) = (0, \dots, 0)$, altså $\epsilon \in \ker L$.

Antag omvendt, at $\epsilon \in \ker L$, dvs. $\epsilon \in O_K^\times$ og $|\sigma_j(\epsilon)| = 1$ for $1 \le j \le r_1 + r_2$. Dette viser, at punkterne $\varphi(\epsilon) = (\sigma_1(\epsilon), \dots, \sigma_{r_1+r_2}(\epsilon))$ ligger i en begrænset del af gitteret $\Lambda = \varphi(O_K) \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Ifølge sætning 82 (den lette del) er der kun endelig mange muligheder for $\varphi(\epsilon)$ og dermed for ϵ. Dette viser, at $\ker L$ er endelig multiplikativ gruppe. Da $-1 \in O_K^\times$ har orden 2, er $|\ker L|$ lige. At $(\ker L, \cdot)$ er cyklisk, følger af det velkendte resultat, at enhver endelig undergruppe af $K^\times$ er cyklisk, når K er et (kommutativt) legeme (jf. eksempel 10). Dette viser (i).

(ii). For at vise, at $L(O_K^\times)$ er et gitter i Π benyttes igen sætning 82 (den svære del). Da $L(O_K^\times)$ er en undergruppe i $(\Pi, +)$, er det tilstrækkeligt at vise diskretheden, dvs. at enhver mængde

$$\mathcal{B} = \mathcal{B}(c) = \{(\lambda_1, \dots, \lambda_{r_1+r_2}) \mid |\lambda_j| < c,\ \lambda_1 + \cdots + \lambda_{r_1+r_2} = 0\},$$

hvor $c > 0$ er en vilkårlig konstant, kun indeholder endeligt mange punkter fra $L(O_K^\times)$. Imidlertid er

$$l^{-1}(\mathcal{B}) \subseteq \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_1| < e^c, \ldots, |x_{r_1+r_2}| < e^{c/2}\},$$

der er en begrænset delmængde af $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Da $\Lambda = \varphi(O_K)$ er et (fuldt) gitter i $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$, er der kun endeligt mange $\alpha \in O_K$ med $\varphi(\alpha) \in l^{-1}(\mathcal{B})$. Specielt er der kun endeligt mange $\alpha \in O_K^\times$ med $\varphi(\alpha) \in l^{-1}(\mathcal{B})$. Dette viser det ønskede, nemlig at $|L(O_K^\times) \cap \mathcal{B}| < \infty$.

For sluttelig at vise, at $L(O_K^\times)$ er et fuldt (dvs. $r_1 + r_2 - 1$–dimensionalt) gitter i Π, bemærkes først, at $l(\mathcal{S}) = \Pi$, idet

$$x \in \mathcal{S} \Leftrightarrow |N(x)| = 1 \Leftrightarrow \sum_{j=1}^{r_1+r_2} l_j(x) = \log|N(x)| = 0 \Leftrightarrow l(x) \in \Pi.$$

Lad $\Pi_0 = l(\mathcal{S}_0)$, hvor $\mathcal{S}_0$ er en begrænset delmængde af $\mathcal{S}$, som opfylder sætning 84. Da findes en konstant $c > 0$, så at ethvert $x = (x_1, \ldots, x_{r_1+r_2}) \in \mathcal{S}_0$ har $|x_j| < c$ for $1 \leq j \leq r_1 + r_2$. Da tillige

$$\prod_{j=1}^{r_1} |x_j| \prod_{j=r_1+1}^{r_1+r_2} |x_j|^2 = 1,$$

må der også gælde $|x_j| > c^{-n+1}$ for $1 \leq j \leq r_1 + r_2$, når $x \in \mathcal{S}_0$. Men dette viser, at $\Pi_0 = l(\mathcal{S}_0)$ er en begrænset delmængde af Π.

Ifølge sætning 84 er

$$\mathcal{S} = \bigcup_{\epsilon \in O_K^\times} \varphi(\epsilon) \cdot \mathcal{S}_0,$$

hvorfor der tilsvarende (efter anvendelse af l) må gælde

$$\Pi = \bigcup_{\epsilon \in O_K^\times} (L(\epsilon) + \Pi_0).$$

Dette betyder, at den begrænsede delmængde Π_0 ved at underkastes alle gittertranslationer fra gitteret $L(O_K^\times) \subseteq \Pi$ giver en overdækning af Π. Men heraf følger, at $L(O_K^\times)$ nødvendigvis er et fuldt gitter i Π. □

Bevis for sætning 81. Ifølge sætning 85 er $O_K^\times / \ker L$ en fri gruppe af rang $r = r_1 + r_2 - 1$, og $\ker L$ er undergruppen af $O_K^\times$ bestående af alle enhedsrødder i $O_K^\times$. Dette viser Dirichlet's enhedssætning. □

Bemærkning. Ifølge Dirichlet's enhedssætning findes en enhedsrod $\zeta \in O_K^\times$ og enheder $\epsilon_1, \ldots, \epsilon_r$, hvor $r = r_1 + r_2 - 1$, så at enhver enhed $\epsilon \in O_K^\times$ på en og kun en måde kan skrives på formen

$$\epsilon = \zeta^l \epsilon_1^{n_1} \cdots \epsilon_r^{n_r},$$

hvor $l \in \{0, 1, \ldots, w-1\}$, og $n_1, \ldots, n_r \in \mathbb{Z}$. Her betegner w ordenen af undergruppen af enhedsrødder i $O_K^\times$. Et sæt enheder af denne type kaldes et sæt af *fundamentalenheder* for $O_K^\times$.

Da de eneste reelle enhedsrødder er $\{\pm 1\}$, er $w = 2$ for alle algebraiske tallegemer K med $r_1 > 0$. Med andre ord: $w > 2$ kan kun forekomme for algebraiske tallegemer K, hvor $n = 2r_2$ (og $r_1 = 0$), såkaldt *totalt imaginære* algebraiske tallegemer. Vigtige eksempler på sådanne algebraiske tallegemer er – udover de imaginært kvadratiske tallegemer (hvor $w = 2$ pånær i de to tilfælde: $\mathbb{Q}(i)$ med $w = 4$ og $\mathbb{Q}(\sqrt{-3})$ med $w = 6$) – cirkeldelingslegemer $\mathbb{Q}(e^{2\pi i/n})$, $n \geq 3$.

Bestemmelse af enheder. I det følgende vil vi give nogle eksempler på bestemmelse af enheder i et algebraisk tallegeme. Cirkeldelingslegemer vil blive behandlet i kapitel 4.

Eksempel 36. For et reelt kvadratisk tallegeme $K = \mathbb{Q}(\sqrt{D})$, hvor $D > 1$ og kvadratfri, er (jf eksempel 33) $r_1 = 2, r_2 = 0$, dvs. $r = 1$. Ifølge bemærkningen ovenfor er $w = 2$, og følgelig er

$$O_K^\times = \{\pm\epsilon^n \mid n \in \mathbb{Z}\},$$

hvor ϵ er en fundamentalenhed. Når ϵ er en fundamentalenhed, er også ϵ^{-1}, $-\epsilon$, $-\epsilon^{-1}$ det - og ingen andre enheder. Der findes derfor en entydigt bestemt fundamentalenhed $\epsilon > 1$.

For $D \equiv 2, 3 \pmod 4$ er (jf. eksempel 33) $\epsilon = a + b\sqrt{D} \in O_K^\times$, hvis og kun hvis (a, b) er en heltalsløsning til ligningen

$$N(x + y\sqrt{D}) = x^2 - Dy^2 = \pm 1,$$

dvs. til den *Pell'ske* eller *ikke–Pell'ske ligning.*

En systematisk metode til bestemmelse af en fundamentalenhed $\epsilon > 1$ beror på udvikling af $\sqrt{D}$ i en regulær kædebrøk:

$$\sqrt{D} = [a_0, a_1, a_2, \ldots], \ a_i \in \mathbb{N}.$$

Denne kædebrøk er periodisk med forperiode a_0:

$$\sqrt{D} = [a_0, \overline{a_1, \dots, a_k}],$$

og når $k \in \mathbb{N}$ er den korteste periode, giver konvergenten

$$\frac{p_{k-1}}{q_{k-1}} = [a_0, a_1, \dots, a_{k-1}]$$

den ønskede fundamentalenhed $\epsilon = p_{k-1} + q_{k-1}\sqrt{D} > 1$, forudsat konvergenten er skrevet på uforkortelig form med positiv nævner (og tæller). Hvis k er lige, har den ikke–Pell'ske ligning ingen løsning, dvs. $N(\epsilon) = 1$, i hvilket tilfælde, der ikke findes enheder af norm -1. Hvis k er ulige, er den ikke–Pells'ske ligning løsbar, og $N(\epsilon) = -1$.

For $D = 6$ er $\sqrt{6} = [2, \overline{2, 4}]$, dvs. $k = 2$ er lige. Svarende til $2 + \frac{1}{2} = \frac{5}{2}$ fås fundamentalenheden $\epsilon = 5 + 2\sqrt{6}$, der har $N(\epsilon) = 1$. Der findes ingen enheder med norm -1 (= den ikke–Pell'ske ligning har ingen løsninger).

For $D \equiv 1 \pmod 4$ er (jf. sætning 80) $\epsilon = a + b\frac{1}{2}(1 + \sqrt{D}) \in O_K^\times$, hvis og kun hvis (a, b) er en heltalsløsning til ligningen

$$(*) \qquad N(x + y\tfrac{1}{2}(1 + \sqrt{D})) = x^2 + xy + \tfrac{1}{4}(1 - D)y^2 = \pm 1.$$

En systematisk metode til bestemmelse af en fundamentalenhed $\epsilon > 1$ beror på udvikling af $\frac{1}{2}(-1 + \sqrt{D})$ i en regulær kædebrøk:

$$\tfrac{1}{2}(-1 + \sqrt{D}) = [a_0, a_1, a_2, \dots], \ a_i \in \mathbb{N}.$$

Denne kædebrøk er periodisk med forperiode a_0:

$$\tfrac{1}{2}(-1 + \sqrt{D}) = [a_0, \overline{a_1, \dots, a_k}],$$

og når $k \in \mathbb{N}$ er den korteste periode, giver konvergenten

$$\frac{p_{k-1}}{q_{k-1}} = [a_0, a_1, \dots, a_{k-1}]$$

den ønskede fundamentalenhed $\epsilon = p_{k-1} + q_{k-1}\frac{1}{2}(1 + \sqrt{D}) > 1$, forudsat konvergenten er skrevet på uforkortelig form med positiv nævner (og tæller). Hvis k er lige, har ligningen (*) ingen løsning, når højre side er -1, dvs. $N(\epsilon) = 1$,

i hvilket tilfælde, der ikke findes enheder af norm -1. Hvis k er ulige, er ligningen (*) løsbar, når højre side er -1, og $N(\epsilon) = -1$.

For $D = 61$ er $\frac{1}{2}(-1+\sqrt{61}) = [3, \overline{2, 2, 7}]$, dvs. $k = 3$ er ulige. Svarende til $3+1/(2+\frac{1}{2}) = \frac{17}{5}$ fås fundamentalenheden $\epsilon = 17+\frac{5}{2}(1+\sqrt{61}) = \frac{1}{2}(39+5\sqrt{61})$, der har $N(\epsilon) = -1$.

Eksempel 37. For $K = \mathbb{Q}(\sqrt[3]{2})$ er (jf eksempel 34) $r = 1$ og $O_K = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}$. Følgelig er

$$(*) \qquad O_K^\times = \{\pm\epsilon^n \mid n \in \mathbb{Z}\},$$

hvor ϵ er en fundamentalenhed. Ved om fornødent at erstatte ϵ med $-\epsilon$, $\epsilon^{-1}, -\epsilon^{-1}$ kan vi gerne antage, at $\epsilon \in]0, 1[$. Da $\epsilon_0 = \sqrt[3]{2} - 1 \in O_K$ har minimalpolynomiet f_0, hvor

$$f_0(x) = (x+1)^3 - 2 = x^3 + 3x^2 + 3x - 1,$$

fremgår det (jf sætning 7), at $N(\epsilon_0) = 1$, så at $\epsilon_0 \in O_K^\times$. Da $\epsilon_0 = 0.2599\cdots \in]0, 1[$ følger det af (*), at der findes et $l \in \mathbb{N}$, så at $\epsilon_0 = \epsilon^l$. Antag nu (indirekte), at $\epsilon_0 \neq \epsilon$, dvs. $l \geq 2$. Da er

$$\epsilon = \epsilon_0^{1/l} \geq \epsilon_0^{1/2} > \tfrac{1}{2},$$

dvs. $\epsilon \in]\frac{1}{2}, 1[$. Lad $\epsilon's$ konjugerede være $\epsilon^{(2)}, \epsilon^{(3)} = \overline{\epsilon^{(2)}}$. Da er minimalpolynomiet f for ϵ givet ved

$$f(x) = x^3 - s_1x^2 + s_2x - s_3 \in \mathbb{Z}[x],$$

hvor

$$\begin{aligned} s_1 &= \epsilon + \epsilon^{(2)} + \overline{\epsilon^{(2)}} = S(\epsilon), \\ s_2 &= \epsilon(\epsilon^{(2)} + \overline{\epsilon^{(2)}}) + \epsilon^{(2)}\overline{\epsilon^{(2)}}, \\ s_3 &= \epsilon\epsilon^{(2)}\overline{\epsilon^{(2)}} = N(\epsilon). \end{aligned}$$

Da $\epsilon > 0$, er $N(\epsilon) > 0$, altså $N(\epsilon) = 1$. Da videre $|\epsilon^{(2)}| = \epsilon^{-1/2} < \sqrt{2}$, er derfor på den ene side

$$-3 < -2\sqrt{2} + \tfrac{1}{2} < s_1 < 1 + 2\sqrt{2} < 4,$$

altså $s_1 \in [-2,3]$. På den anden side er

$$\epsilon = a + b\sqrt[3]{2} + \sqrt[3]{4}, \quad \text{med} \quad a,b,c \in \mathbb{Z},$$

hvorfor

$$s_1 = S(\epsilon) = 3a \equiv 0 \pmod 3.$$

Tilsammen viser dette, at $s_1 \in \{0,3\}$. Vi betragter dernæst

$$s_2 = g(\epsilon) \quad \text{med} \quad g(x) = x(s_1 - x) + x^{-1}.$$

Da

$$g'(x) = s_1 - 2x - x^{-2},\ g''(x) = -2 + 2x^{-3},$$

er $g''(x) > 0$ for $x \in\ [\frac{1}{2}, 1[$. Altså er g' voksende i $[\frac{1}{2}, 1[$, hvorfor

$$g'(x) < g'(1) = s_1 - 3 \leq 0 \quad \text{for} \quad x \in\ [\tfrac{1}{2}, 1[.$$

Følgelig er g aftagende i $[\frac{1}{2}, 1]$, hvorfor

$$s_1 = g(1) < g(x) < g(\tfrac{1}{2}) = \tfrac{1}{2}s_1 + \tfrac{7}{4} \quad \text{for} \quad x \in\ ]\tfrac{1}{2}, 1[.$$

Specielt er derfor

$$(**) \qquad s_1 < s_2 = g(\epsilon) < \tfrac{1}{2}s_1 + \tfrac{7}{4}.$$

Hvis $s_1 = 3$, skulle $s_2 \in\ ]3, \frac{13}{4}[$ ifølge (**), hvilket er en modstrid, da $s_2 \in \mathbb{Z}$. Derfor er $s_1 = 0$ og dermed $s_2 = 1$ ifølge (**), dvs. $f(x) = x^3 + x - 1$. Da f er voksende i $[\frac{1}{2}, 1]$, og $f(\frac{1}{2}) < 0 < f(1)$, har f præcist et nulpunkt i $]\frac{1}{2}, 1[$. En nærmere udregning af dette nulpunkt viser derfor, at den eneste mulighed for ϵ er $\epsilon = 0.68\cdots$. Imidlertid er da

$$\epsilon^4 < 0.7^4 < 0.25 < \epsilon_0 < 0.3 < 0.68^3 < \epsilon^3,$$

hvorfor

$$\epsilon_0 \notin \{\epsilon^l \mid l \in \mathbb{N}\}.$$

Dette er den ønskede modstrid. Altså er $\epsilon = \epsilon_0 = \sqrt[3]{2} - 1$ en fundamentalenhed for $O_K^\times$.

Eksempel 38. For $K = \mathbb{Q}(2\cos 2\pi/7)$ er (jf eksempel 35) $O_K = \mathbb{Z} + \mathbb{Z}\vartheta + \mathbb{Z}\vartheta^2$, hvor $\vartheta = \vartheta^{(1)} = 2\cos(2\pi/7)$. Da minimalpolynomiet $g(x) = x^3 + x^2 - 2x - 1$

for ϑ har de tre reelle nulpunkter $\vartheta^{(j)} = 2\cos(2\pi j/7)$, $1 \leq j \leq 3$, er $r_1 = 3, r_2 = 0$, altså $r = 2$. Ifølge ovenstående bemærkning er derfor

$$O_K^\times = \{\pm\epsilon_1^{n_1}\epsilon_2^{n_2} \mid n_1, n_2 \in \mathbb{Z}\},$$

hvor (ϵ_1, ϵ_2) er et sæt af fundamentalenheder. Vi fandt i eksempel 35, at $K/\mathbb{Q}$ er galois med $G = \mathrm{Gal}_{K/\mathbb{Q}} \simeq C_3$. Derfor er isomorfierne $\{\sigma_1, \sigma_2, \sigma_3\} \in G$ karakteriseret ved deres virkning på nulpunkterne $\vartheta^{(j)}$, $1 \leq j \leq 3$, i g. Lad derfor

$$\sigma_1 \leftrightarrow (1),\ \sigma_2 \leftrightarrow (\vartheta^{(1)}\ \vartheta^{(2)}\ \vartheta^{(3)}),\ \sigma_3 \leftrightarrow (\vartheta^{(1)}\ \vartheta^{(3)}\ \vartheta^{(2)}).$$

Da er

$$\begin{aligned}\underline{b}_1 &= L(\vartheta^{(1)}) = (\log|\vartheta^{(1)}|, \log|\vartheta^{(2)}|, \log|\vartheta^{(3)}|),\\ \underline{b}_2 &= L(\vartheta^{(2)}) = (\log|\vartheta^{(2)}|, \log|\vartheta^{(3)}|, \log|\vartheta^{(1)}|).\end{aligned}$$

En numerisk udregning (lommeregner) af $\vartheta^{(j)} = 2\cos(2\pi j/7)$, $1 \leq j \leq 3$, viser, at

$$\vartheta^{(1)} = 1.2469\cdots,\ \vartheta^{(2)} = -0.4450\cdots,\ \vartheta^{(3)} = -1.8019\cdots,$$

hvoraf

$$\log|\vartheta^{(1)}| = 0.2207\cdots,\ \log|\vartheta^{(2)}| = -0.8095\cdots,\ \log|\vartheta^{(3)}| = 0.5888\cdots.$$

Det fremgår heraf, at $M = \mathbb{Z}\underline{b}_1 + \mathbb{Z}\underline{b}_2$ er et fuldt (dvs. 2-dimensionalt) delgitter af $L(O_K^\times)$. Lad nu

$$\mathcal{P} = \{t_1\underline{b}_1 + t_2\underline{b}_2 \mid |t_1| \leq \tfrac{1}{2}, |t_2| \leq \tfrac{1}{2}\}.$$

Da er $\Pi = \mathcal{P} + M$. Antag nu (indirekte), at $[L(O_K^\times) : M] > 1$. Da findes en enhed $\epsilon \in O_K^\times$, så at

$$L(\epsilon) = (\lambda_1, \lambda_2, \lambda_3) \in \mathcal{P} \setminus \{\underline{0}\} \quad \text{og} \quad N(\epsilon) = 1. \tag{1}$$

Af ovenstående udregninger fremgår imidlertid, at $(\lambda_1, \lambda_2, \lambda_3) \in \mathcal{P}$ opfylder ulighederne

$$\begin{aligned}|\lambda_1| &\leq \tfrac{1}{2}(0.2207\cdots + 0.8095\cdots) = 0.5151\cdots,\\ |\lambda_2| &\leq \tfrac{1}{2}(0.8095\cdots + 0.5888\cdots) = 0.6992\cdots,\\ |\lambda_3| &\leq \tfrac{1}{2}(0.5888\cdots + 0.2207\cdots) = 0.4047\cdots.\end{aligned}$$

For det betragtede $\epsilon \in O_K^\times$ gælder derfor

$$|\epsilon^{(1)}| \le e^{0.5151\cdots} = 1.6738\cdots, |\epsilon^{(2)}| \le e^{0.6992\cdots} = 2.0121\cdots,$$
$$|\epsilon^{(3)}| \le e^{0.4047\cdots} = 1.4989\cdots.$$

Specielt er derfor

$$|\epsilon^{(1)} + \epsilon^{(2)} + \epsilon^{(3)}| \le 5.1850\cdots,$$
$$|\epsilon^{(1)}\epsilon^{(2)} + \epsilon^{(2)}\epsilon^{(3)} + \epsilon^{(3)}\epsilon^{(1)}| \le 8.8936\cdots,$$

og minimalpolynomiet $f = f_\epsilon$ for ϵ har derfor formen

$$f(x) = x^3 - Ax^2 + Bx - 1 \in \mathbb{Z}[x], \quad \text{hvor} \quad |A| \le 5,\ |B| \le 8. \tag{2}$$

Vi vil nu udregne diskriminanten $D(1, \epsilon, \epsilon^2)$ som funktion af A, B:

$$D(1,\epsilon,\epsilon^2) = \det \begin{pmatrix} S(1) & S(\epsilon) & S(\epsilon^2) \\ S(\epsilon) & S(\epsilon^2) & S(\epsilon^3) \\ S(\epsilon^2) & S(\epsilon^3) & S(\epsilon^4) \end{pmatrix} = \det \begin{pmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix},$$

hvor

$$s_\nu = {\epsilon^{(1)}}^\nu + {\epsilon^{(2)}}^\nu + {\epsilon^{(3)}}^\nu,\ 1 \le \nu \le 4.$$

Af (2) fremgår, at

$$\epsilon^{(1)} + \epsilon^{(2)} + \epsilon^{(3)} = A,\ \epsilon^{(1)}\epsilon^{(2)} + \epsilon^{(2)}\epsilon^{(3)} + \epsilon^{(3)}\epsilon^{(1)} = B,\ \epsilon^{(1)}\epsilon^{(2)}\epsilon^{(3)} = 1,$$

hvoraf man let finder

$$s_0 = 3,\ s_1 = A,\ s_2 = A^2 - 2B,\ s_3 = A^3 - 3AB + 3,\ s_4 = A^4 - 4A^2B + 4A + 2B^2.$$

Efter en simpel determinantudregning finder man derfor

$$D(1,\epsilon,\epsilon^2) = D(f) = A^2B^2 - 4A^3 - 4B^3 + 18AB - 27. \tag{3}$$

På den anden side er ifølge eksempel 35

$$D(1,\epsilon,\epsilon^2) = m^2 d = m^2 \cdot 49, \quad m \in \mathbb{N}. \tag{4}$$

Det medfølgende PARI-program UNITS finder først de polynomier f af formen (2) , for hvilke diskriminanten $D(f)$ givet ved (3) er af formen (4). Af de ialt

$11 \cdot 17 = 187$ polynomier, der undersøges, drejer det sig om 6, nemlig svarende til

$$(A, B) = (-4, 3), (-2, -1), (-1, -2), (3, -4), (5, -8), (5, 6),$$

for hvilke de tilhørende værdier af m er: 1,1,1,1,7,1.

For hvert af disse 6 polynomier findes herefter nulpunkterne (ved en Newton approksimation), og $L(\epsilon)$ beregnes (med tilfældig koordinatrækkefølge):

$$(1.0303\cdots, 0.3681\cdots, -1.3984\cdots),$$

$$(0.8095\cdots, -0.5888\cdots, -0.2207\cdots),$$

$$(0.5888\cdots, -0.8095\cdots, 0.2207\cdots),$$

$$(-0.3681\cdots, -1.0303\cdots, 1.3984\cdots),$$

$$(0.1474\cdots, -1.9873\cdots, 1.8399\cdots),$$

$$(-1.6191\cdots, 0.4414\cdots, 1.1777\cdots).$$

Uanset permutationer af koordinaterne tilhører intet af de ialt 36 tripler mængden $\mathcal{P}$, idet den numerisk største koordinat er for stor, og dette viser derfor, at den indirekte antagelse var forkert. Hermed er vist, at $(\vartheta^{(1)}, \vartheta^{(2)})$, er et sæt af fundamentalenheder, dvs.

$$O_K^\times = \{\pm {\vartheta^{(1)}}^{n_1} {\vartheta^{(2)}}^{n_2} \mid n_1, n_2 \in \mathbb{Z}\}.$$

Regulatoren. Lad K være et algebraisk tallegeme med $[K : \mathbb{Q}] = n$, og lad $(\epsilon_1, \ldots, \epsilon_r)$, hvor $r = r_1 + r_2 - 1$, være et sæt af fundamentalenheder i $O_K^\times$. Lad $L = (L_1, \ldots, L_{r+1})$ være den logaritmiske afbildning af $O_K^\times$ ind i $\Pi \subset \mathbb{R}^{r+1}$.

Definition. Ved *regulatoren* R for K forstås

$$R = \tfrac{1}{r+1} |\det A|,$$

hvor

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ L_1(\epsilon_1) & L_2(\epsilon_1) & \ldots & L_{r+1}(\epsilon_1) \\ \vdots & \vdots & \ddots & \vdots \\ L_1(\epsilon_r) & L_2(\epsilon_r) & \ldots & L_{r+1}(\epsilon_r) \end{pmatrix}.$$

For $K = \mathbb{Q}$ og $K = \mathbb{Q}(\sqrt{D})$, $D < 0$ og kvadratfri, er $r = 0$, dvs. $A = (1)$, hvorfor $R = 1$.

Bemærkning. Det må først indses, at regulatoren er veldefineret, dvs. uafhængig af valget af fundamentalenheder og af rækkefølgen af afbildningerne L_j, $1 \leq j \leq r+1 = r_1 + r_2$. Da $(1, 1, \ldots, 1) \in \mathbb{R}^{r+1}$ er ortogonal på

$$\Pi = \mathrm{span}_{\mathbb{R}}(L(\epsilon_1), \ldots, L(\epsilon_r)),$$

er $|\det A|$ lig produktet af $\|(1, 1, \ldots, 1)\|$ og gitterdeterminanten $d(M)$ for det r-dimensionale gitter $M = L(O_K^{\times}) \subset \Pi$. Derfor er

$$R = \tfrac{\sqrt{r+1}}{r+1} d(M) = \tfrac{1}{\sqrt{r+1}} d(M),$$

og det viser lovligheden af definitionen.

Ved i determinantformlen for R at addere alle søjler pånær den s'te til den s'te søjle fås (for $r > 0$):

$$R = |\det(L_j(\epsilon_i))_{j \neq s}|.$$

Fx finder man heraf, at $R = \log \epsilon$, hvor $\epsilon > 1$ er en fundamentalenhed, når K er et reelt kvadratisk tallegeme eller et reelt kubisk talegeme med diskriminant $d < 0$, idet $r = 1$ i begge disse tilfælde.

Vi anfører uden bevis følgende berømte sætning:

Sætning 86. *(C. L. Siegel, R. Brauer). Lad K være et (variabelt) algebraisk tallegeme af grad n, diskriminant d, klassetal h og regulator R. Da gælder:*

$$\frac{\log(hR)}{\log\sqrt{|d|}} \to 1 \quad \textit{for} \quad \frac{n}{\log|d|} \to 0.$$

Bemærkning. For $K = \mathbb{Q}(\sqrt{D})$, hvor $D < 0$ og kvadratfri, er $n = 2$ og $R = 1$. Af sætning 86 følger derfor, at

$$\log h \sim \log\sqrt{|d|} \quad \text{for} \quad |d| \to \infty \quad (\text{dvs. } -D \to \infty).$$

Heraf følger, at der kun er endeligt mange imaginært kvadratiske tallegemer af et givet klassetal h (jf. den historiske note side 3.36). Beklageligvis er sætning 86 *ineffektiv*, dvs. den indeholder ikke information om hurtigheden

af konvergensen. Af samme grund har sætningen ikke kunnet bidrage til bestemmelsen af samtlige imaginært kvadratiske tallegemer af klassetal 1, 2, etc.

For $K = \mathbb{Q}(\sqrt{D})$, hvor $D > 1$ og kvadratfri, er $n = 2$ og $R = \log \epsilon$, hvor $\epsilon > 1$ er en fundamentalenhed. Af sætning 86 følger derfor

$$\log(h \log \epsilon) \sim \log \sqrt{d} \quad \text{for} \quad d \to \infty \quad (\text{dvs. } D \to \infty).$$

Da R varierer uregelmæssigt med D, kan der ikke tilsvarende sluttes noget om antallet af reelt kvadratiske tallegememer af et givet klassetal h.

Ud fra omfattende beregninger af klassetal er den mest plausible hypotese, at der fx findes uendeligt mange reelt kvadratiske tallegemer af klassetal 1.

Opgaver:

Opgave 1. Gennemfør øvelsen efter sætning 62.

Opgave 2. I denne opgave vil vi diskutere nogle resultater fra den geometriske talteori med vigtige anvendelser i algebraisk talteori.

Først nogle nye begreber: Lad $\mathcal{M}$ være en åben delmængde af $\mathbb{R}^n$. Et fuldt gitter Λ i $\mathbb{R}^n$, kaldes $\mathcal{M}$-*tilladeligt*, hvis $\Lambda \cap \mathcal{M}$ er tom eller lig $\{\underline{0}\}$. Den *kritiske determinant* $\Delta(\mathcal{M})$ defineres ved

$$\Delta(\mathcal{M}) = \inf_{\Lambda \text{ er } \mathcal{M}-\text{tilladeligt}} d(\Lambda),$$

idet $\Delta(\mathcal{M}) = \infty$, hvis der ikke findes et $\mathcal{M}$-tilladeligt gitter Λ. For $0 < \Delta(\mathcal{M}) < \infty$ kaldes et $\mathcal{M}$-tilladeligt gitter Λ et *kritisk gitter* for $\mathcal{M}$, hvis $d(\Lambda) = \Delta(\mathcal{M})$. Bemærk: Selvom $0 < \Delta(\mathcal{M}) < \infty$, findes der ikke altid kritiske gitre.

Den fundamentale anvendelse i algebraisk talteori er følgende: For ethvert algebraisk tallegeme K betragtes (med sædvanlige betegnelser):

$$\mathcal{M} = \mathcal{M}_{r_1,r_2} = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |N(x)| < 1\},$$

hvor

$$N(x) = x_1 \cdots x_{r_1} |x_{r_1+1}|^2 \cdots |x_{r_1+r_2}|^2.$$

Vi har vist (jf side 3.49), at $\varphi(O_K) = \Lambda$ er et fuldt gitter i $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ med

$$d(\Lambda) = 2^{-r_2}\sqrt{|d|}.$$

Da $|N(\varphi(\alpha))| = |N(\alpha)| \geq 1$ for $\alpha \in O_K \setminus \{0\}$, er Λ $\mathcal{M}$-tilladeligt. Derfor er $d(\Lambda) \geq \Delta(\mathcal{M})$, dvs.

$$(*) \qquad |d| \geq 4^{r_2}\Delta(\mathcal{M})^2.$$

På tilsvarende måde ses det (jf sætning 69), at enhver idealklasse C i K indeholder et helt ideal $\mathfrak{a}$, som opfylder uligheden

$$(**) \qquad N(\mathfrak{a}) \leq \frac{1}{2^{r_2}\Delta(\mathcal{M})}\sqrt{|d|}.$$

I kraft af (*) og (**) er det væsentligt at have kendskab til $\Delta(\mathcal{M})$ som funktion af r_1 og r_2, hvor $[K : \mathbb{Q}] = n = r_1 + 2r_2$. Præcise værdier kendes imidlertid kun for $n = 2, 3$, idet

$$\Delta(\mathcal{M}_{0,1}) = \tfrac{1}{2}\sqrt{3}, \quad \Delta(\mathcal{M}_{2,0}) = \sqrt{5}, \quad \Delta(\mathcal{M}_{1,1}) = \tfrac{1}{2}\sqrt{23}, \quad \Delta(\mathcal{M}_{3,0}) = 7.$$

For $(r_1, r_2) = (0, 1)$ er bestemmelsen af $\Delta(\mathcal{M})$ ensbetydende med at finde den tætteste gitterformige pakning af enhedscirkler, og det er elementært.

For $(r_1, r_2) = (2, 0)$ er bestemmelsen af $\Delta(\mathcal{M})$ essentielt ensbetydende med Hurwitz'sætning om approksimation af reelle tal.

De to kubiske tilfælde, der begge skyldes H. Davenport (*On the product of three homogeneous linear forms* I, Proc. Lond. Math. Soc. (2) 44 (1938), 412-431), er teknisk komplicerede.

I disse fire tilfælde kan (*) ikke forbedres, idet der findes kvadratiske tallegemer af diskriminant $d = -3$ og $d = 5$ (jf sætning 51) samt kubiske tallegemer af diskriminant $d = -23$ (jf opgave 12) og $d = 49$ (jf eksempel 35). I disse tilfælde er det relevante $\Lambda = \varphi(O_K)$ derfor et kritisk gitter for $\mathcal{M}$.

Et berømt generelt resultat er følgende vurdering af H. Minkowski:

$$(***) \qquad \Delta\big(\mathcal{M}_{r_1,r_2}\big) \geq \frac{n^n}{n!}\left(\frac{\pi}{8}\right)^{r_2}.$$

Vis Minkowski's ulighed (***) for $= 2, 3$. Vink: I hvert af de 4 tilfælde betragtes et dellegeme $K \subseteq \mathcal{M}$, med følgende egenskaber: K er konvekst, K er symmetrisk om $\underline{0}$ og $\mathrm{vol}(K)$ er så stort som muligt.

Opgave 3. De imaginært kvadratiske tallegemer $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ og $\mathbb{Q}(\sqrt{-163})$ har klassetal 1. Diskutér forskellige beviser herfor.

Opgave 4. Vis, at $K = \mathbb{Q}(\sqrt{7})$ har klassetal $h = 1$. Vis endvidere, at $\epsilon = 8 + 3\sqrt{7}$ er en fundamentalenhed for $O_K^\times$.

Opgave 5. Vis, at den diophantiske ligning

$$x^3 = y^2 - 7$$

ikke har nogen løsning $(x, y) \in \mathbb{Z}^2$.

Vink: Vis først, at der for en eventuel løsning (x, y) til ligningen gælder

$$y + \sqrt{7} = \eta(u + v\sqrt{7})^3,$$

hvor $u, v \in \mathbb{Z}$, og $\eta = 1, \epsilon, \epsilon^{-1}$, idet $\epsilon = a + b\sqrt{7} > 1$ er en fundamentalenhed i $K = \mathbb{Q}(\sqrt{7})$ (jf opgave 4). Vis herved, at

$$(*) \qquad 1 = a(3u^2v + 7v^3) \pm b(u^3 + 21uv^2).$$

Vis endelig ved kongruenser modulo 3 og 9, at (*) er umulig.

Opgave 6. Betragt et vilkårligt kubisk tallegeme $K = \mathbb{Q}(\vartheta)$, hvor det (uden indskrænkning) kan antages, at ϑ er helt algebraisk. Idet d, r_1, r_2 har den sædvanlige betydning, skal man først vise følgende karakteriseringer af kubiske tallegemer:

A. $d > 0 \Leftrightarrow r_1 = 3, r_2 = 0$.

B. $d < 0 \Leftrightarrow r_1 = 1, r_2 = 1$.

Vink: Benyt, at diskriminanten d for O_K kan udtrykkes ved $D(1, \vartheta, \vartheta^2)$, som igen kan udtrykkes ved rødderne i minimalpolynomiet for ϑ.

For $d > 0$ skal det dernæst vises, at følgende to egenskaber er ækvivalente:

1. d er et kvadrattal.

2. $K/\mathbb{Q}$ er cyklisk (dvs. $K/\mathbb{Q}$ er galois med $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_3$).

Opgave 7. Betragt et vilkårligt kubisk tallegeme $K = \mathbb{Q}(\vartheta)$, hvor det (uden indskrænkning) kan antages, at ϑ er helt algebraisk. Lad minimalpolynomiet f for ϑ være

$$f(x) = x^3 - Ax^2 + Bx - C \in \mathbb{Z}[x].$$

Vis, at D=$D(1, \vartheta, \vartheta^2)$ – jf eksempel 38 – kan udtrykkes ved A, B, C på følgende måde:

$$D = D(f) = A^2B^2 - 4A^3C - 4B^3 + 18ABC - 27C^2.$$

Slut heraf, at $d = D/m^2$, hvor $m \in \mathbb{N}$.

Vis specielt, at der findes kubiske tallegemer af følgende diskriminanter:

$$d = -23, -31, 49, 81, 148, 169.$$

Opgave 8. I denne opgave betragtes *rent kubiske tallegemer*, dvs. tallegemer $K = \mathbb{Q}(\sqrt[3]{D})$, $D = ab^2$, hvor $a, b \in \mathbb{Z}$ er kvadratfrie, indbyrdes primiske og $ab \neq \pm 1$. Vis, at

$$O_K = \vartheta_0\mathbb{Z} + \vartheta_1\mathbb{Z} + \vartheta_2\mathbb{Z},$$

hvor

$$\vartheta_1 = \sqrt[3]{ab^2},$$
$$\vartheta_2 = \sqrt[3]{a^2b},$$
$$\vartheta_0 = \begin{cases} 1, & \text{hvis} \quad a \not\equiv \pm b \pmod 9 \quad \text{(type I)}, \\ \frac{1+a\vartheta_1+b\vartheta_2}{3}, & \text{hvis} \quad a \equiv \pm b \pmod 9 \quad \text{(type II)}. \end{cases}$$

Vis derved, at diskriminanten d for K er givet ved

$$d = \begin{cases} -27a^2b^2 & \text{(type I)}, \\ -3a^2b^2 & \text{(type II)}. \end{cases}$$

Vink: Generalisér fremgangsmåden i eksempel 34.

Opgave 9. Vis, at $K = \mathbb{Q}(\sqrt[3]{2})$ har klassetal $h = 1$. Vink: Benyt eksempel 34 (eller opgave 8) samt et resultat fra opgave 2.

Opgave 10. Betragt $K = \mathbb{Q}(i)$ og $R = O_K$. Vis ved et simpelt argument, at $N = N_{K/\mathbb{Q}} : R \to \mathbb{N}_0$ ikke er den minimale euklidiske funktion på R.

Vis derpå, at N heller ikke er ækvivalent med den minimale euklidiske funktion f på R. Vink: Find $f^{-1}(n)$ for $n \leq 2$.

Opgave 11. Betragt $K = \mathbb{Q}(\sqrt[3]{2})$ og $R = O_K$. Vis, at normen $N = N_{K/\mathbb{Q}}$ bestemmer euklidisk funktion $|N| : R \to \mathbb{N}_0$ på R. Vink: Benyt (jf eksempel 34), at

$$N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc = F(a, b, c) \quad a, b, c \in \mathbb{Q},$$

og vis, at der til ethvert sæt $(a, b, c) \in \mathbb{R}^3$ findes et sæt $(a_0, b_0, c_0) \in \mathbb{R}^3$ med

$$a \equiv a_0 \pmod 1, \quad b \equiv b_0 \pmod 1, \quad c \equiv c_0 \pmod 1,$$

så at $|F(a_0, b_0, c_0)| < 1$.

Opgave 12. Betragt det reelle kubiske tallegeme $K = \mathbb{Q}(\vartheta)$, hvor ϑ er rod i polynomiet $f(x) = x^3 - x - 1$.

1) Vis, at diskriminanten $d = -23$, og angiv en $\mathbb{Z}$-basis for O_K.

2) Bestem en fundamentalenhed for $O_K^\times$.

3) Vis, at K har klassetal $h = 1$.

Det kan vises, at der kun findes et reelt kubisk tallegeme af diskriminant $d = -23$, og at $d \leq -31$ for alle øvrige reelt kubiske tallegemer med $d < 0$.

Opgave 13. Betragt det reelle kubiske tallegeme $K = \mathbb{Q}(\vartheta)$, hvor ϑ er rod i polynomiet $f(x) = x^3 + x - 1$.

1) Vis, at diskriminanten $d = -31$, og angiv en $\mathbb{Z}$-basis for O_K.

2) Bestem en fundamentalenhed for $O_K^\times$.

3) Vis, at K har klassetal $h = 1$.

Det kan vises, at der kun findes et reelt kubisk tallegeme af diskriminant $d = -31$.

Opgave 14. Betragt legemet $\mathbb{Q}(\sqrt[3]{2})$ (jf eksemplerne 34 og 37). Vis, at enhedsgruppen $O_K^\times$ er isomorf med den multiplikative gruppe $\mathcal{M}$ af matricer af formen

$$M = \begin{pmatrix} a & 2b & 2c \\ c & a & b \\ b & 2c & a \end{pmatrix}$$

med $\det M = \pm 1$.

Opgave 15. Betragt legemet $\mathbb{Q}(\vartheta)$, hvor $\vartheta = 2\cos(2\pi/7)$) (jf eksemplerne 34 og 37). Vis, at

$$\alpha = a + b\vartheta + c\vartheta^2 \in O_K^\times,$$

netop hvis $a, b, c \in \mathbb{Z}$, og

$$a^3 + b^3 + c^3 - a^2b + 5a^2c - 2ab^2 + 6ac^2 - b^2c - 2bc^2 - abc = \pm 1.$$

Vink: Udregn $N(\alpha)$. Eksakt beregning er ikke altid det nemmeste!

Opgave 16. Betragt legemet $K = \mathbb{Q}(i, \sqrt{7+3i})$. Vis, at $r_1 = 0, r_2 = 2$, og derfor $r = 1$. Vis, at

$$\epsilon = 99 - 98i + (28 - 42i)\sqrt{7+3i} \in O_K^\times.$$

Vis også, at ϵ har minimalpolynomiet

$$f(x) = x^4 - 396x^3 + 77622x^2 - 396x + 1.$$

Det kan vises, at ϵ er en fundamentalenhed.

4. Cirkeldelingslegemer. Kummer's sætning

Vi vil i dette kapitel benytte, at cirkeldelingspolymiet Φ_n, $n \in \mathbb{N}$, der er givet ved

$$\Phi_n(x) = \prod_{1 \le m \le n,\, \gcd(m,n)=1} (x - \zeta^m), \quad \text{hvor} \quad \zeta = e^{2\pi i/n},$$

tilhører $\mathbb{Z}[x]$, er irreducibelt i $\mathbb{Q}(x)$ og har grad $\varphi(n)$.

I det følgende er $n = l$ et ulige primtal, hvorfor $\zeta = e^{2\pi i/l}$, og $K = \mathbb{Q}(\zeta)$. Da er ζ^j for $1 \le j \le l-1$ nulpunkter i polynomiet Φ_l, der opfylder

$$\Phi_l(x) = \frac{x^l - 1}{x - 1} = x^{l-1} + x^{l-2} + \cdots + x + 1 = \prod_{j=1}^{l-1}(x - \zeta^j). \tag{1}$$

Af (1) aflæses at

$$S(\zeta^j) = -1 \quad \text{for} \quad 1 \le j \le l-1. \tag{2}$$

Indsættes $x = 1$ i (1), fås endvidere formlen

$$l = \prod_{j=1}^{l-1}(1 - \zeta^j). \tag{3}$$

Det er i visse sammenhænge fordelagtigt at benytte $\lambda = 1 - \zeta$ som frembringer for K i stedet for ζ. Formlerne (1), (2), (3) for ζ kan da oversættes til følgende formler for λ:

Tallene $\lambda^{(j)} = 1 - \zeta^j$ er for $1 \le j \le l-1$ nulpunkter i polynomiet Ψ_l, der opfylder

(1')

$$\Psi_l(x) = (-1)^l \frac{(1-x)^l - 1}{x} = x^{l-1} - \binom{l}{1}x^{l-2} + \cdots + \binom{l}{l-1} = \prod_{j=1}^{l-1}(x - \lambda^{(j)}).$$

Af (2) eller (1') aflæses at

$$S(\lambda^{(j)}) = l \quad \text{for} \quad 1 \le j \le l-1. \tag{2'}$$

Endelig aflæses af (3) eller (1') at

$$l = \prod_{j=1}^{l-1} \lambda^{(j)} = N(\lambda). \tag{3'}$$

Lad nu

$$\xi = \prod_{j=1}^{(l-1)/2} (\zeta^j - \zeta^{-j}).$$

Da

$$(\zeta^j - \zeta^{-j})^2 = -(1-\zeta^{2j})(1-\zeta^{-2j}),$$

er

$$\xi^2 = (-1)^{(l-1)/2} \prod_{j=1}^{(l-1)/2} (1-\zeta^{2j})(1-\zeta^{-2j}) = (-1)^{(l-1)/2)} \prod_{j=1}^{l-1} (1-\zeta^j).$$

Ifølge (3) gælder derfor

$$\xi^2 = (-1)^{(l-1)/2} l. \tag{4}$$

Sætning 87. *Lad $K = \mathbb{Q}(\zeta)$. Da er K totalt imaginært, dvs. $r_1 = 0$, $r_2 = [K : \mathbb{Q}]/2 = (l-1)/2$. Udvidelsen $K/\mathbb{Q}$ er galois med Galoisgruppe $G = Gal(K/\mathbb{Q}) \simeq C_{l-1}$.*

K indeholder netop et dellegeme af grad $(l-1)/2$, nemlig

$$K_0 = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(2\cos(2\pi/l)) = K \cap \mathbb{R}.$$

K_0 er totalt reelt, dvs. $r_1 = [K_0 : \mathbb{Q}] = (l-1)/2$, $r_2 = 0$, idet de konjugerede til $2\cos(2\pi/l)$ er $2\cos(2\pi j/l)$, $1 \le j \le (l-1)/2$. Udvidelsen $K_0/\mathbb{Q}$ er galois med Galoisgruppe $G_0 = Gal(K_0/\mathbb{Q}) \simeq C_{(l-1)/2}$.

K indeholder netop et kvadratisk dellegeme, nemlig

$$k = \mathbb{Q}\left(\sqrt{(-1)^{(l-1)/2} l}\right).$$

Bevis. Sætningens påstande vedrørende K selv og K_0 er allerede vist i eksempel 12. Bemærk, at Galoisgrupperne G og G_0 består af

$$G = \{\zeta \mapsto \zeta^j \mid 1 \le j \le l-1\},$$

og

$$G_0 = \{2\cos(2\pi/l) \mapsto 2\cos(2\pi j/l) \mid 1 \leq j \leq (l-1)/2\}.$$

At K indeholder netop et kvadratisk tallegeme følger af Galoisteoriens hovedsætning, idet $G \simeq C_{l-1}$ netop indeholder en undergruppe af orden $(l-1)/2$. Formel (4) viser nu, at dette kvadratiske tallegeme må være

$$k = \mathbb{Q}(\xi) = \mathbb{Q}\left(\sqrt{(-1)^{(l-1)/2}l}\right).$$

Dette viser sætningen. □

Bemærkning. I kraft af karakteriseringen $K_0 = K \cap \mathbb{R}$, kaldes K_0 *det l'te reelle cirkeldelingslegeme*. Bemærk, at de to enhedsgrupper $O_K^\times$ og $O_{K_0}^\times$ har samme rang $r = (l-3)/2$. Ifølge Dirichlet's enhedssætning følger heraf, at kvotientgruppen $O_K^\times/O_{K_0}^\times$ er en endelig gruppe. I sætning 91 bestemmes denne kvotientgruppe.

Sætning 88. *Lad $K = \mathbb{Q}(\zeta)$. Da er $l = (1-\zeta)^{l-1}\epsilon$, hvor $\epsilon \in O_K^\times$.*

Bevis. Lad j være valgt vilkårligt i intervallet $1 \leq j \leq l-1$, og lad $j' \in \mathbb{N}$ være bestemt (modulo l), så at $jj' \equiv 1 \pmod{l}$. Da $\zeta \in O_K$, er

$$\frac{1-\zeta^j}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{j-1} \in O_K,$$

og

$$\frac{1-\zeta}{1-\zeta^j} = \frac{1-(\zeta^j)^{j'}}{1-\zeta^j} = 1 + \zeta^j + \cdots + \zeta^{j(j'-1)} \in O_K.$$

Dette viser, at $1-\zeta^j$ og $1-\zeta$ er associerede i O_K, altså

$$1-\zeta^j = (1-\zeta)\epsilon_j, \quad \text{hvor} \quad \epsilon_j \in O_K^\times.$$

Af formel (3) får vi derfor, at

$$l = (1-\zeta)^{l-1}\epsilon, \quad \text{hvor} \quad \epsilon = \prod_1^{l-1} \epsilon_j \in O_K^\times.$$

Dette viser sætningen. □

Bemærkning. Sætning 88 viser, at

$$(l) = lO_K = ((1-\zeta))^{l-1} = (\lambda)^{l-1}. \tag{5}$$

Heraf (eller af (3')) følger, at $N((\lambda)) = l$. Hovedidealet (λ) er derfor et primideal af grad 1 i O_K. Formel (5) viser, at hovedidealet $(l) = lO_K$ er (fuldt) forgrenet, og at primidealet (λ) har forgreningsindex $l-1$.

Sætning 89. *Lad $K = \mathbb{Q}(\zeta)$, og $\lambda = 1-\zeta$. Da er*

$$O_K = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{l-2} = \mathbb{Z}[\lambda] = \mathbb{Z} + \mathbb{Z}\lambda + \cdots + \mathbb{Z}\lambda^{l-2}.$$

For diskriminanten d for K gælder

$$d = (-1)^{(l-1)/2} l^{l-2}.$$

Bevis. Da

$$\zeta^{l-1} = -1 - \zeta - \cdots - \zeta^{l-2}$$

er det klart, at de fire udtryk for O_K er ækvivalente, og at følgelig

$$D(1, \zeta, \cdots, \zeta^{l-2}) = D(1, \lambda, \cdots, \lambda^{l-2}).$$

Da

$$S(\zeta^j) = \begin{cases} -1 & \text{for} \quad 1 \le j \le l-1 \quad \text{og} \quad l+1 \le j \le 2l-4 \\ l-1 & \text{for} \quad j = 0, l \end{cases}$$

finder vi (jf. eksempel 7 og opgave 4 i kapitel 1):

$$D(1, \zeta, \cdots, \zeta^{l-2}) = \begin{vmatrix} S(1) & S(\zeta) & S(\zeta^2) & \dots & S(\zeta^{l-2}) \\ S(\zeta) & S(\zeta^2) & S(\zeta^3) & \dots & S(\zeta^{l-1}) \\ S(\zeta^2) & S(\zeta^3) & S(\zeta^4) & \dots & S(1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S(\zeta^{l-2}) & S(\zeta^{l-1}) & S(1) & \dots & S(\zeta^{2l-4}) \end{vmatrix}$$

$$= \begin{vmatrix} l-1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & l-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & l-1 & \dots & -1 \end{vmatrix} = \begin{vmatrix} l & -1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & l \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & l & \dots & 0 \end{vmatrix}$$

$$= (-1)^{(l-1)/2} l^{l-2}.$$

Vi mangler nu kun at vise, at $O_K = \mathbb{Z}[\lambda] = \mathbb{Z} + \mathbb{Z}\lambda + \cdots + \mathbb{Z}\lambda^{l-2}$. Af beviset for sætning 17 om udvidelser af Dedekindringe fremgår, at ethvert $\alpha \in O_K$ har formen

$$\alpha = \frac{a_0 + a_1\lambda + \cdots + a_{l-2}\lambda^{l-2}}{l^{l-2}}, \quad \text{hvor} \quad a_j \in \mathbb{Z} \quad \text{for} \quad 0 \leq j \leq l-2.$$

I dette udtryk forkortes med den højeste potens af l, som går op i alle koefficienter a_j og i l^{l-2}. Herefter er α skrevet på formen

$$\alpha = \frac{b_0 + b_1\lambda + \cdots + b_{l-2}\lambda^{l-2}}{l^s}, \quad \text{hvor} \quad b_j \in \mathbb{Z} \quad \text{for} \quad 0 \leq j \leq l-2,$$

med $s \geq 0$, og hvor der for $s \geq 1$ gælder, at $\exists j_0 \in \{0, \ldots, l-2\}$, så at $l \nmid b_{j_0}$.

Antag nu (indirekte), at $s \geq 1$, og lad $j_0 \geq 0$ være valgt minimalt. Der gælder da

$$l \mid b_0, \ldots, l \mid b_{j_0-1}, l \nmid b_{j_0}.$$

Da $l \mid b_0 + b_1\lambda + \cdots + b_{l-2}\lambda^{l-2} = \alpha l^s$, gælder derfor

$$l \mid b_{j_0}\lambda^{j_0} + \cdots + b_{l-2}\lambda^{l-2} = \lambda^{j_0}(b_{j_0} + b_{j_0+1}\lambda + \cdots).$$

Imidlertid er $l = \lambda^{l-1}\epsilon$, $\epsilon \in O_K^\times$, og da $j_0 < l-1$, følger heraf, at $\lambda \mid b_{j_0} + b_{j_0+1}\lambda + \cdots$. Dette viser, at $\lambda \mid b_{j_0}$ og dermed $l \mid b_{j_0}$, hvilket er en modstrid. Hermed er sætningen bevist. □

Sætning 90. *Lad $K = \mathbb{Q}(\zeta)$. Da er gruppen af enhedsrødder i $O_K^\times$ af orden $w = 2l$, og den består af*

$$\{\pm\zeta^g \mid 1 \leq g \leq l\} = \{(-\zeta)^g \mid 1 \leq g \leq 2l\}. \tag{6}$$

Bevis. Ifølge Dirichlet's enhedssætning er gruppen af enhedsrødder i $O_K^\times$ cyklisk af orden $w \in \mathbb{N}$, dvs. den består af

$$\{e^{2\pi i m/w} \mid 1 \leq m \leq w\}.$$

Da gruppen af enhedsrødder i $O_K^\times$ indeholder (6) som en undergruppe af orden $2l$, vil $2l \mid w$. Skriver vi nu $w = l^s q$, hvor $l \nmid q$, vil der derfor gælde $s \geq 1$ og $q \geq 2$. Graden af $e^{2\pi i/w}$ er $\varphi(w)$, og da φ er multiplikativ, fås

$$\varphi(w) = \varphi(l^s)\varphi(q) = (l-1)l^{s-1}\varphi(q).$$

Da $e^{2\pi i/w} \in O_K^\times \subset K$ og $[K:\mathbb{Q}] = l-1$, må der også gælde $\varphi(w) \leq l-1$. Dette viser, at $s = 1$ og $q \leq 2$. Da der også gjaldt $q \geq 2$, er $q = 2$, dvs. $w = 2l$. Hermed er sætningen bevist. □

Sætning 91. *(Kummer's enhedssætning). Lad $K = \mathbb{Q}(\zeta)$. Da er enhver enhed $\epsilon \in O_K^\times$ af formen*

$$\epsilon = \zeta^g \epsilon_0,$$

hvor $1 \leq g \leq l$ og $\epsilon_0 \in O_{K_0}^\times = O_K^\times \cap \mathbb{R}$.

Bevis. Lad

$$\epsilon = a_0 + a_1\zeta + \cdots + a_{l-2}\zeta^{l-2} = g(\zeta), \quad a_j \in \mathbb{Z},$$

være en vilkårlig enhed i $O_K^\times$. Betragt $\mu = \epsilon/\overline{\epsilon}$. Da automorfierne i $G = \mathrm{Gal}(K/\mathbb{Q})$ er givet ved $\sigma_j : \zeta \mapsto \zeta^j$, $1 \leq j \leq l-1$, er de konjugerede til μ af formen

$$\mu^{(j)} = \sigma_j(\mu) = \sigma_j\left(\frac{g(\zeta)}{g(\zeta^{-1})}\right) = \frac{g(\zeta^j)}{g(\zeta^{-j})} = \frac{g(\zeta^j)}{\overline{g(\zeta^j)}}.$$

Specielt er derfor

$$|\mu^{(j)}| = 1 \quad \text{for} \quad 1 \leq j \leq l-1.$$

Dette viser, at $\mu \in \ker L$, hvor L er den logaritmiske afbildning for $O_K^\times$, hvorfor μ er en enhedsrod (jf sætning 85 (i)). Ifølge sætning 90 gælder derfor enten

$$\epsilon = \zeta^g \overline{\epsilon}, \quad \text{hvor} \quad 1 \leq g \leq l, \tag{7+}$$

eller

$$\epsilon = -\zeta^g \overline{\epsilon}, \quad \text{hvor} \quad 1 \leq g \leq l. \tag{7–}$$

Vi vil nu vise, at (7–) ikke kan forekomme. Antag derfor (indirekte), at der findes en enhed $\epsilon \in O_K^\times$, hvor (7–) gælder. Da $\zeta = 1 - \lambda \equiv 1 \pmod{\lambda}$, er $\zeta^j \equiv 1 \pmod{\lambda}$ for ethvert $j \in \mathbb{N}$. Da $\overline{\zeta} = \zeta^{l-1}$ er også $\overline{\zeta}^j \equiv 1 \pmod{\lambda}$ for ethvert $j \in \mathbb{N}$. Der gælder da

$$\epsilon \equiv \overline{\epsilon} \equiv a_0 + a_1 + \cdots + a_{l-2} = T \pmod{\lambda},$$

men af den indirekte antagelse følger, at der også gælder

$$\epsilon \equiv -\overline{\epsilon} \pmod{\lambda}.$$

Derfor gælder

$$2T \equiv \epsilon + \overline{\epsilon} \equiv 0 \pmod{\lambda} \Rightarrow 2T \equiv 0 \pmod{l} \Rightarrow T \equiv 0 \pmod{l}.$$

Men da er $\epsilon \equiv T \equiv 0 \pmod{\lambda}$, hvilket er en modstrid, da λ ikke er en enhed ($|N(\lambda)| = l$).

Følgelig gælder (7+) for enhver enhed $\epsilon \in O_K^\times$. Vælg nu $s \in \mathbb{N}$, så at $2s \equiv g \pmod{l}$ (enten $2s = g$ eller $2s = g + l$ vil være brugbar). Da er

$$\frac{\epsilon}{\zeta^s} = \overline{\left(\frac{\epsilon}{\zeta^s}\right)} \in \mathbb{R},$$

hvorfor

$$\epsilon/\zeta^s = \epsilon_0 \in O_K^\times \cap \mathbb{R} = O_{K_0}^\times.$$

Hermed er sætningen bevist. □

Bemærkning. Det følger umiddelbart af Kummer's enhedssætning, at

$$O_K^\times / O_{K_0}^\times \simeq C_{l-1}.$$

Kummer's sætning. Med baggrund i de foregående sætninger skal vi nu omtale E. Kummer's berømte bidrag til Fermats problem (jf indledningen). Først en hjælpesætning.

Sætning 92. *Lad $K = \mathbb{Q}(\zeta)$, og $\lambda = 1 - \zeta$. Lad $x, y, m, n \in \mathbb{Z}$, hvor $m \not\equiv n \pmod{l}$, være givne. Da er hovedidealerne $(x + \zeta^m y)$ og $(x + \zeta^n y)$ indbyrdes primiske i O_K, hvis og kun hvis gcd$(x, y) = 1$ og $l \nmid x + y$.*

Bevis. Det er klart, at $\gcd(x, y) = 1$ er en nødvendig betingelse. Da

$$x + \zeta^m y \equiv x + \zeta^n y \equiv x + y \pmod{\lambda},$$

vil (λ) være en fælles divisor for $(x + \zeta^m x)$ og $(x + \zeta^n y)$, såfremt $\lambda \,|\, x + y \Leftrightarrow l = |N(\lambda)| \,|\, x + y$. Dette viser nødvendigheden af betingelsen $l \nmid x + y$.

Vi viser dernæst tilstrækkeligheden af de to betingelser. Vi skal derfor under antagelse af disse vise, at idealet

$$\mathfrak{a} = (x + \zeta^m y)O_K + (x + \zeta^n y)O_K$$

indeholder 1, altså at $\mathfrak{a} = O_K$. På grund af symmetrien mellem m og n kan vi gerne antage, at $n \geq m$. Det observeres nu, at

$$x + \zeta^m y - (x + \zeta^n y) = \zeta^m (1 - \zeta^{n-m}) y = \zeta^m \lambda \epsilon_{n-m} y \in \mathfrak{a},$$

hvor $\epsilon_{n-m} \in O_K^\times$, hvorfor

$$\lambda y \in \mathfrak{a}.$$

Tilsvarende er

$$(x + \zeta^m y)\zeta^n - (x + \zeta^n y)\zeta^m = -\zeta^m (1 - \zeta^{n-m}) x = -\zeta^m \lambda \epsilon_{n-m} x \in \mathfrak{a},$$

hvorfor

$$\lambda x \in \mathfrak{a}.$$

Da $\gcd(x, y) = 1$ findes der $r, s \in \mathbb{Z}$, så at $rx + sy = 1$, og følgelig er

$$\lambda = r(\lambda x) + s(\lambda y) \in \mathfrak{a}.$$

Heraf følger imidlertid, at

$$l = \lambda^{l-1} \epsilon \in \mathfrak{a},$$

og

$$x + y = x + \zeta^m y + (1 - \zeta^m) y = x + \zeta^m y + \lambda \epsilon_m y \in \mathfrak{a}.$$

Da $\gcd(x + y, l) = 1$ findes der $u, v \in \mathbb{Z}$, så at $u(x + y) + vl = 1$, og følgelig er

$$1 = u(x + y) + vl \in \mathfrak{a}.$$

Hermed er sætningen bevist. □

Definition. Et ulige primtal l kaldes *regulært*, hvis l ikke går op i klassetallet h for cirkeldelingslegemet $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$.

Sætning 93. *(Kummer, 1850). Fermat's ligning*

$$x^l + y^l = z^l$$

har ingen løsninger $(x, y, z) \in (\mathbb{Z} \setminus \{0\})^3$*, når* l *er et regulært primtal.*

Bevis. Beviset føres indirekte, idet det antages at der for et regulært primtal l findes en løsning $(x, y, z) \in (\mathbb{Z} \setminus \{0\})^3$. På grund af ligningens homogenitet kan det gerne antages, at $\gcd(x, y, z) = 1$. Men da gælder

$$\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1, \tag{8}$$

idet en fælles divisor for to af tallene x, y, z pga. ligningen vil gå op i det tredie.

Man skelner nu mellem to hovedtilfælde:

1. tilfælde: $l \nmid xyz$,

2. tilfælde: $l \mid xyz$.

På indeværende stadium kan vi kun gennemføre beviset for 1. tilfælde. Da

$$z \equiv z^l = x^l + y^l \equiv x + y \pmod{l},$$

gælder derfor

$$l \nmid x + y \quad \text{og} \quad l \nmid x - z. \tag{9}$$

Da l er ulige, kan Fermat's ligning faktoriseres på følgende måde over O_K:

$$\prod_{j=0}^{l-1} (x + \zeta^j y) = z^l.$$

Af sætning 92 og (8)–(9) fremgår, at idealerne $(x + \zeta^j y) = (x + \zeta^j y)O_K$ for $0 \leq j \leq l - 1$ er parvis indbyrdes primiske. Da O_K er en Dedekindring følger det derfor af idealligningen

$$\prod_{j=0}^{l-1} (x + \zeta^j y)O_K = (zO_K)^l,$$

at hver af faktorerne på venstre side er l'te potens af et helt ideal i O_K. Specielt er derfor

$$(x + \zeta y)O_K = \mathfrak{a}^l. \tag{10}$$

hvor $\mathfrak{a}$ er et helt ideal i O_K. Da $l \nmid h$, findes et naturligt tal m, så at $lm \equiv 1 \pmod{h}$, og der gælder da

$$\mathfrak{a} \simeq \mathfrak{a}^{lm} = (x + \zeta y)^m O_K,$$

dvs.

$$\mathfrak{a} = \alpha O_K, \quad \text{hvor} \quad \alpha \in O_K,$$

er et hovedideal i O_K. Af (10) fås derfor, at

$$x + \zeta y = \epsilon \alpha^l, \quad \text{hvor} \quad \epsilon \in O_K^\times,\ \alpha \in O_K. \tag{11}$$

Da vi i Fermat's ligning kan ombytte y og $-z$ (uden at forlade tilfælde 1), fås tilsvarende:

$$x - \zeta z = \epsilon' \alpha'^l, \quad \text{hvor} \quad \epsilon' \in O_K^\times,\ \alpha' \in O_K. \tag{11'}$$

Vi skelner nu mellem tilfældene $l = 3$ og $l \geq 5$.

$l = 3$. Vi har da specielt

$$x^3 + y^3 \equiv z^3 \pmod 9. \tag{12}$$

Da $3 \nmid xyz$, er $x, y, z \equiv \pm 1 \pmod 3$. Imidlertid er

$$(3u \pm 1)^3 = 27u^3 \pm 27u^2 + 9u \pm 1 \equiv \pm 1 \pmod 9,$$

hvorfor

$$x^3 \equiv \pm 1 \pmod 9,\ \ y^3 \equiv \pm 1 \pmod 9,\ \ z^3 \equiv \pm 1 \pmod 9.$$

Dette er i strid med (12). Hermed er uløseligheden af Fermat's ligning vist i første tilfælde for $l = 3$.

$l \geq 5$. I relationen (11) er ifølge sætning 89

$$\alpha = a_0 + a_1\zeta + \cdots + a_{l-2}\zeta^{l-2}, \quad \text{hvor} \quad a_j \in \mathbb{Z}.$$

Da de blandede multinomialkoefficienter er delelige med l, er

$$\begin{aligned} \alpha^l &\equiv {a_0}^l + {a_1}^l\zeta^l + \cdots + {a_{l-2}}^l\zeta^{(l-2)l} \pmod l \\ &= {a_0}^l + {a_1}^l + \cdots + {a_{l-2}}^l \\ &\equiv a_0 + a_1 + \cdots + a_{l-2} = T \pmod l. \end{aligned}$$

Endvidere er ifølge sætning 91

$$\epsilon = \zeta^g \epsilon_0, \quad g \in \mathbb{Z},\ \epsilon_0 \in O_{K_0}^\times.$$

Følgelig giver (11) anledning til kongruensen

$$x + \zeta y \equiv \zeta^g \eta \pmod l, \tag{13}$$

hvor $g \in \mathbb{Z},\ \eta = \epsilon_0 T \in O_{K_0}$. Anvender vi herpå automorfien $\zeta \mapsto \zeta^{-1} = \overline{\zeta} \in G = \mathrm{Gal}(K/\mathbb{Q})$ fås, da $\eta \in K_0$:

$$x + \zeta^{-1} y \equiv \zeta^{-g} \eta \pmod{l}. \tag{14}$$

Ved i kongruenserne (13) og (14) at eliminere η fås

$$\zeta^{-g}(x + \zeta y) \equiv \zeta^{g}(x + \zeta^{-1} y) \pmod{l},$$

eller

$$x\zeta^{g} + y\zeta^{g-1} - x\zeta^{-g} - y\zeta^{1-g} \equiv 0 \pmod{l}. \tag{15}$$

Imidlertid følger det af sætning 89, at der for $b_j \in \mathbb{Z}$ gælder:

$$b_0 + b_1\zeta + \cdots + b_{l-2}\zeta^{l-2} \equiv 0 \pmod{l} \Leftrightarrow b_0 \equiv b_1 \equiv \cdots \equiv b_{l-2} \equiv 0 \pmod{l}.$$

Antag først, at eksponenterne

$$g, g-1, -g, 1-g \tag{16}$$

i (15) parvist er inkongruente modulo l og ingen er kongruent med $l-1$ modulo l. Da følger det direkte af (15), at $x \equiv y \equiv 0 \pmod{l}$. Dette er i strid med (8), hvorfor beviset straks er afsluttet i dette tilfælde.

Antag dernæst, at en af eksponenterne i (16) er kongruent med $l-1$ modulo l. Da har vi følgende restklassemuligheder modulo l:

g	$g-1$	$-g$	$1-g$
$l-1$	$l-2$	1	2
0	$l-1$	0	1
1	0	$l-1$	0
2	1	$l-2$	$l-1$

I hvert af de fire tilfælde er netop en eksponent $\equiv l-1 \pmod{l}$, da $l \geq 5$. Indsætter vi derfor i (15) $\zeta^{l-1} = -1 - \zeta - \cdots - \zeta^{l-2}$ bringes (15) på kanonisk form $b_0 + b_1\zeta + \cdots + b_{l-2}\zeta^{l-2}$, hvorfor alle $b_j \equiv 0 \pmod{l}$. Da $l - 1 > 3$ vil mindst et b_j have en koefficient $\pm x$ eller $\pm y$. Derfor er $xy \equiv 0 \pmod{l}$ i strid med, at vi er i 1. tilfælde. Beviset er derfor også afsluttet i dette tilfælde.

Antag endelig, at to af eksponenterne i (16) er kongruente modulo l. Da $g \not\equiv g-1 \pmod{l}$ og $-g \not\equiv 1-g \pmod{l}$, har vi en af følgende fire muligheder:

(a) $g \equiv -g \pmod{l} \Leftrightarrow g \equiv 0 \pmod{l}$,

(b) $g \equiv 1-g \pmod{l} \Leftrightarrow g \equiv (l+1)/2 \pmod{l}$,

(c) $g-1 \equiv -g \pmod{l} \Leftrightarrow g \equiv (l+1)/2 \pmod{l}$,

(d) $g-1 \equiv 1-g \pmod{l} \Leftrightarrow g \equiv 1 \pmod{l}$.

Det ses, at tilfældene (a) og (d) allerede er betragtet ovenfor. Endvidere ses det, at tilfældene (b) og (c) er sammenfaldende og svarer til, at $g \equiv (l+1)/2 \pmod{l}$. I dette tilfælde er

$$g \equiv 1-g \equiv (l+1)/2 \pmod{l} \quad \text{og} \quad g-1 \equiv -g \equiv (l-1)/2 \pmod{l},$$

hvorfor (15) har formen

$$-(x-y)\zeta^{(l-1)/2} + (x-y)\zeta^{(l+1)/2} \equiv 0 \pmod{l}.$$

Følgelig er

$$x \equiv y \pmod{l}. \tag{16}$$

For at føre dette til en modstrid benyttes også kongruensen

$$x \equiv -z \pmod{l}, \tag{16'}$$

der på tilsvarende måde fremkommer af (11'). Indsættes (16) og (16') i kongruensen $x+y \equiv z \pmod{l}$ fås

$$3x \equiv 0 \pmod{l}.$$

Da $l > 3$, er derfor $x \equiv 0 \pmod{l}$, hvilket er i strid med at vi er i tilfælde 1.

Hermed er sætningen bevist i første tilfælde. □

Bemærkning. Kummer viste, at følgende tre betingelser for et primtal $l \geq 5$ er ensbetydende:

(i) l er et regulært primtal.

(ii) Potenssummen $S_k = 1^k + 2^k + \cdots + (l-1)^k \not\equiv 0 \pmod{l^2}$ for $k = 2, 4, \ldots, l-3$.

(iii) Tælleren i Bernoullitallet B_k er ikke deleligt med l for $k = 2, 4, \ldots, l-3$.

Her er Bernoullitallene B_k for $k \in \mathbb{N}$ defineret ved

$$\frac{t}{e^t - 1} = 1 + \sum_{k=1}^{\infty} \frac{B_k}{k!} t^k.$$

Det er let at se, at

$$B_1 = -1/2 \quad \text{og} \quad B_{2k+1} = 0 \quad \text{for} \quad k \geq 1,$$

samt at

$$1 + \sum_{j=1}^{k-1} \binom{k}{j} B_k = 0 \quad \text{for} \quad k \geq 2.$$

For Bernoullitallene gælder en række formler. Vi vil specielt fremhæve Euler's formel:

$$B_{2k} = (-1)^{k-1} \frac{2(2k)!}{(2\pi)^{2k}} \zeta(2k),$$

og von Staudt/Clausens formel (1840):

$$B_{2k} + \sum_{p-1 \,|\, 2k,\ p \text{ primtal}} \frac{1}{p} \equiv 0 \pmod 1.$$

Sidstnævnte formel viser, at nævneren i B_{2k} er givet ved den simple formel

$$\prod_{p-1 \,|\, 2k,\ p \text{ primtal}} p.$$

Kummer fandt (1850) de irregulære primtal < 100, nemlig 37, 59 og 67. Senere (1874) undersøgte han primtal < 164 og fandt (efter "mühsame Rechnungen") yderligere følgende irregulære primtal: 101, 103, 131, 149, 157.

Den danske matematiker K. L. Jensen var den første der viste, at der er uendeligt mange irregulære primtal (endda af formen $l \equiv -1 \pmod 4$). Det er stadig uklart, om der er uendeligt mange regulære primtal.

Der henvises til indledningen og i øvrigt til P. Ribenboim: 13 *Lectures on Fermat's Last Theorem*, 1979.

I det medfølgende PARI-program KUMMER er beregnet en tabel over Bernoullital B_{2k}, $k \leq 20$, samt en tabel over irregulære primtal < 500. Ved mere omfattende beregninger af irregulære primtal er det ikke hensigtsmæssigt at bruge Bernoullital, der er besværlige at beregne og optager for megen lagerplads. I stedet benyttes forskellige kongruensbetingelser for potenssummer.

Opgaver:

Opgave 1. Betragt $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$ og l et ulige primtal. Som sædvanligt er $\lambda = 1 - \zeta$. Find direkte diskriminanten $D(1, \lambda, \ldots, \lambda^{l-2})$.

Opgave 2. Betragt $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$ og l et ulige primtal. Som sædvanligt er $K_0 = K \cap \mathbb{R}$. Vis, at

$$O_{K_0} = O_K \cap K_0 = O_K \cap \mathbb{R}.$$

Vis herved, at sættet $(\omega_1, \ldots, \omega_{(l-1)/2})$, hvor

$$\omega_j = 2\cos\tfrac{2\pi j}{l} \quad \text{for} \quad 1 \leq j \leq \tfrac{1}{2}(l-1),$$

udgør en $\mathbb{Z}$-basis for O_{K_0}. Idet $S = S_{K_0/\mathbb{Q}}$, skal man vise, at der for $1 \leq r, s \leq (l-1)/2$ gælder

$$S(\omega_r \omega_s) = \begin{cases} -2 & \text{for} \quad r \neq s, \\ l-2 & \text{for} \quad r = s. \end{cases}$$

Vis herved, at diskriminanten d_0 for O_{K_0} er bestemt ved

$$d_0 = l^{\frac{l-3}{2}}.$$

Opgave 3. Betragt $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$ og l et ulige primtal. Som sædvanligt er $K_0 = K \cap \mathbb{R}$. Vis, at $l = \lambda_0^{(l-1)/2}\epsilon_0$, hvor $\lambda_0 = 2 - 2\cos(2\pi/l)$ og $\epsilon_0 \in {O_{K_0}}^{\times}$.

Opgave 4. Betragt $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$ og l et ulige primtal. Som sædvanligt er $K_0 = K \cap \mathbb{R}$. Vis, at regulatorerne R for K og R_0 for K_0 opfylder relationen

$$R = 2^{\frac{l-3}{2}} R_0.$$

Opgave 5. Betragt $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$ og l et ulige primtal. Vis, at O_K er euklidisk mht. normen for $l = 3, 5, 7$. (H. W. Lenstra, Jr. har udstrakt den angivne liste til også at omfatte $l = 11$).

Vink: Lad $\alpha \in K$ være skrevet (ikke entydigt!) på formen

$$\alpha = u_0 + u_1\zeta + \cdots + u_{l-1}\zeta^{l-1} = f(\zeta), \quad \text{hvor} \quad u_0, u_1, \ldots, u_{l-1} \in \mathbb{Q}.$$

Vis først formlen

$$\sum_{k=1}^{\frac{l-1}{2}} f(\zeta^k)f(\zeta^{-k}) = \sum_{k=1}^{\frac{l-1}{2}} \left(\sum_{i=0}^{l-1} u_i\zeta^{ik}\right)\left(\sum_{j=0}^{l-1} u_j\zeta^{-jk}\right)$$
$$= \tfrac{1}{2}(l-1)\sum_{i=1}^{l-1} u_i^2 - \sum_{0\le i<j\le l-1} u_iu_j$$
$$= \tfrac{1}{2}\sum_{0\le i<j\le l-1}(u_i-u_j)^2.$$

Anvend derpå uligheden mellem geometrisk og aritmetisk middelværdi til at vise, at

$$\sqrt[\frac{l-1}{2}]{N(\alpha)} \le \frac{1}{l-1}\sum_{0\le i<j\le l-1}(u_i-u_j)^2.$$

Vis derpå, at der til ethvert givet sæt $(u_0,\ldots,u_{l-1}) \in \mathbb{R}^n$ findes et sæt $(v_0,\ldots,v_{n-1}) \in \mathbb{R}^n$ med $u_j \equiv v_j \pmod 1$ for $0 \le j \le n-1$, så at

$$(*) \qquad \sum_{0\le i<j\le n-1}(v_i-v_j)^2 \le \frac{n^2-1}{12}.$$

Uligheden (*), der skyldes H. W. Lenstra, Jr., er bedst mulig, idet der gælder lighedstegn, når (og pånær rækkefølge kun når) $u_j \equiv u_0 + j/n \pmod 1$ for $1 \le j \le n-1$.

Opgave 6. Betragt $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/l}$ og l et ulige primtal. Som sædvanligt er $K_0 = K \cap \mathbb{R}$. Vis, at

$$\frac{1-\zeta^j}{1-\zeta}\cdot\frac{1-\zeta^{-j}}{1-\zeta^{-1}} = \left(\frac{\sin\frac{j\pi}{l}}{\sin\frac{\pi}{l}}\right)^2.$$

Vis herved, at

$$\theta_j = \frac{\sin\frac{j\pi}{l}}{\sin\frac{\pi}{l}} \in O_K^\times \quad \text{for} \quad 1 \le j \le l-1.$$

Vink: Benyt Kummer's enhedssætning.

Om enhederne θ_j, som Kummer kaldte *Kreiseinheiten*, gælder følgende vigtige resultat:

$$[U_0 : U] = h(K_0),$$

hvor $U_0 = O_K^\times \cap \mathbb{R}_+$, og U er undergruppen heri frembragt af

$$\{\theta_j \mid 2 \le j \le (l-1)/2\}.$$

5. Dedekind's zeta-funktion

Lad K være et algebraisk tallegeme. Vi vil betragte *Dedekind's zeta-funktion*, der er defineret ved rækken

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

hvor summationen udstrækkes over alle hele idealer $\mathfrak{a} \neq (0)$ i O_K. Den variable s er kompleks og skrives traditionelt $s = \sigma + it$, hvor $\sigma, t \in \mathbb{R}$. Vi viser nedenfor, at rækken er absolut konvergent for $\sigma = \Re s > 1$, og at den fremstillede funktion $\zeta_K(s)$ er holomorf (analytisk) i halvplanen $\{s \in \mathbb{C} \mid \sigma > 1\}$. Det er en vigtig kendsgerning (som vi ikke vil gå ind på), at $\zeta_K(s)$ har en entydig analytisk fortsættelse til $\mathbb{C}$, og at $\zeta(s)$ herved bliver meromorf i $\mathbb{C}$ og tilmed holomorf overalt pånær det ene punkt $s = 1$, hvor der er en pol af 1. orden. Denne pols residuum

$$\lim_{s \to 1}(s-1)\zeta_K(s)$$

er af fundamental betydning i algebraisk talteori. Dette fremgår af følgende

Sætning 94. (Dedekind's klassetalsformel). *Lad K være et vilkårligt algebraisk tallegeme af grad $n = r_1 + 2r_2$. Da gælder formlen*

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}R}{w\sqrt{|d|}} \cdot h,$$

hvor R er regulatoren for $O_K^\times$, w er ordenen af gruppen af enhedsrødder i $O_K^\times$, d er diskriminanten for O_K, og h er klassetallet for K.

Bevis. Vi skal vise, at

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \kappa \cdot h, \tag{1}$$

hvor

$$\kappa = \frac{2^{r_1+r_2}\pi^{r_2}R}{w\sqrt{|d|}}. \tag{2}$$

Vi vil dog nøjes med at vise lidt mindre, nemlig

$$\lim_{s\to 1+}(s-1)\zeta_K(s)=\kappa\cdot h. \tag{1+}$$

I det følgende antager vi, at den variable $s\in]1,\infty[$. Vi skriver nu

$$\zeta_K(s)=\sum_{\mathfrak{a}}\frac{1}{N(\mathfrak{a})^s}=\sum_{C\in\mathrm{Cl}(K)}f(s,C),$$

hvor vi for hver idealklasse $C\in\mathrm{Cl}(K)$ sætter

$$f(s,C)=\sum_{\mathfrak{a}\in C}\frac{1}{N(\mathfrak{a})^s}, \tag{3}$$

Det er overalt underforstået, at $\mathfrak{a}\neq(0)$ er et helt ideal i O_K. Det bemærkes, at rækken i (3) for $s>1$ er delrække af en konvergent række med positive led og derfor selv konvergent. Ideen er nu at vise, at

$$\lim_{s\to 1+}(s-1)f(s,C)=\kappa. \tag{4+}$$

uafhængigt af $C\in\mathrm{Cl}(K)$. Da $h=|\mathrm{Cl}(K)|$ vil (4+) medføre (1+).

Lad $\mathfrak{a}'\in C^{-1}$ være et fast valgt helt ideal, og lad $\mathfrak{a}\neq(0)$ være et helt ideal i O_K. Da gælder

$$\mathfrak{a}\in C\Leftrightarrow\mathfrak{a}\mathfrak{a}'\sim(1)\Leftrightarrow\mathfrak{a}=(\alpha)/\mathfrak{a}',\quad \alpha\in\mathfrak{a}'\setminus\{0\},$$

idet

$$\mathfrak{a}'\,|\,(\alpha)\Leftrightarrow(0)\neq(\alpha)\subseteq\mathfrak{a}'\Leftrightarrow\alpha\in\mathfrak{a}'\setminus\{0\},$$

Vi har derfor

$$f(s,C)=N(\mathfrak{a}')^s\sum_{(\alpha)\subseteq\mathfrak{a}'}N((\alpha))^{-s}$$

eller

$$f(s,C)=N(\mathfrak{a}')^s{\sum_{\alpha\in\mathfrak{a}'}}'|N(\alpha)|^{-s}, \tag{5}$$

hvor $\sum'$ angiver, at der i hver klasse af associerede elementer i $\mathfrak{a}'$ (bortset fra nulklassen) skal udtages præcist et α.

Vi benytter nu de tidligere betragtede afbildninger

$$\varphi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \quad \text{og} \quad l : (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \to \mathbb{R}^{r_1+r_2},$$

der var defineret ved henholdsvis

$$\varphi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)),$$

og

$$l(x) = (\log|x_1|, \dots, \log|x_{r_1}|, 2\log|x_{r_1+1}|, \dots, 2\log|x_{r_1+r_2}|).$$

Vi minder endvidere om, at $O_K^\times$ har en naturlig gruppevirkning på $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ ved, at

$$(\epsilon, x) \mapsto \varphi(\epsilon) \cdot x = (\sigma_1(\epsilon)x_1, \dots, \sigma_{r_1+r_2}(\epsilon)x_{r_1+r_2}).$$

Lad nu $\{\epsilon_1, \dots, \epsilon_r\}$, hvor $r = r_1+r_2-1$, være et system af fundamentalenheder i $O_K^\times$, og definér $(e, e_1, \dots, e_r)$ ved

$$e = (1, \dots, 1, 2, \dots 2), \ e_j = L(\epsilon_j) = l \circ \varphi(\epsilon_j), \ 1 \le j \le r,$$

idet der er r_1 1-taller og r_2 2-taller i e. Det er tidligere vist, at

$$\operatorname{span}_{\mathbb{R}}(e_1, \dots, e_r) = \Pi = \{(\lambda_1, \dots, \lambda_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \mid \lambda_1 + \cdots \lambda_{r_1+r_2} = 0\},$$

og da $e \notin \Pi$, er derfor $(e, e_1, \dots, e_r)$ en $\mathbb{R}$-basis for $\mathbb{R}^{r_1+r_2}$. Vi sætter

$$\mathcal{P} = \{\xi e + \xi_1 e_1 + \cdots + \xi_r e_r\} \mid \xi \in \mathbb{R}, \ \xi_j \in [0,1[\quad \text{for} \quad 1 \le j \le r\},$$

og definerer $X \subset (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ ved

$$x \in X \Leftrightarrow \begin{cases} l(x) \in \mathcal{P}, \\ \operatorname{Arg} x_1 \in [0, 2\pi/w[. \end{cases}$$

Endelig sættes

$$X_0 = X \cap \{x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \mid |N(x)| \le 1\}.$$

Vi påstår, at følgende gælder:

(i) X er en kegle i $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ med toppunkt i 0.

(ii) X er et fundamentalområde for gruppevirkningen af $O_K^\times$ på $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$.

(iii) $\mathrm{vol}(X_0) = 2^{r_1}\pi^{r_2}R/w$.

Inden vi viser disse påstande i almindelighed, vil vi først betragte situationen, når $[K:\mathbb{Q}] = 2$. Der er to tilfælde:

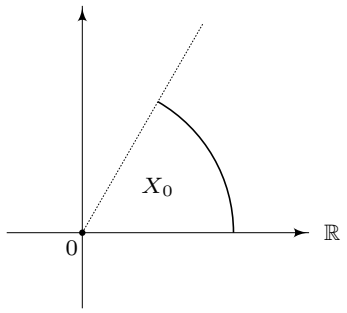
1) $r_1 = 0, r_2 = 1$ (K imaginært kvadratisk): Da er

$$(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times = \mathbb{C}^\times,$$

og

$$X = \{x_1 \in \mathbb{C}^\times \mid 0 \leq \mathrm{Arg}\ x_1 < 2\pi/w\},$$

hvor $w = 4$ for $K = \mathbb{Q}(\sqrt{-1})$ og $w = 6$ for $K = \mathbb{Q}(\sqrt{-3})$ og $w = 2$ i alle andre tilfælde.



X er altså et vinkelrum af størrelse $2\pi/w$. Det er klart, at X er fundamentalområde for gruppen $O_K^\times = \{e^{2\pi ij/w} \mid 1 \leq j \leq w\}$. Endvidere er $\mathrm{vol}(X_0) = \pi/w$, hvilket er i overensstemmelse med (*iii*), da $r_1 = 0,\ r_2 = 1,\ R = 1$.

2) $r_1 = 2, r_2 = 0$ (K reelt kvadratisk): Da er

$$(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times = \mathbb{R}^{2\,\times} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1x_2 = N(x) \neq 0\}.$$

I dette tilfælde er $r = 1$ og vælges fundamentalenheden $\epsilon > 1$, er $\varphi(\epsilon) = (\epsilon, \pm\epsilon^{-1})$. Derfor er

$$e = (1,1),\ e_1 = (\log\epsilon, -\log\epsilon).$$

For $(t_1, t_2) \in \mathbb{R}^2$ er

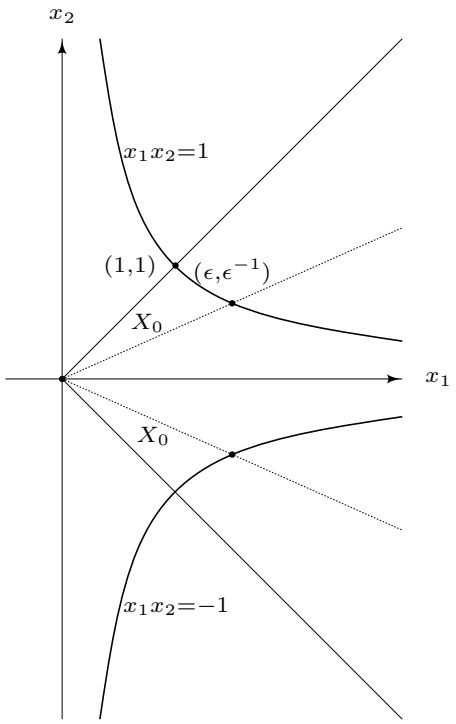
$$(t_1, t_2) = \frac{t_1 + t_2}{2}e + \frac{t_1 - t_2}{2\log\epsilon}e_1.$$

Derfor gælder

$$l(x) = (\log|x_1|, \log|x_2|) \in \mathcal{P} \Leftrightarrow \log|x_1/x_2|/\log\epsilon^2 \in [0,1[\Leftrightarrow 1 \leq |x_1/x_2| < \epsilon^2.$$

Da $w = 2$, er derfor

$$X = \{x = (x_1, x_2) \in \mathbb{R}^2 \mid x_1 > 0,\ 1 \leq x_1/|x_2| < \epsilon^2\}.$$



Det er geometrisk klart, at X er fundamentalområde for gruppen

$$O_K^\times = \{\pm\epsilon^n \mid n \in \mathbb{Z}\}.$$

Endvidere er

$$\mathrm{vol}(X_0) = 2\left(\int_0^1 t dt + \int_1^\epsilon \frac{dt}{t} - \int_0^\epsilon \frac{t}{\epsilon^2} dt\right) = 2(\tfrac{1}{2} + \log\epsilon - \tfrac{1}{2}) = 2\log\epsilon,$$

hvilket er i overensstemmelse med (iii), da $r_1 = 2,\ r_2 = 0,\ R = \log\epsilon,\ w = 2$.

Vi vender nu tilbage til beviset for påstandene (i), (ii) og (iii):

(i). Vi skal vise, at $x \in X,\ t > 0 \Rightarrow tx \in X$. Da

$$\text{Arg } (tx)_1 = \text{Arg } tx_1 = \text{Arg } x_1,$$

og

$$\begin{aligned} l(tx) =&(\log t + \log|x_1|, \dots, \log t + \log|x_{r_1}|, \\ &\quad 2\log t + 2\log|x_{r_1+1}|, \dots, 2\log t + 2\log|x_{r_1+r_2}|) \\ =&(\log t)e + l(x), \end{aligned}$$

er dette imidlertid klart.

(ii). Vi skal vise, at der til et givet $y \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ findes præcist et par $(\epsilon, x) \in O_K^\times \times X$, så at

$$\varphi(\epsilon) \cdot x = y. \tag{6}$$

Antag, at (6) gælder. Ved at anvende afbildningen l fås da

$$l(\varphi(\epsilon)) + l(x) = l(y). \tag{7}$$

Da

$$l(\varphi(\epsilon)) \in \Pi_0 = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r,\ l(x) \in \mathcal{P},$$

og $\mathcal{P}$ er et fundamentalområde for virkningen af $(\Pi_0, +)$ på $\mathbb{R}^{r_1+r_2}$, fastlægger (7) entydigt værdien af $l(\varphi(\epsilon))$, dvs. ϵ er bestemt pånær en faktor ζ, som er en w'te enhedsrod. Da $[0, 2\pi/w[$ er et fundamentalområde for virkningen af gruppen af enhedsrødder i $O_K^\times$ på mængden af argumenter $= \mathbb{R} \pmod{2\pi}$, er faktoren entydigt bestemt ved at Arg $x_1 \in [0, 2\pi/w[$. Denne analyse viser, at der højst findes et par (ϵ, x) som tilfredsstiller (6). Omvendt bestemmes imidlertid ved den anvendte fremgangsmåde et sådant par.

(iii). Det fremgår af (ii), at mængderne

$$X_j = \varphi(e^{2\pi ij/w}) \cdot X_0,\ 0 \le j < w,$$

er disjunkte, og at

$$T = \bigcup_{j=0}^{w-1} X_j = \{x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \mid l(x) \in \mathcal{P},\ |N(x)| \le 1\}.$$

Da afbildningen $x \mapsto y \cdot x$ er en lineær afbildning af $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ af determinant $N(y)$, er specielt afbildningen $x \mapsto \varphi(e^{2\pi ij/w}) \cdot x$ en volumenbevarende afbildning af $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$. Følgelig er

$$\mathrm{vol}(X_0) = \tfrac{1}{w}\mathrm{vol}(T).$$

Da T er symmetrisk mht. koordinaterne $x_1, \ldots, x_{r_1}$, er derfor

$$\mathrm{vol}(X_0) = \frac{2^{r_1}}{w}\mathrm{vol}(T_+), \tag{8}$$

hvor

$$T_+ = \{x \in (\mathbb{R}_+^{r_1} \times \mathbb{C}^{r_2})^\times \mid l(x) \in \mathcal{P},\ |N(x)| \leq 1\}.$$

For at vise (*iii*) skal vi derfor godtgøre, at

$$\mathrm{vol}(T_+) = \pi^{r_2} R. \tag{9}$$

For at udføre volumenberegningen i (9) skiftes først fra de retvinklede koordinater:

$$x_1, \ldots, x_{r_1}, x_{r_1+1} = x'_{r_1+1} + ix''_{r_1+1}, \ldots, x_{r_1+r_2} = x'_{r_1+r_2} + ix''_{r_1+r_2}$$

til polære koordinater:

$$\rho_1, \ldots, \rho_{r_1}, \rho_{r_1+1}, \varphi_1, \ldots, \rho_{r_1+r_2}, \varphi_{r_2},$$

idet koordinatskiftet er givet ved:

$$\begin{aligned} x_j &= \rho_j \quad \text{for} \quad 1 \leq j \leq r_1, \\ x'_{r_1+j} &= \rho_{r_1+j}\cos\varphi_j \quad \text{for} \quad 1 \leq j \leq r_2, \\ x''_{r_1+j} &= \rho_{r_1+j}\sin\varphi_j \quad \text{for} \quad 1 \leq j \leq r_2. \end{aligned}$$

Volumenfaktoren (= absolutværdien af funktionaldeterminanten) ved beregning af volumen i polære koordinater er derfor

$$\rho_{r_1+1} \cdots \rho_{r_1+r_2}.$$

For $x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ er $l(x)$ udtrykt ved den naturlige basis for $(\mathbb{R}^{r_1+r_2})$ givet ved

$$\begin{aligned} l(x) =& (l_1(x), \ldots, l_{r_1+r_2}(x)) \\ =& (\log|x_1|, \ldots, \log|x_{r_1}|, 2\log|x_{r_1+1}|, \ldots, 2\log|x_{r_1+r_2}|), \end{aligned}$$

hvor

$$\sum_{j=1}^{r_1+r_2} l_j(x) = \log|N(x)|.$$

På den anden side kan $l(x)$ fremstilles ved basen $(e, e_1, \dots, e_r)$:

$$l(x) = \xi e + \xi_1 e_1 + \cdots + \xi_r e_r,$$

hvor $e, e_1, \dots, e_r$ udtrykkes ved den naturlige basis på følgende måde:

$$\begin{aligned}
e &= (1, \dots, 1, 2, \dots 2),\\
e_1 &= (\log|\sigma_1(\epsilon_1)|, \dots, \log|\sigma_{r_1}(\epsilon_1)|, 2\log|\sigma_{r_1+1}(\epsilon_1)|, \dots, 2\log|\sigma_{r_1+r_2}(\epsilon_1)|),\\
&\vdots\\
e_r &= (\log|\sigma_1(\epsilon_r)|, \dots, \log|\sigma_{r_1}(\epsilon_r)|, 2\log|\sigma_{r_1+1}(\epsilon_r)|, \dots, 2\log|\sigma_{r_1+r_2}(\epsilon_r)|).
\end{aligned}$$

Heraf fås

$$\sum_{j=1}^{r_1+r_2} l_j(x) = (r_1 + 2r_2)\xi + \sum_{k=1}^{r} \xi_k \log|N(\epsilon_k)| = n\xi.$$

Ved at sammenholde de to udtryk for $\sum l_j(x)$ fås altså

$$\xi = \tfrac{1}{n}\log|N(x)|,$$

dvs. $|N(x)| \le 1$ modsvarer $\xi \le 0$. Vi finder derfor

$$\mathrm{vol}(T_+) = (2\pi)^{r_2} \int_\Omega \rho_{r_1+1} \cdots \rho_{r_1+r_2} d\rho_1 \cdots d\rho_{r_1+r_2},$$

hvor

$$\begin{aligned}
\Omega = \{&(\rho_1, \dots, \rho_{r_1+r_2}) \in \mathbb{R}_+^{r_1+r_2} \mid (\log\rho_1, \dots, \log\rho_{r_1},\\
&2\log\rho_{r_1+1}, \dots, 2\log\rho_{r_1+r_2}) = \xi e + \xi_1 e_1 + \cdots + \xi_r e_r,\ \xi \le 0,\ \xi_j \in [0,1[\}.
\end{aligned}$$

Dette udtryk for $\mathrm{vol}(T_+)$ kan simplificeres ved at indføre de variable $\tau_1, \dots, \tau_{r_1+r_2}$ ved

$$\tau_j = \begin{cases} \rho_j & \text{for} \quad 1 \le j \le r_1, \\ \rho_j^2 & \text{for} \quad r_1 < j \le r_1 + r_2. \end{cases}$$

Vi finder herved

$$\mathrm{vol}(T_+) = \pi^{r_2} \int_{\Omega'} d\tau_1 \cdots d\tau_{r_1+r_2},$$

hvor

$$\begin{aligned}\Omega' =&\{(\tau_1,\dots,\tau_{r_1+r_2})\in\mathbb{R}_+^{r_1+r_2}\mid(\log\tau_1,\dots,\log\tau_{r_1+r_2})\\ &=\xi e+\xi_1e_1+\cdots+\xi_re_r,\ \xi\le 0,\ \xi_j\in[0,1[\}.\end{aligned}$$

Endelig erstattes parameteren ξ af ξ_0 givet ved

$$\xi_0=e^{n\xi}=\tau_1\cdots\tau_{r_1+r_2}, \tag{10}$$

idet parameterintervallet $\xi\le 0$ modsvarer $\xi_0\in]0,1]$. Herved fås

$$\mathrm{vol}(T_+)=\pi^{r_2}\int_{]0,1[^{r_1+r_2}}\left\|\frac{\partial\tau}{\partial\xi}\right\|d\xi_0\cdots d\xi_r, \tag{11}$$

hvor $\|\frac{\partial\tau}{\partial\xi}\|$ er absolutværdien af funktionaldeterminanten for afbildningen

$$(\xi_0,\dots,\xi_r)\mapsto(\tau_1,\dots,\tau_{r_1+r_2})$$

givet ved

$$\log\tau_k=\left(\tfrac{1}{n}\log\xi_0+\sum_{j=1}^{r}\xi_j\log|\sigma_k(\epsilon_j)|\right)f_k,$$

hvor

$$f_k=\begin{cases}1 & \text{for}\quad 1\le k\le r_1,\\ 2 & \text{for}\quad r_1<k\le r_1+r_2.\end{cases}$$

Følgelig er

$$\frac{\partial\tau_k}{\partial\xi_j}=\begin{cases}\tau_k\frac{f_k}{n\xi_0} & \text{for}\quad j=0,\\ \tau_kf_k\log|\sigma_k(\epsilon_j)|=\tau_kL_k(\epsilon_j) & \text{for}\quad 1\le j\le r.\end{cases}$$

Altså er

$$\left\|\frac{\partial\tau}{\partial\xi}\right\|=\tau_1\cdots\tau_{r_1+r_2}\frac{1}{n\xi_0}|\det B|=\frac{1}{n}|\det B|, \tag{12}$$

hvor

$$B=\begin{pmatrix}1 & \dots & 1 & 2 & \dots & 2\\ L_1(\epsilon_1) & \dots & L_{r_1}(\epsilon_1) & L_{r_1+1}(\epsilon_1) & \dots & L_{r_1+r_2}(\epsilon_1)\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ L_1(\epsilon_r) & \dots & L_{r_1}(\epsilon_r) & L_{r_1+1}(\epsilon_r) & \dots & L_{r_1+r_2}(\epsilon_r)\end{pmatrix}.$$

Ved at addere alle øvrige søjler i B til den første søjle og derpå udvikle determinanten efter denne søjle fås

$$|\det B| = nR, \tag{13}$$

hvor R er regulatoren for K. Derfor er $\|\frac{\partial\tau}{\partial\xi}\| = R$, og af (11)-(13) fås nu (9) og dermed (*iii*).

Ifølge egenskab (*ii*) kan vi omskrive formel (5) til

$$f(s,C) = N(\mathfrak{a}')^s \sum_{x\in M\cap X} |N(x)|^{-s}, \tag{14}$$

hvor $M = \varphi(\mathfrak{a}')$ er indlejringen af $\mathfrak{a}'$ i $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. Vi har tidligere vist, at $\Lambda = \varphi(O_K)$ er et fuldt gitter i $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ med gitterdeterminant

$$d(\Lambda) = 2^{-r_2}\sqrt{|d|}.$$

Da $[\Lambda : M] = [\varphi(O_K) : \varphi(\mathfrak{a}')] = |O_K/\mathfrak{a}'| = N(\mathfrak{a}')$ følger heraf, at M er et fuldt gitter i $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ med gitterdeterminant

$$d(M) = N(\mathfrak{a}')d(\Lambda) = 2^{-r_2}N(\mathfrak{a}')\sqrt{|d|}. \tag{15}$$

Vi vil sluttelig vise, at

$$\lim_{s\to 1^+}(s-1)\sum_{x\in M\cap X}|N(x)|^{-s} = \frac{\mathrm{vol}(X_0)}{d(M)}. \tag{16}$$

Vi bemærker dog først, at (16) sammen med (15), (14) og (*iii*) viser den ønskede relation (4+).

Sæt for $t > 1$:

$$\mathcal{N}(t) = |M\cap tX_0| = |\tfrac{1}{t}M\cap X_0|.$$

Ifølge (*i*) er derfor $\mathcal{N}(t)$ antallet af punkter i $M\cap X$ for hvilke $|N(x)|\le t^n \Leftrightarrow |N(x)|^{1/n}\le t$. Da

$$\mathrm{vol}(X_0) = \lim_{t\to\infty}\mathcal{N}(t)d(\tfrac{1}{t}M) = d(M)\lim_{t\to\infty}\mathcal{N}(t)t^{-n},$$

er

$$\lim_{t\to\infty}\mathcal{N}(t)t^{-n} = \mathrm{vol}(X_0)/d(M).$$

Lad nu $x_1, x_2, \ldots$ være samtlige punkter i $M \cap X$ ordnet efter voksende værdier af $|N(x)|$, og sæt $t_k = |N(x_k)|^{1/n}$. Af definitionen på $\mathcal{N}(t)$ følger da, at der for ethvert $\epsilon > 0$ gælder, at

$$\mathcal{N}(t_k - \epsilon) < k \leq \mathcal{N}(t_k),$$

hvoraf

$$\frac{\mathcal{N}(t_k - \epsilon)}{t_k^n} < \frac{k}{t_k^n} \leq \frac{\mathcal{N}(t_k)}{t_k^n}.$$

Da

$$\lim_{k \to \infty} \frac{\mathcal{N}(t_k)}{t_k^n} = \frac{\mathrm{vol}(X_0)}{d(M)},$$

findes der derfor til det givne $\epsilon > 0$ et $k_0 = k_0(\epsilon)$, så at

$$(1 - \epsilon)\frac{\mathrm{vol}(X_0)}{d(M)} < \frac{k}{t_k^n} < (1 + \epsilon)\frac{\mathrm{vol}(X_0)}{d(M)} \quad \text{for} \quad k \geq k_0.$$

Da $t_k = |N(x_k)|^{1/n}$ følger heraf for $k \geq k_0$ og $s > 1$:

$$(17) \qquad (1 - \epsilon)^s \left(\frac{\mathrm{vol}(X_0)}{d(M)}\right)^s \frac{1}{k^s} < \frac{1}{|N(x_k)|^s} < (1 + \epsilon)^s \left(\frac{\mathrm{vol}(X_0)}{d(M)}\right)^s \frac{1}{k^s}.$$

Vi vil senere vise, at

$$(18) \qquad \lim_{s \to 1_+} (s - 1) \sum_{k=1}^{\infty} \frac{1}{k^s} = 1.$$

Af (18) fås for $k_0 \in \mathbb{N}$:

$$\lim_{s \to 1_+} (s - 1) \sum_{k \geq k_0} \frac{1}{k^s} = 1,$$

og kombineret med (17) følger nu umiddelbart, at

$$\begin{aligned}(1 - \epsilon)\frac{\mathrm{vol}(X_0)}{d(M)} &\leq \liminf_{s \to 1_+} (s - 1) \sum_k \frac{1}{|N(x_k)|^s} \leq \limsup_{s \to 1_+} (s - 1) \sum_k \frac{1}{|N(x_k)|^s} \\ &\leq (1 + \epsilon)\frac{\mathrm{vol}(X_0)}{d(M)}.\end{aligned}$$

I $\sum_k$ er i første instans $k \geq k_0$, men da gælder disse uligheder også for $k \in \mathbb{N}$, og det er denne form, vi benytter i det følgende. Da ulighederne gælder for ethvert $\epsilon > 0$, fås for $\epsilon \to 0_+$:

$$\lim_{s \to 1_+} (s-1) \sum_{k \in \mathbb{N}} \frac{1}{|N(x_k)|^s} = \frac{\mathrm{vol}(X_0)}{d(M)}.$$

Hermed er sætningen bevist. □

Dirichlet karakterer. Lad G være en endelig abelsk gruppe af orden $m = |G|$. Vi vil sædvanligvis anvende multiplikativ skrivemåde og betegner da gruppens etelement med e og det inverse til $a \in G$ med a^{-1}.

Definition. En afbildning $\chi : G \to \mathbb{C}^\times$ kaldes en *karakter* på G, hvis

$$\chi(ab) = \chi(a)\chi(b) \quad \text{for} \quad a, b \in G,$$

dvs hvis χ er en gruppehomomorfi af $(G, \cdot)$ ind i $(\mathbb{C}^\times, \cdot)$.

Bemærkning. Da $\chi(a)^m = \chi(a^m) = \chi(e) = 1$, for ethvert $a \in G$, er alle værdier for χ derfor m'te enhedsrødder.

Lad $V = V_G$ være vektorrummet af alle funktioner $f : G \to \mathbb{C}$. I V indføres på naturlig måde et *indre produkt* $(\cdot, \cdot)$ ved

$$(f, g) = \frac{1}{m} \sum_{a \in G} f(a)\overline{g(a)} \quad \text{for} \quad f, g \in V.$$

Herved bliver V et m-dimensionalt unitært rum, og den tilsvarende *norm* $\| \cdot \| : V \to [0, \infty[$ er givet ved

$$\|f\|^2 = \frac{1}{m} \sum_{a \in G} |f(a)|^2.$$

Vi vil undertiden også benytte betegnelsen

$$\mathcal{M}(f) = \frac{1}{m} \sum_{a \in G} f(a)$$

for *middelværdien* af funktionen $f \in V$.

Lad $\hat{G}$ være mængden af alle karakterer på G. Da er $\hat{G} \subset V = V_G$. Ved punktvis multiplikation: $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ for $a \in G$ defineres en multiplikation i $\hat{G}$, idet $\chi_1\chi_2$ er en karakter, når χ_1, χ_2 er det. Med denne multiplikation bliver $\hat{G}$ en gruppe med $\chi_0 = 1_G$ som etelement og med $\chi^{-1} = \overline{\chi}$. Betegnelser: $\hat{G}$ kaldes *karaktergruppen* for G, og χ_0 *hovedkarakteren* for G.

Det kan endelig noteres, at karaktererne $\chi \in \hat{G}$ udgør et ortonormalsystem i det unitære rum $V = V_G$. Da alle værdier for en karakter χ er m'te enhedsrødder, er

$$\|\chi\|^2 = \frac{1}{m}\sum_{a\in G} 1 = 1 \quad \text{for} \quad \chi \in \hat{G}.$$

For to forskellige karakterer $\chi_1, \chi_2 \in \hat{G}$ er $(\chi_1, \chi_2) = \mathcal{M}(\chi_1\overline{\chi_2})$, og det skal derfor vises, at $\mathcal{M}(\chi) = 0$, når $\chi \in \hat{G} \setminus \{\chi_0\}$. For en karakter $\chi \neq \chi_0$ findes et $b \in G$, så at $\chi(b) \neq 1$, og der gælder da

$$\mathcal{M}(\chi) = \frac{1}{m}\sum_{a\in G}\chi(ab) = \frac{1}{m}\sum_{a\in G}\chi(a)\chi(b) = \chi(b)\mathcal{M}(\chi).$$

Men da $\chi(b) \neq 1$ følger heraf, at $\mathcal{M}(\chi) = 0$.

Af dette resultat følger, at karaktererne på G er lineært uafhængige funktioner i $V = V_G$, hvorfor $|\hat{G}| \leq m = |G| = \dim_{\mathbb{C}} V$. For at kunne vise mere om dette, har vi brug for følgende sætning om abelske grupper:

Sætning 95. (Struktursætning for abelske grupper). *Enhver endeligt frembragt abelsk gruppe er isomorf med det (ydre) direkte produkt af endeligt mange cykliske grupper.*

Bevis. Ved dette bevis benyttes additiv skrivemåde. Lad derfor $(G, +)$ være en abelsk gruppe med frembringere $g_1, \ldots, g_n$, og lad $E = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (med n addender) være en fri abelsk gruppe af rang n og med kanonisk basis $(e_1^*, \ldots, e_n^*)$. Lad $\varphi : E \to G$ være homomorfien definereret ved

$$\varphi\left(\sum_{j=1}^{n} x_j e_j^*\right) = \sum_{j=1}^{n} x_j g_j, \quad x_j \in \mathbb{Z}.$$

Da φ er surjektiv er $G \simeq E/F$, hvor $F = \ker\varphi$. Ifølge elementardivisorsætningen (sætning 52) findes der da en basis $(e_1, \ldots, e_n)$ for E og en basis

$(f_1, \ldots, f_r)$ for F, således at $f_j = m_j e_j$ med $m_j \in \mathbb{N}$ for $1 \leq j \leq r \leq n$. Men heraf følger, at

$$G \simeq \mathbb{Z}/(m_1\mathbb{Z}) \oplus \cdots \oplus \mathbb{Z}/(m_r\mathbb{Z}) \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z},$$

med $n - r$ eksemplarer af $\mathbb{Z}$. □

Korollar. *Enhver endelig abelsk gruppe er isomorf med det (ydre) direkte produkt af endeligt mange endelige cykliske grupper.*

Sætning 96. *Lad G være en endelig abelsk gruppe af orden $m = |G|$. Da er $|\hat{G}| = m$. Karaktererne i $\hat{G}$ udgør en ortonormal basis for det unitære rum $V = V_G$, og $\hat{G} \simeq G$. For karaktererne $\chi \in \hat{G}$ gælder følgende ortogonalitetsrelationer:*

$$\frac{1}{m}\sum_{a\in G}\chi(a) = \begin{cases} 1 & \text{når} \quad \chi = \chi_0, \\ 0 & \text{når} \quad \chi \neq \chi_0, \end{cases}$$

og

$$\frac{1}{m}\sum_{\chi\in\hat{G}}\chi(a) = \begin{cases} 1 & \text{når} \quad a = e, \\ 0 & \text{når} \quad a \neq e. \end{cases}$$

Bevis. Ifølge korollaret til sætning 95 kan vi antage, at $G = C_{m_1} \times \cdots \times C_{m_r}$, hvor C_{m_j} er cyklisk af orden m_j og med frembringer a_j for $1 \leq j \leq r$. Et vilkårligt element $a \in G$ har da formen

$$a = (a_1^{\alpha_1}, \ldots, a_r^{\alpha_r}), \quad \text{hvor} \quad \alpha_j \in \mathbb{Z}/(m_j\mathbb{Z}), \quad 1 \leq j \leq r.$$

Vi får da defineret $m = m_1 \cdots m_r$ forskellige karakterer $\chi \in \hat{G}$ ved at sætte

$$\chi(a) = \zeta_1^{\alpha_1} \cdots \zeta_r^{\alpha_r},$$

hvor ζ_j er en vilkårlig m_j'te enhedsrod for $1 \leq j \leq r$. Karaktergruppen $\hat{G}$ er det (indre) direkte produkt af de cykliske undergrupper

$$\hat{G}_j = \langle\chi_j\rangle, \quad \text{hvor} \quad \chi_j(a) = e^{2\pi i\alpha_j/m_j}, \quad 1 \leq j \leq r.$$

Følgelig er $\hat{G} \simeq G$. Påstanden vedrørende ortonormal basis følger nu af tidligere bemærkninger.

Vi har tidligere vist den første ortogonalitetsrelation, som siger, at $\mathcal{M}(\chi) = 1$ for $\chi = \chi_0$ og ellers 0. Denne ortogonalitetsrelation udtrykker derfor præcist, at matricen

$$M = \frac{1}{\sqrt{m}} \left(\chi_r(a_s)\right)_{r,s=1,\dots,m}$$

hvor $\chi_1, \dots, \chi_m$ er samtlige karakterer på G, og $a_1, \dots, a_m$ er samtlige elementer i G, er en unitær matrix, dvs. opfylder relationen

$$MM^* = M\overline{M^t} = I,$$

Den anden ortogonalitetsrelation følger nu af, at den transponerede til en unitær matrix er unitær. Hermed er sætningen bevist. □

Definition. En afbildning $\chi : \mathbb{Z} \to \mathbb{C}$ kaldes en *Dirichlet karakter modulo* D, hvor $D \in \mathbb{N}$, hvis χ har følgende egenskaber:

(*i*) χ er periodisk med periode D,

(*ii*) $\chi(a) = 0$, når $\gcd(a, D) > 1$,

(*iii*) restriktionen af χ til den primiske restklassegruppe $G = (\mathbb{Z}/D\mathbb{Z})^\times$ modulo D er en karakter på G.

Dirichlet karakteren, der er 1 på de primiske restklasser modulo D og ellers 0, kaldes *hovedkarakteren* modulo D, og den betegnes χ_0.

En afbildning $\chi : \mathbb{Z} \to \mathbb{C}$ kaldes en *Dirichlet karakter*, hvis χ er en Dirichlet karakter modulo D for et $D \in \mathbb{N}$.

En Dirichlet karakter χ kaldes *kvadratisk*, såfremt $\chi \neq \chi_0$ og $\chi^2 = \chi_0$, og den kaldes *lige* hhv. *ulige*, såfremt χ som funktion på $\mathbb{Z}$ er lige hhv. ulige.

Bemærkning. Enhver Dirichlet karakter χ er stærkt multiplikativ, dvs. $\chi(ab) = \chi(a)\chi(b)$ for $a, b \in \mathbb{Z}$. Dette følger direkte af definitionen. Da $\chi(-1)^2 = \chi(1) = 1$ er $\chi(-1) = \pm 1$ for enhver Dirichlet karakter χ, hvorfor $\chi(-a) = \chi(-1)\chi(a) = \pm\chi(a)$. Dette viser, at enhver Dirichlet karakter χ enten er lige (når $\chi(-1) = 1$) eller ulige (når $\chi(-1) = -1$).

Lad χ' være en Dirichlet karakter modulo D', og lad $D' \mid D$, hvor $D \in \mathbb{N}$. Man kan da definere $\chi : \mathbb{Z} \to \mathbb{C}$ ved

$$\chi(a) = \begin{cases} \chi'(a) & \text{når} \quad \gcd(a, D) = 1, \\ 0 & \text{når} \quad \gcd(a, D) > 1. \end{cases}$$

Det er klart, at χ er en Dirichlet karakter modulo D, og karakteren χ siges at være *induceret* af χ'.

Definition. En Dirichlet karakter χ modulo D, kaldes *primitiv*, såfremt χ ikke er induceret af nogen Dirichlet karakter χ' modulo D', hvor $D' \neq D$.

Sætning 97. *Enhver Dirichlet karakter χ er induceret af en entydigt bestemt primitiv karakter. Modulus af denne primitive karakter betegnes $\mathfrak{f} = \mathfrak{f}_\chi$ og kaldes χ's minimale modulus (tysk: Führer, engelsk: conductor).*

Bevis. 1. Hvis $D' \mid D$ vil enhver primisk restklasse $a' \pmod{D'}$ indeholde et tal a som er primisk med D. For at vise dette lader vi P betegne produktet af alle primfaktorer p i D, for hvilke $p \nmid D'$. Da er $\gcd(P, D') = 1$, og der findes derfor $x, y \in \mathbb{Z}$, så at $xP + yD' = a' - 1$. Sæt $a = a' - yD' = 1 + xP$. Da er $\gcd(a, D) = 1$, idet der for et primtal p gælder, at $p \nmid a$, hverken når $p \mid D'$ eller når $p \mid P$. Dette viser påstanden.

2. Hvis $\chi \pmod{D}$ er induceret af både $\chi' \pmod{D'}$ og $\chi'' \pmod{D''}$, da er χ også induceret af $\tilde{\chi} \pmod{\tilde{D}}$, hvor $\tilde{D} = \gcd(D', D'')$, og

$$\tilde{\chi}(\tilde{a}) = \begin{cases} 0, & \text{når} \quad \gcd(\tilde{a}, \tilde{D}) > 1, \\ \chi(a), & \text{når} \quad \gcd(\tilde{a}, \tilde{D}) = 1,\ a \equiv \tilde{a} \pmod{\tilde{D}},\ \text{og } \gcd(a, D) = 1. \end{cases}$$

Bemærk, at for $\gcd(\tilde{a}, \tilde{D}) = 1$ er $\chi(a) = \chi'(a) = \chi''(a)$, hvorfor restriktionen af χ til sådanne a er periodisk med perioder D' og D'' og dermed med periode $\tilde{D}$. Ifølge denne bemærkning og punkt 1 er $\tilde{\chi}$ da defineret på $\mathbb{Z}$, og $\tilde{\chi}$ inducerer tydeligvis χ. Hvis specielt $D' = D''$, viser konstruktionen, at $\tilde{D} = D' = D''$ og $\tilde{\chi} = \chi' = \chi''$. Bemærk også, at $\tilde{\chi}$ inducerer χ' og χ''.

3. Lad $\chi^{(j)} \pmod{D^{(j)}}$, hvor $1 \leq j \leq r$ være samtlige Dirichlet karakterer, som inducerer den givne Dirichlet karakter $\chi \pmod{D}$, og lad $D' = \gcd(D^{(1)}, \ldots, D^{(r)})$. Af punkt 2 sluttes, at der blandt Dirichlet karaktererne $\chi^{(j)} \pmod{D^{(j)}}$, er netop én med $D^{(j)} = D'$. Denne karakter er primitiv, og alle andre karakterer $D^{(j)}$ er induceret af denne og derfor ikke primitive.

Dette viser sætningen. □

Eksempel 39. For ethvert ulige primtal p bestemmer Legendre symbolet $\chi(x) = (\frac{x}{p})$ en kvadratisk, primitiv Dirichlet karakter modulo p.

For $D = 2$ findes kun $1 = \varphi(2)$ Dirichlet karakter, nemlig hovedkarakteren $\chi_0 \pmod{2}$. Denne er ikke primitiv, da den er induceret af hovedkarakteren $\chi_0 \pmod{1}$.

For $D = 4$ findes $2 = \varphi(4)$ Dirichlet karakterer. Foruden hovedkarakteren $\chi_0 \pmod 4$, som ikke er primitiv, er dette χ_4 defineret ved:

$$\chi_4(x) = \begin{cases} 1 & \text{for} \quad x \equiv 1 \pmod 4, \\ -1 & \text{for} \quad x \equiv -1 \pmod 4, \\ 0 & \text{for} \quad x \equiv 0 \pmod 2. \end{cases}$$

Dirichlet karakteren χ_4 er primitiv, da den ikke er induceret af nogen Dirichlet karakter modulo 1 eller 2.

For $D = 8$ findes $4 = \varphi(8)$ Dirichlet karakterer. Foruden hovedkarakteren $\chi_0 \pmod 8$, som ikke er primitiv, er der $\chi_4 \pmod 8$, som er induceret af $\chi_4 \pmod 4$. Endvidere er der χ_8 og $\chi_4\chi_8$, hvor χ_8 er defineret ved:

$$\chi_8(x) = \begin{cases} 1 & \text{for} \quad x \equiv \pm 1 \pmod 8, \\ -1 & \text{for} \quad x \equiv \pm 3 \pmod 8, \\ 0 & \text{for} \quad x \equiv 0 \pmod 2. \end{cases}$$

Dirichlet karaktererne χ_8 og $\chi_4\chi_8$ er primitive, da de ikke er induceret af nogen Dirichlet karakter modulo 1, 2 eller 4.

Sætning 98. *Lad $D \in \mathbb{N}$. Betragt følgende antal:*

$\varphi(D)$ = *antallet af Dirichlet karakterer modulo D,*
$\psi(D)$ = *antallet af primitive Dirichlet karakterer modulo D,*
$\varphi_r(D)$ = *antallet af reelle Dirichlet karakterer modulo D,*
$\psi_r(D)$ = *antallet af reelle primitive Dirichlet karakterer modulo D.*

De fire funktioner $\varphi, \psi, \varphi_r, \psi_r$ er alle multiplikative, og forbundet ved følgende formler:

$$\varphi(D) = \sum_{D' \mid D} \psi(D'),$$

og

$$\varphi_r(D) = \sum_{D' \mid D} \psi_r(D').$$

Endvidere gælder følgende eksplicite formler for værdierne af disse funktioner på en primtalspotens p^n (værdien 1 for $n = 0$ er dog udeladt):

$$\varphi(p^n) = (p-1)p^{n-1} \quad for \quad n > 0,$$

$$\psi(p^n) = \begin{cases} p-2 & for \quad n = 1, \\ (p-1)^2 p^{n-2} & for \quad n > 1, \end{cases}$$

$$\varphi_r(p^n) = 2 \quad for \quad p > 2, \quad n > 0,$$

$$\psi_r(p^n) = \begin{cases} 1 & for \quad p > 2, \quad n = 1, \\ 0 & for \quad p > 2, \quad n > 1, \end{cases}$$

$$\varphi_r(2^n) = \begin{cases} 1 & for \quad n = 1, \\ 2 & for \quad n = 2, \\ 4 & for \quad n > 2, \end{cases}$$

$$\psi_r(2^n) = \begin{cases} 0 & for \quad n = 1, \\ 1 & for \quad n = 2, \\ 2 & for \quad n = 3, \\ 0 & for \quad n > 3. \end{cases}$$

Bevis. Vi vil benytte følgende velkendte resultater om den primiske restklassegruppe $(\mathbb{Z}/D\mathbb{Z})^\times$:
(1)
$$(\mathbb{Z}/D\mathbb{Z})^\times \simeq (\mathbb{Z}/D_1\mathbb{Z})^\times \times (\mathbb{Z}/D_2\mathbb{Z})^\times, \quad \text{når} \quad D = D_1 D_2, \quad \gcd(D_1, D_2) = 1,$$

tillige med

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq C_{(p-1)p^{n-1}} \quad \text{for} \quad p > 2,\ n \in \mathbb{N}, \tag{2}$$

og

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \begin{cases} C_{2^{n-1}} & \text{for} \quad n = 1, 2, \\ C_2 \times C_{2^{n-2}} & \text{for} \quad n > 2. \end{cases} \tag{3}$$

Af (1) følger nu direkte, at φ og φ_r er multiplikative. Endvidere følger de to forbindende formler direkte af sætning 97, når man tæller alle (reelle) primitive Dirichlet karakterer, der kan inducere (reelle) Dirichlet karakterer modulo D. Benyttes *Möbius produktet*

$$(f * g)(n) = \sum_{d \mid n} f(d) g(\tfrac{n}{d}),$$

kan de to formler også udtrykkes:

$$\varphi = \psi * 1 \quad \text{og} \quad \varphi_r = \psi_r * 1,$$

hvor 1 angiver den talteoretiske funktion, der er identisk 1. Det følger heraf, at også ψ og ψ_r er multiplikative og givet ved *Möbius' omvendingsformel*:

$$\psi = \varphi * \mu \quad \text{og} \quad \psi_r = \varphi_r * \mu. \tag{4}$$

Af formlerne (2) og (3) og sætning 96 følger endvidere de angivne formler for $\varphi(p^n)$ og $\varphi_r(p^n)$. I sidstnævnte tilfælde skal det bemærkes, at en cyklisk gruppe $G = \langle a \rangle$ af lige orden har netop 2 reelle karakterer, nemlig χ_0 og χ_1 fastsat ved $\chi_0(a) = 1$ og $\chi_1(a) = -1$.

Af formel (4) følger endelig, at

$$\psi(p^n) = \varphi(p^n) - \varphi(p^{n-1}) \quad \text{og} \quad \psi_r(p^n) = \varphi_r(p^n) - \varphi_r(p^{n-1}),$$

og dette giver nu de resterende formler. □

Korollar. *Lad $D = D_1 D_2$, hvor gcd$(D_1, D_2) = 1$. Da har enhver (reel) Dirichlet karakter $\chi \pmod D$ formen $\chi = \chi_1 \chi_2$, hvor χ_j er en (reel) Dirichlet karakter modulo D_j for $j = 1, 2$. Dirichlet karakteren χ er primitiv, hvis og kun hvis χ_1 og χ_2 begge er det.*

Bevis. Afbildningen $(\chi_1, \chi_2) \mapsto \chi = \chi_1 \chi_2$ ses ved brug af den kinesiske restklassesætning let at være injektiv, og den er derfor pga. multiplikativiteten af φ og φ_r også surjektiv. Dette viser den første påstand. Den anden følger tilsvarende af, at ψ og ψ_r er multiplikative, idet det er oplagt, at χ primitiv forudsætter, at både χ_1 og χ_2 er det. □

Sætning 99. *Samtlige primitive kvadratiske karakterer er angivet i følgende skema, hvor $m = p_1 \cdots p_r$ er et vilkårligt ulige kvadratfrit tal, og m=1 er tilladt undtagen i første linie af skemaet. Karaktererne $(\frac{\cdot}{m})$, χ_4 og χ_8 er defineret ved*

$$\left(\frac{x}{m}\right) = \left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_r}\right),$$

hvor $(\frac{\cdot}{p})$ er Legendre symbolet, og

$$\chi_4(x) = \begin{cases} (-1)^{\frac{x-1}{2}} & \text{for } x \text{ ulige,} \\ 0 & \text{for } x \text{ lige,} \end{cases}$$

og

$$\chi_8(x) = \begin{cases} (-1)^{\frac{x^2-1}{8}} & \text{for } x \text{ ulige,} \\ 0 & \text{for } x \text{ lige.} \end{cases}$$

De primitive kvadratiske karakterer χ er i bijektiv forbindelse med de kvadratiske tallegemer $\mathbb{Q}(\sqrt{d})$ af diskriminant d, idet forbindelsen er givet ved $d = \chi(-1)\mathfrak{f}_\chi$.

$\mathfrak{f}_\chi$	χ	$\chi(-1)$	d
m	$(\frac{\cdot}{m})$	$(-1)^{\frac{m-1}{2}}$	$(-1)^{\frac{m-1}{2}}m$
$4m$	$\chi_4(\frac{\cdot}{m})$	$(-1)^{\frac{m+1}{2}}$	$(-1)^{\frac{m+1}{2}}4m$
$8m$	$\chi_8(\frac{\cdot}{m})$	$(-1)^{\frac{m-1}{2}}$	$(-1)^{\frac{m-1}{2}}8m$
$8m$	$\chi_4\chi_8(\frac{\cdot}{m})$	$(-1)^{\frac{m+1}{2}}$	$(-1)^{\frac{m+1}{2}}8m$

χ er lige hhv ulige, hvis og kun hvis det tilhørende kvadratiske tallegeme er reelt hhv. imaginært.

For den etablerede korrespondance mellem χ og d gælder

$$\chi(p) = \left(\frac{d}{p}\right) \quad \text{for alle primtal} \quad p.$$

Bevis. Af sætning 97 aflæses, at

$$\psi_r(D) = \begin{cases} 1, & \text{hvis} \quad D = m \quad \text{eller} \quad 4m, \\ 2, & \text{hvis} \quad D = 8m, \\ 0 & \text{ellers,} \end{cases}$$

hvor $m = p_1 \cdots p_r$ er et vilkårligt ulige kvadratfrit tal, dvs. $p_1, \ldots, p_r$ er forskellige ulige primtal og $r \geq 0$. Dette viser, at første søjle i tabellen er korrekt udfyldt.

For $\mathfrak{f}_\chi = m$ findes den tilhørende Dirichlet karakter χ ved brug af ovenstående korollar, idet der må gælde $\chi = \chi_1 \cdots \chi_r$, hvor χ_j er en primitiv reel Dirichlet karakter modulo p_j for $1 \leq j \leq r$. Da $\psi_r(p_j) = 1$ er derfor (jf eksempel 39) $\chi_j = (\frac{\cdot}{p_j})$ for $1 \leq j \leq r$. Dette viser, at χ har den i tabellen angivne form. Ved brug af 1. supplement til reciprocitetssætningen fås nu

$$(-1)^{\frac{m-1}{2}} \equiv m = p_1 \cdots p_r \equiv \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) = \left(\frac{-1}{m}\right) \pmod 4,$$

hvilket viser, at $\chi(-1) = (\frac{-1}{m}) = (-1)^{(m-1)/2}$. De hertil korresponderende kvadratiske tallegemer $\mathbb{Q}(\sqrt{d})$ er netop alle med diskriminant $d \equiv 1 \pmod 4$.

Tilfældene $\mathfrak{f}_\chi = 4m, 8m$ behandles på samme måde (jf eksempel 39), men detaljerne forbigås.

Da $d = \chi(-1)\mathfrak{f}_\chi$ er $\operatorname{sign} d = \chi(-1)$, og dette viser umiddelbart, at de reelle kvadratiske tallegemer svarer til de lige karakter og de imaginært kvadratiske tallegemer svarer til de ulige karakterer.

Vi vil endelig vise den angivne formel for $\chi(p)$, og vi nøjes igen med tilfældet $m = p_1 \cdots p_r$. Da formlen gælder, hvis $p \,|\, m$ (begge sider bliver 0), kan vi antage $p \nmid m$. Ved brug af reciprocitetssætningen fås da for p ulige:

$$\begin{aligned}\chi(p) = \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_r}\right) &= (-1)^{\frac{p-1}{2}(\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2})} \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\frac{m-1}{2}} \left(\frac{m}{p}\right) = \left(\frac{(-1)^{\frac{m-1}{2}} m}{p}\right) = \left(\frac{d}{p}\right).\end{aligned}$$

Formlen vises let for $p = 2$. Hermed er sætningen bevist. □

Bemærkning. Karakteren χ, der i kraft af sætning 99 hører til et kvadratisk tallegeme $K = \mathbb{Q}(\sqrt{d})$, kaldes *Kronecker karakteren* for K. Det bemærkes, at den viste relation $\chi(p) = (\frac{d}{p})$ helt fastlægger χ ud fra d, idet enhver primisk restklasse modulo $|d|$ indeholder (uendeligt mange) primtal p ifølge Dirichlet's sætning om primtal i differensrækker.

Definition. Lad χ være en Dirichlet karakter modulo D, og lad $\zeta = e^{2\pi i/D}$. For $c \in \mathbb{Z}$ kaldes summen

$$\tau_c(\chi) = \sum_{x \bmod D} \chi(x)\zeta^{cx},$$

hvor x gennemløber alle restklasser modulo D, en *gaussisk sum*. Specielt kaldes $\tau = \tau_1$ en *normeret gaussisk sum*.

Historisk note. Gauss betragtede sådanne summer i *Disquisitiones Arithmeticae* (Art. 356), når χ er den kvadratiske karakter modulo p, for et ulige primtal p. Han angiver også det korrekte fortegn for denne sum. Dette viste han dog først i 1811 ved brug af formlen

$$\sum_{x=0}^{p-1} \zeta^{x^2} = (\zeta - \zeta^{-1})(\zeta^3 - \zeta^{-3}) \cdots (\zeta^{p-2} - \zeta^{-(p-2)}).$$

Sætning 100. *Lad $\chi \pmod D$ være en vilkårlig primitiv Dirichlet karakter. Der gælder da*

$$\tau_c(\chi) = \overline{\chi(c)}\tau(\chi),$$

og

$$|\tau(\chi)| = \sqrt{D}.$$

Antag dernæst, at χ er en primitiv kvadratisk karakter med $f_\chi = \mathfrak{f}$. Da er

$$\tau(\chi) = \begin{cases} \sqrt{\mathfrak{f}} & \textit{hvis} \quad \chi \quad \textit{er lige,} \\ i\sqrt{\mathfrak{f}} & \textit{hvis} \quad \chi \quad \textit{er ulige.} \end{cases}$$

Bevis. 1. For at vise den første påstand antages først, at $\gcd(c, D) = 1$. Da er

$$\tau(\chi) = \sum_{x \bmod D} \chi(cx)\zeta^{cx} = \chi(c) \sum_{x \bmod D} \chi(x)\zeta^{cx} = \chi(c)\tau_c(\chi).$$

Da $\chi(c)^{-1} = \overline{\chi(c)}$, viser dette rigtigheden af påstanden. Tilbage er det (vanskeligere) tilfælde, hvor $\gcd(c, D) = r > 1$. Da er $\chi(c) = 0$, og vi skal derfor vise, at også $\tau_c(\chi) = 0$. Sæt $D' = D/r$. For ethvert $z \in \mathbb{Z}$, så at $z \equiv 1 \pmod{D}'$ og $\gcd(z, D) = 1$ (for eks. $z = 1$) finder vi

$$\begin{aligned} \tau_c(\chi) &= \sum_{x \bmod D} \chi(x)\zeta^{cx} = \sum_{x \bmod D} \chi(xz)\zeta^{cxz} = \chi(z) \sum_{x \bmod D} \chi(x)\zeta^{cx} \\ &= \chi(z)\tau_c(\chi), \end{aligned}$$

idet de to egenskaber for z benyttes ved henholdvis det tredie og det andet lighedstegn. Hvis derfor $\chi(z) \neq 1$, følger heraf $\tau_c(\chi) = 0$, som ønsket. Alternativt er $\chi(z) = 1$ for alle $z \in \mathbb{Z}$, hvor $z \equiv 1 \pmod{D'}$ og $\gcd(z, D) = 1$. Følgelig er $\chi(z_1) = \chi(z_2) \neq 0$ for alle $z_1, z_2 \in \mathbb{Z}$, hvor $z_1 \equiv z_2 \pmod{D'}$ og $\gcd(z_1, D) = \gcd(z_2, D) = 1$. Men dette viser, at $\chi \pmod{D}$ bestemmer en Dirichlet karakter $\chi' \pmod{D'}$, som inducerer χ, hvilket er en modstrid.

2. For $D \in \mathbb{N}$ betragtes vektorrummet V_D af funktioner $f : \mathbb{Z} \to \mathbb{C}$, der er periodiske med periode D. Med det indre produkt $(\cdot, \cdot)$ defineret ved

$$(f, g) = \frac{1}{D} \sum_{x \bmod D} f(x)\overline{g(x)}$$

bliver V_D et unitært vektorrum af dimension D. Det bemærkes, at alle Dirichlet karakterer modulo D tilhører dette rum. I V_D er endvidere (for $c \in \mathbb{Z}$) funktionerne:

$$f_c : x \mapsto \zeta^{cx}, \quad \text{hvor} \quad \zeta = e^{2\pi i/D}.$$

Udregningen

$$\begin{aligned}(f_c, f_{c'}) =& \frac{1}{D} \sum_{x \bmod D} f_c(x)\overline{f_{c'}(x)} = \frac{1}{D} \sum_{x \bmod D} \zeta^{(c-c')x} \\ =& \begin{cases} 1 & \text{for} \quad c \equiv c' \pmod{D}, \\ 0 & \text{for} \quad c \not\equiv c' \pmod{D} \end{cases}\end{aligned}$$

viser, at $(f_1, \ldots, f_D)$ er en ortonormal basis for V_D. For en Dirichlet karakter χ modulo D er da

$$\chi = \sum_{1}^{D} \alpha_c f_c,$$

hvor

$$\alpha_c = (\chi, f_c) = \frac{1}{D} \sum_{x \bmod D} \chi(x)\zeta^{-cx} = \frac{1}{D}\tau_{-c}(\chi).$$

Ved brug af punkt 1 følger derfor, at

$$|\alpha_c| = \begin{cases} \frac{1}{D}|\tau(\chi)| & \text{for} \quad \gcd(c, D) = 1, \\ 0 & \text{for} \quad \gcd(c, D) > 1. \end{cases}$$

Vi kan nu udregne $\|\chi\|^2$ på to måder:

$$\|\chi\|^2 = \frac{1}{D} \sum_{x \bmod D} |\chi(x)|^2 = \frac{\varphi(D)}{D},$$

og

$$\|\chi\|^2 = \left\| \sum_1^D \alpha_c f_c \right\|^2 = \sum_1^D |\alpha_c|^2 = \frac{\varphi(D)}{D^2} |\tau(\chi)|^2.$$

Sammenligning mellem de to udtryk giver straks $|\tau(\chi)| = \sqrt{D}$.

3. For en reel Dirichlet karakter χ modulo D gælder

$$\overline{\tau(\chi)} = \sum_{x \mod D} \chi(x)\zeta^{-x} = \sum_{x \mod D} \chi(-x)\zeta^x = \chi(-1)\tau(\chi).$$

Sammen med det ovenfor viste gælder derfor for en primitiv reel Dirichlet karakter χ modulo $\mathfrak{f}$:

$$\tau(\chi) = \begin{cases} \pm\sqrt{\mathfrak{f}}, & \text{hvis} \quad \chi(-1) = 1, \\ \pm i\sqrt{\mathfrak{f}}, & \text{hvis} \quad \chi(-1) = -1, \end{cases}$$

eller ækvivalent hermed

$$\tau(\chi)^2 = \chi(-1)\mathfrak{f}.$$

Pånær fortegnsbestemmelsen har vi hermed også vist den sidste påstand. Beviset herfor vil vi forbigå, men der henvises fx til E. Landau: *Vorlesungen über Zahlentheorie, Band* 1, i hvilken der gives 4 forskellige beviser for dette, når χ er den kvadratiske karakter modulo et ulige primtal. Beviset følger derefter let for en vilkårlig primitiv kvadratisk karakter.

Hermed er sætningen bevist. □

Eksempel 40. Vi vil benytte de viste resultater om gaussiske summer til at opnå et kort bevis for reciprocitetssætningen og 2. supplement til denne.

Lad p være et ulige primtal og χ en primitiv kvadratisk karakter, hvor $p \nmid \mathfrak{f} = \mathfrak{f}_\chi$. Idet $\zeta = e^{2\pi i/\mathfrak{f}}$ betragtes de gaussiske summer

$$\tau(\chi) = \sum_{x \mod \mathfrak{f}} \chi(x)\zeta^x, \quad \tau_p(\chi) = \sum_{x \mod \mathfrak{f}} \chi(x)\zeta^{px}.$$

Da $\gcd(p, \mathfrak{f}) = 1$, og χ er reel, følger af sætning 100, at

$$\tau_p(\chi) = \overline{\chi(p)}\tau(\chi) = \chi(p)\tau(\chi). \tag{5}$$

Endvidere følger det af sætning 100 (uden brug af fortegnet for den gaussiske sum), at

$$\tau(\chi)^2 = \chi(-1)\mathfrak{f}. \tag{6}$$

Lad nu $K = \mathbb{Q}(\zeta)$. Vi vil midlertidigt operere i ringen $O_K \supseteq \mathbb{Z}[\zeta]$. Da p er et ulige primtal, og $\chi(x) = 0, \pm 1$, fås ved brug af (5)

$$\begin{aligned}\tau(\chi)^p &\equiv \sum_{x \mod \mathfrak{f}} \chi(x)^p \zeta^{px} \pmod{p} \\ &= \sum_{x \mod \mathfrak{f}} \chi(x)\zeta^{px} = \tau_p(\chi) = \chi(p)\tau(\chi).\end{aligned}$$

Heraf fås

$$\tau(\chi)^2 \left(\chi(p) - (\tau(\chi)^2)^{\frac{p-1}{2}}\right) \equiv 0 \pmod{p},$$

eller ved brug af (6)

$$\chi(-1)\mathfrak{f}\left(\chi(p) - (\chi(-1)\mathfrak{f})^{\frac{p-1}{2}}\right) \equiv 0 \pmod{p}.$$

Da $O_K \cap \mathbb{Q} = \mathbb{Z}$, gælder sidstnævnte kongruens også i $\mathbb{Z}$, og da $p \nmid \chi(-1)\mathfrak{f}$, gælder følgelig

$$\chi(p) \equiv \chi(-1)^{\frac{p-1}{2}} \mathfrak{f}^{\frac{p-1}{2}} \pmod{p}.$$

Ved brug af Euler's kriterium (jf sætning 58) omskrives dette til

$$\chi(p) \equiv \chi(-1)^{\frac{p-1}{2}} \left(\frac{\mathfrak{f}}{p}\right) \pmod{p}.$$

Da begge sider af denne kongruens har værdier ± 1 og $p > 2$, gælder derfor

$$\chi(p) = \chi(-1)^{\frac{p-1}{2}} \left(\frac{\mathfrak{f}}{p}\right). \tag{7}$$

Vi betragter først tilfældet $\mathfrak{f} = q$, hvor $q \neq p$ er et ulige primtal. Da er $\chi = (\frac{\cdot}{q})$, hvorfor (7) specialiserer til

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{q}{p}\right),$$

som ved brug af Euler's kriterium giver reciprocitetssætningen:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Dernæst betragter vi tilfældet $\mathfrak{f} = 8$ med $\chi = \chi_8$. Da χ_8 er lige, giver (7) i dette tilfælde 2. supplement:

$$\left(\frac{2}{p}\right) = \left(\frac{8}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Det kan endelig bemærkes, at

$$\pm\sqrt{\chi(-1)\mathfrak{f}} = \tau(\chi) \in K = \mathbb{Q}(\zeta), \quad \zeta = e^{\frac{2\pi i}{\mathfrak{f}}},$$

hvorfor cirkeldelingslegemet K indeholder det kvadratiske tallegeme

$$k = \mathbb{Q}\left(\sqrt{\chi(-1)\mathfrak{f}}\right).$$

Dette blev vist i sætning 87 i det specielle tilfælde, hvor $\mathfrak{f} = l$ er et ulige primtal.

L-rækker og Euler produkter. I dette afsnit vil vi benytte såkaldte *Dirichlet rækker*, dvs. rækker af formen

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \text{hvor} \quad a_n \in \mathbb{C},\ s = \sigma + it \in \mathbb{C}, \tag{1}$$

og hvor $n^s = e^{s \log n}$. Vi vil specielt interessere os for følgende to typer af Dirichlet rækker:

$$\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

hvor $\mathfrak{a} \neq (0)$ gennemløber alle hele idealer i et algebraisk tallegeme K, dvs. koefficienten a_n er antallet af hele idealer $\mathfrak{a}$ i K med $N(\mathfrak{a}) = n$, samt

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

hvor χ er en vilkårlig Dirichlet karakter. Den første type har vi allerede benyttet til definition af Dedekind's zeta-funktion. Den anden type række kaldes *L-rækken* hørende til Dirichlet karakteren χ, og den benyttes til at definere *L-funktionen* $L(s, \chi)$.

Før vi studerer de nævnte specielle Dirichlet rækker, vil vi først (uden bevis) anføre nogle klassiske konvergenssætninger for Dirichlet rækker:

Sætning 101. *Hvis Dirichlet rækken* (1) *er absolut konvergent i punktet* $s_0 = \sigma_0 + it_0$*, da er den absolut konvergent i halvplanen* $\{s = \sigma + it \mid \sigma \geq \sigma_0\}$*.*

Der findes et entydigt bestemt $\sigma_a \in \mathbb{R} \cup \{\pm\infty\}$*, kaldet den absolutte konvergensabscisse med den egenskab, at (1) er absolut konvergent for* $s \in \mathbb{C}$ *med* $\sigma = \Re s > \sigma_a$ *og ikke absolut konvergent for* $s \in \mathbb{C}$ *med* $\sigma = \Re s < \sigma_a$ [*modificeret, når* $\sigma_a = \pm\infty$]*.*

Sætning 102. *Hvis Dirichlet rækken* (1) *er konvergent i punktet* $s_0 = \sigma_0 + it_0$*, da er den uniformt konvergent i enhver kompakt delmængde af halvplanen* $\{s = \sigma + it \mid \sigma > \sigma_0\}$*. Der findes et entydigt bestemt* $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$*, kaldet konvergensabscissen med den egenskab, at (1) er konvergent for* $s \in \mathbb{C}$ *med* $\sigma = \Re s > \sigma_c$ *og divergent for* $s \in \mathbb{C}$ *med* $\sigma = \Re s < \sigma_c$ [*modificeret, når* $\sigma_c = \pm\infty$]*.*

Dirichlet rækken (1) fremstiller en holomorf funktion i konvergenshalvplanen $\{s \in \mathbb{C} \mid \sigma = \Re s > \sigma_c\}$*.*

Der gælder altid $0 \leq \sigma_a - \sigma_c \leq 1$ [$\sigma_a = \sigma_c$*, hvis en af dem er* $\pm\infty$]*.*

Hvis Dirichlet rækken (1) har en begrænset afsnitsfølge for $s = s_0$*, men er divergent i punktet* $s_0 = \sigma_0 + it_0$*, da er* $\sigma_c = \sigma_0$*.*

Bemærkning. Konvergensteorien for Dirichlet rækker minder meget om den tilsvarende teori for potensrækker. Således svarer de to konvergensabscisser til konvergensradius. To danske matematikere har bidraget til denne teori, nemlig J. L. W. V. Jensen (1859-1925) og H. Bohr (1887-1951).

Sætning 103. *Dirichlet rækken*

$$\sum_1^\infty \frac{1}{n^s}$$

har konvergensabscisser $\sigma_a = \sigma_c = 1$*. Den ved rækken fremstillede funktion* $\zeta(s)$ *er holomorf i halvplanen* $\{s = \sigma + it \mid \sigma > 1\}$*. Denne funktion – Riemann's zeta-funktion – har en entydig analytisk fortsættelse til halvplanen* $\{s = \sigma + it \mid \sigma > 0\}$*. Bortset fra en pol for* $s = 1$ *med residuum* 1 *er* $\zeta(s)$ *holomorf i sidstnævnte halvplan.*

Bevis. Som bekendt giver integralkriteriet umiddelbart, at rækken

$$\sum_1^\infty \frac{1}{n^s}$$

er konvergent for $s = \sigma > 1$ og divergent for $s = 1$. Af sætningerne 101-102 fremgår da, at $\sigma_a = \sigma_c = 1$, samt at $\zeta(s)$ er holomorf i halvplanen $\{s = \sigma + it \mid \sigma > 1\}$.

For at udvide $\zeta(s)$ betragtes Dirichlet rækken

$$\sum_1^\infty \frac{(-1)^{n-1}}{n^s}, \tag{2}$$

der for $s = 0$ har en begrænset men divergent afsnitsfølge. Ifølge sætning 102 er derfor $\sigma_c = 0$, og (2) fremstiller en holomorf funktion $\eta_2(s)$ i halvplanen $\{s = \sigma + it \mid \sigma > 0\}$. For $\Re s > 1$ gælder endvidere

$$\eta_2(s) = \sum_1^\infty \frac{(-1)^{n-1}}{n^s} = \sum_1^\infty \frac{1}{n^s} - 2\sum_1^\infty \frac{1}{(2n)^s} = (1 - 2^{1-s})\zeta(s).$$

Derfor kan $\zeta(s)$ udvides til halvplanen $\Re s = \sigma > 0$ ved at sætte

$$\zeta(s) = (1 - 2^{1-s})^{-1}\eta_2(s),$$

og $\zeta(s)$ bliver herved holomorf i denne halvplan, dog evt. pånær nulpunkterne for funktionen $f_2(s) = 1 - 2^{1-s}$. Disse nulpunkter er

$$s = 1 + \frac{2\pi i n}{\log 2}, \quad \text{hvor} \quad n \in \mathbb{Z},$$

som derfor i første instans må udelades fra definitionsmængden for $\zeta(s)$.

Analogt betragtes Dirichlet rækken

$$1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots, \tag{3}$$

hvor koefficienterne har periode 3. Her vises nu på tilsvarende måde, at Dirichlet rækken (3) bestemmer en holomorf funktion $\eta_3(s)$ i halvplanen $\{s = \sigma + it \mid \sigma > 0\}$, og at $\eta_3(s) = (1 - 3^{1-s})\zeta(s)$ for $\Re s > 1$. Derfor kan $\zeta(s)$ også udvides til halvplanen $\Re s = \sigma > 0$ ved at sætte

$$\zeta(s) = (1 - 3^{1-s})^{-1}\eta_3(s),$$

og $\zeta(s)$ bliver herved holomorf i denne halvplan, dog evt. pånær nulpunkterne for funktionen $f_3(s) = 1 - 3^{1-s}$. Disse nulpunkter er

$$s = 1 + \frac{2\pi i m}{\log 3}, \quad \text{hvor} \quad m \in \mathbb{Z}.$$

Af identitetsætningen for holomorfe funktioner følger, at de to udvidelser af $\zeta(s)$ stemmer overens pånær i de nævnte nulpunkter. Imidlertid kan det let ses, at tallet 1 er det eneste fælles nulpunkt. Thi antag, at

$$1 + \frac{2\pi i n}{\log 2} = 1 + \frac{2\pi i m}{\log 3}.$$

Da er $2\pi i(n \log 3 - m \log 2) = 0$, altså $3^n = 2^m$, og dette er pga. den entydige primfaktorisering i $\mathbb{Q}^\times$ kun muligt for $m = n = 0$. Ved brug af den ene eller den anden af disse udvidelsesmuligheder følger derfor, at ζ-funktionen er holomorf for $\Re s = \sigma > 0$ pånær i punktet $s = 1$. I en udprikket omegn af punktet $s = 1$ gælder

$$\zeta(s) = \frac{\eta_2(s)}{f_2(s)},$$

hvor $f_2(s) = 1 - 2^{1-s}$. Da

$$f_2'(s) = 2^{1-s} \log 2,$$

har $f_2(s)$ følgende Taylorudvikling med centrum i 1:

$$f_2(s) = (\log 2)(s-1) + \cdots .$$

Da

$$\eta_2(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \log 2,$$

følger det, at $\zeta(s)$ har en pol af første orden med residuum 1 for $s = 1$.

Hermed er sætningen bevist. □

Sætning 104. *Lad $\chi \pmod D$ være en vilkårlig Dirichlet karakter. For den tilsvarende L-række*

$$\sum_1^\infty \frac{\chi(n)}{n^s}$$

gælder da, at

$$\sigma_c = \sigma_a = 1, \quad \textit{når} \quad \chi = \chi_0,$$

$$\sigma_c = 0,\ \sigma_a = 1, \quad \textit{når} \quad \chi \neq \chi_0.$$

Den ved L-rækken fremstillede L-funktion

$$L(s,\chi) = \sum_1^\infty \frac{\chi(n)}{n^s}, \quad \Re s = \sigma > \sigma_c,$$

er holomorf i den angivne konvergenshalvplan.

Bevis. At L-rækken har $\sigma_a = 1$ for ethvert χ følger af, at

$$\sum_1^\infty |\chi(n)n^{-s}| = \sum_1^\infty \chi_0(n)n^{-\sigma},$$

hvor χ_0 er hovedkarakteren modulo D, og $\sigma = \Re s$. Da $\chi_0(n) = 0, 1$ er sidstnævnte række konvergent for $\sigma > 1$, idet $\sum_1^\infty n^{-\sigma}$ er en konvergent majorantrække. På den anden side er rækken

$$\sum_1^\infty \frac{\chi_0(n)}{n}$$

divergent, hvilket fremgår ved sammenligning med den divergente række

$$\sum_1^\infty \frac{1}{nD+1}.$$

Af det viste fremgår også, at $\sigma_c = 1$ for χ_0.

For $\chi \neq \chi_0$ følger det af den første ortogonalitetsrelation i sætning 96, at $\sum_1^D \chi(n) = 0$, og da χ er periodisk med periode D, har rækken $\sum_1^\infty \chi(n)$ derfor en begrænset afsnitsfølge, medens rækken naturligvis er divergent. Af sætning 102 fremgår da, at $\sigma_c = 0$, når $\chi \neq \chi_0$.

Hermed er sætningen bevist. □

Sætning 105. *Antag, at funktionen $f : \mathbb{N} \to \mathbb{C}$ er stærkt multiplikativ, og at $f(1) = 1$. Da gælder*

$$\sum_1^\infty f(n) = \prod_p \frac{1}{1 - f(p)},$$

forudsat rækken er absolut konvergent.

Bevis. Da rækken er absolut konvergent og dermed konvergent gælder for hvert $n > 1$:

$$f(n)^m = f(n^m) \to 0 \quad \text{for} \quad m \to \infty.$$

Heraf følger, at $|f(n)| < 1$ for $n > 1$. Vi betragter nu et vilkårligt afsnit i produktet:

$$P(x) = \prod_{p \le x} \frac{1}{1 - f(p)} = \prod_{p \le x} \left(1 + f(p) + f(p)^2 + \cdots\right),$$

hvor de uendelige kvotientrækker er absolut konvergente, da $|f(p)| < 1$ for ethvert primtal p. Da produktet af endeligt mange absolut konvergente rækker er absolut konvergent, finder vi

$$P(x) = \sum_{n \in \mathcal{A}(x)} f(n),$$

hvor

$$\mathcal{A}(x) = \{n \in \mathbb{N} \mid \text{alle primfaktorer i } n \text{ er } \le x\}.$$

Følgelig er

$$\sum_1^\infty f(n) - \sum_{n \in \mathcal{A}(x)} f(n) = \sum_{n \in \mathcal{A}'(x)} f(n),$$

hvor $\mathcal{A}'(x) = \mathbb{N} \setminus \mathcal{A}(x)$. Altså er

$$\left| \sum_1^\infty f(n) - P(x) \right| \le \sum_{n \in \mathcal{A}'(x)} |f(n)| \le \sum_{n > x} |f(n)|,$$

eftersom $A(x)$ med sikkerhed indeholder alle $n \le x$. Af den absolutte konvergens af $\sum_1^\infty f(n)$ følger derfor, at

$$P(x) \to \sum_1^\infty f(n) \quad \text{for} \quad x \to \infty.$$

Hermed er sætningen bevist. □

Sætning 106. *For enhver Dirichlet karakter* $\chi \pmod D$ *er*

$$L(s,\chi) = \sum_1^\infty \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}} \quad \textit{for} \quad \Re s > 1.$$

Den angivne produktfremstilling af $L(s,\chi)$ *kaldes Euler-produktet.*

Lad $\chi \neq \chi_0 \pmod D$ *være induceret af den primitive karakter* ψ*. Da gælder*

$$L(s,\chi) = L(s,\psi) \prod_{p \mid D} \left(1 - \frac{\psi(p)}{p^s}\right) \quad \textit{for} \quad \Re s > 0.$$

For $\chi_0 \pmod D$ *gælder*

$$L(s,\chi_0) = \zeta(s) \prod_{p \mid D} \left(1 - \frac{1}{p^s}\right) \quad \textit{for} \quad \Re s > 1.$$

Ved denne formel udvides $L(s,\chi_0)$ *til halvplanen* $\{s = \sigma + it \mid \sigma > 0\}$*, og* $L(s,\chi_0)$ *er holomorf i denne halvplan pånær i punktet* $s = 1$*, hvor* $L(s,\chi_0)$ *har en pol af første orden med residuum*

$$\prod_{p \mid D} \left(1 - \frac{1}{p}\right) = \frac{\varphi(D)}{D}.$$

Bevis. Da L-rækken har $\sigma_a = 1$ ifølge sætning 104, og χ er stærkt multiplikativ følger den første påstand umiddelbart af sætning 105.

For ethvert primtal p er

$$\chi(p) = \begin{cases} \psi(p) & \text{når} \quad p \nmid D, \\ 0 & \text{når} \quad p \mid D. \end{cases}$$

Derfor gælder for $\Re s = \sigma > 1$:

$$\begin{aligned} L(s,\psi) &= \prod_p \left(1 - \frac{\psi(p)}{p^s}\right)^{-1} = \prod_{p \mid D} \left(1 - \frac{\psi(p)}{p^s}\right)^{-1} \prod_{p \nmid D} \left(1 - \frac{\psi(p)}{p^s}\right)^{-1} \\ &= \prod_{p \mid D} \left(1 - \frac{\psi(p)}{p^s}\right)^{-1} \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \mid D} \left(1 - \frac{\psi(p)}{p^s}\right)^{-1} L(s,\chi). \end{aligned}$$

Dette viser den ønskede formel for $\Re s = \sigma > 1$. Ved analytisk fortsættelse gælder den derfor også for $\Re s = \sigma > 0$, når $\chi \neq \chi_0$.

Såfremt $\chi = \chi_0 \pmod D$, er $\psi = \chi_0 \pmod 1$, og formlen for $L(s, \chi_0)$ er derfor specialtilfælde af formlen for $L(s, \chi)$. Da den elementære faktor

$$\prod_{p \mid D} \left(1 - \frac{1}{p^s}\right)$$

er holomorf i $\mathbb{C}$, følger det af sætning 103, at $L(s, \chi_0)$ er holomorf i halvplanen $\{\Re s > 0\}$ pånær i punktet $s = 1$, hvor der er en pol af første orden med det angivne residuum.

Sætning 107. *Lad K være et algebraisk tallegeme, og sæt $N = [K : \mathbb{Q}]$. Da gælder*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}},$$

i halvplanen $\{s = \sigma + it \mid \sigma > \sigma_a\}$, hvor σ_a er den absolutte konvergensabscisse for rækken. Endvidere er $\sigma_c = \sigma_a \leq 1$.

Den angivne produktfremstilling af $\zeta_K(s)$ kaldes Euler-produktet.

Bevis. Idet a_n er antallet af hele idealer $\mathfrak{a}$ i K med $N(\mathfrak{a}) = n$, kan vi skrive

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \sum_{1}^{\infty} \frac{a_n}{n^s}.$$

Da $a_n \geq 0$ for $n \in \mathbb{N}$ og $n^{-\sigma} > 0$ for $\sigma \in \mathbb{R}$, er sidstnævnte række en Dirichlet række med $\sigma_a = \sigma_c$, eftersom begge disse konstanter er bestemt alene ved konvergensforholdene på $\mathbb{R}$. Derfor er Dirichlet rækken absolut konvergent i halvplanen $\{s = \sigma + it \mid \sigma > \sigma_a = \sigma_c\}$ og divergent i halvplanen $\{s = \sigma + it \mid \sigma < \sigma_c = \sigma_a\}$.

Beviset for produktformlen er ganske som i sætning 105 dog med den modifikation, at det her beror på, at O_K er en Dedekind ring, og at idealnormen er stærkt multiplikativ.

For hvert primtal p betragtes primidealdekompositionen

$$(p) = pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

hvor $N(\mathfrak{p}_j) = p^{f_j}$ for $1 \leq j \leq r$, og

$$\sum_{j=1}^{r} e_j f_j = N = [K : \mathbb{Q}].$$

For $s = \sigma > 1$ gælder derfor

$$\prod_{\mathfrak{p} \mid (p)} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \leq \left(\frac{1}{1 - \frac{1}{p^s}} \right)^N,$$

hvorfor

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \leq \prod_{p} \left(\frac{1}{1 - \frac{1}{p^s}} \right)^N = \zeta(s)^N.$$

Heraf følger, at alle afsnit for rækken

$$\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

er opadtil begrænsede ved $\zeta(s)^N$, når $s = \sigma > 1$. Dette viser, at at $\sigma_a \leq 1$.

Hermed er sætningen bevist. □

Bemærkning. Der gælder faktisk altid $\sigma_a = \sigma_c = 1$ for Dedekind's zeta-funktion. Thi hvis $\sigma_a = \sigma_c < 1$, ville $\zeta_K(s)$ være holomorf for $s = 1$, og Dedekind's klassetalsformel ville da give $h = 0$, hvilket er en modstrid.

Sætning 108. *Lad $K = \mathbb{Q}(\sqrt{d})$ være et kvadratisk tallegeme med diskriminant d, og lad χ være den tilhørende Kronecker karakter. Da gælder:*

(i) $\zeta_K(s) = \zeta(s)L(s,\chi)$ *for* $\Re s > 1$.

(ii) $L(1,\chi) \neq 0$.

(iii) $\zeta_K(s)$ *defineret ved (i) for $\sigma > 0$ er holomorf pånær i punktet $s = 1$, hvor $\zeta_K(s)$ har en pol af første orden med residuum $L(1,\chi)$.*

Bevis. *(i)* Ifølge sætning 62 gælder for hvert primtal p:

$$\prod_{\mathfrak{p} \mid (p)} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right) = \left(1 - \frac{1}{p^s}\right) \left(1 - \frac{(\frac{d}{p})}{p^s}\right),$$

idet rigtigheden umiddelbart checkes i de tre tilfælde $(\frac{d}{p}) = 0, \pm 1$. Ved brug af sætningerne 106 og 99 finder vi derfor for $\Re s = \sigma > 1$:

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \prod_p \prod_{\mathfrak{p} \mid (p)} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \prod_p \frac{1}{1 - \frac{1}{p^s}} \frac{1}{1 - \frac{(\frac{d}{p})}{p^s}}$$
$$= \prod_p \frac{1}{1 - \frac{1}{p^s}} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_p \frac{1}{1 - \frac{1}{p^s}} \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} = \zeta(s) L(s, \chi).$$

(ii) Antag (indirekte), at $L(1, \chi) = 0$. Ifølge (i) er $\zeta_K(s)$ da holomorf for $s = 1$, hvorfor

$$\lim_{s \to 1} (s - 1) \zeta_K(s) = 0.$$

Ifølge Dedekind's klassetalsformel er da $h = h(K) = 0$, modstrid!

(iii) følger nu umiddelbart af $(i) - (ii)$ samt sætningerne 103-104.

Hermed er sætningen bevist. □

Sætning 109. *Lad $\chi \pmod D \neq \chi_0$ være en vilkårlig Dirichlet karakter. Da er $L(1, \chi) \neq 0$.*

Bevis. Lad χ_0 være hovedkarakteren modulo D. Da gælder følgende ulighed:

$$L(s, \chi_0)^3 |L(s, \chi)|^4 |L(s, \chi^2)|^2 > 1 \quad \text{for} \quad s = \sigma > 1. \tag{4}$$

Til beviset benyttes uligheden mellem geometrisk og aritmetisk middelværdi (for tre tal):

$$x_1 x_2 x_3 \leq \left(\frac{x_1 + x_2 + x_3}{3} \right)^3 \quad \text{for} \quad x_1, x_2, x_3 \geq 0. \tag{5}$$

Endvidere benyttes den elementære ulighed

$$3 + 4 \cos \vartheta + 2 \cos 2\vartheta \geq 0 \quad \text{for} \quad \vartheta \in \mathbb{R}, \tag{6}$$

der følger af, at venstre side i (6) er $(1 + 2 \cos \vartheta)^2$. Endelig benyttes følgende ulighed:

$$(1 - \alpha)^3 |1 - \alpha e^{i\vartheta}|^4 |1 - \alpha e^{2i\vartheta}|^2 < 1 \quad \text{for} \quad 0 < \alpha < 1, \ \vartheta \in \mathbb{R}. \tag{7}$$

Ulighed (7) fås ud fra (5) (med $x_1 = x_2 = 1 - 2\alpha\cos\vartheta + \alpha^2$ og $x_3 = 1 - 2\alpha\cos 2\vartheta + \alpha^2$) samt (6) på følgende måde:

$$\begin{aligned}(1-\alpha)^3|1-\alpha e^{i\vartheta}|^4|1-\alpha e^{2i\vartheta}|^2 & \\ =&(1-\alpha)^3(1-2\alpha\cos\vartheta+\alpha^2)^2(1-2\alpha\cos 2\vartheta+\alpha^2)\\ \le&(1-\alpha)^3(1-\tfrac{\alpha}{3}(4\cos\vartheta+2\cos 2\vartheta)+\alpha^2)^3\\ \le&(1-\alpha)^3(1+\alpha+\alpha^2)^3=(1-\alpha^3)^3<1.\end{aligned}$$

For at vise (4) betragtes det bidrag til Euler produktet, som hidrører fra et bestemt primtal p:

$$\left((1-\chi_0(p)p^{-s})^3|1-\chi(p)p^{-s}|^4|1-\chi(p)^2p^{-s}|^2\right)^{-1}.$$

Såfremt $p \mid D$ er bidraget 1, og for $p \nmid D$ er bidraget > 1 ifølge (7) anvendt med

$$\alpha = p^{-s} \quad \text{og} \quad e^{i\vartheta} = \chi(p),$$

og dette viser (4).

Efter disse forberedelser kan vi nu vise, at $L(1,\chi) \neq 0$.

Vi betragter først tilfældet, hvor χ ikke er kvadratisk, dvs. $\chi^2 \neq \chi_0$. Antag (indirekte), at $Ł(1,\chi) = 0$. Da har funktionen

$$L(s,\chi_0)^3L(s,\chi)^4L(s,\chi^2)^2,$$

ifølge sætning 106 et nulpunkt for $s = 1$, eftersom $L(s,\chi_0)$ har en pol af første orden, og $L(s,\chi^2)$ er holomorf for $s = 1$, og $4 > 3$. Men dette strider mod (4).

Såfremt χ er kvadratisk, kan vi ifølge sætning 106 antage, at χ er primitiv, og da er $L(s,\chi) \neq 0$ ifølge sætning 108.

Hermed er sætningen bevist. □

Historisk note. Det bemærkelsesværdige trick med at udnytte uligheden (6) til at opnå uligheden (4), går tilbage til J. Hadamard (1896). Han benyttede det på lignende måde til at vise, at $\zeta(s)$ ikke har nulpunkter for $\Re s = 1$. Denne omstændighed er afgørende for det analytiske bevis for *primtalssætningen*. Det bør også fremhæves, at de bærende elementer i det analytiske bevis for Dirichlet's sætning om primtal i differensrækker er sætning 96 (specielt den anden ortogonalitetsrelation) og sætning 109.

Der henvises til fx. A. E. Ingham: *The Distribution of Prime Numbers*, 1932, og T. Estermann: *Introduction to Modern Prime Number Theory*, 1961.

Summation af L-rækker. I dette afsnit vil vise, at $L(1,\chi)$ kan summeres på endelig form, når $\chi \pmod D$ er en fra hovedkarakteren forskellig Dirichlet karakter. På grund af formlen i sætning 106 kan det uden indskrænkning antages, at χ er en primitiv karakter modulo D, hvor $D > 1$. Da χ har periode D, kan vi skrive

$$L(s,\chi) = \sum_{x \pmod D} \chi(x) \sum_{n \equiv x \pmod D} \frac{1}{n^s}.$$

Den inderste række er derfor en Dirichlet række

$$\sum_1^\infty \frac{a_n(x)}{n^s},$$

hvor

$$a_n(x) = \begin{cases} 1 & \text{for} \quad n \equiv x \pmod D, \\ 0 & \text{for} \quad n \not\equiv x \pmod D. \end{cases}$$

Funktionerne $n \mapsto a_n(x)$ er periodiske med periode D, og da vektorrummet V_D af alle funktioner, der har periode D, har en ortonormal basis $(f_1, \ldots, f_D)$, hvor

$$f_c : n \mapsto \zeta^{cn}, \quad \zeta = e^{\frac{2\pi i}{D}} \quad \text{for} \quad 1 \le c \le D,$$

kan $a_n(x)$ på entydig måde skrives

$$a_n(x) = \sum_{c=1}^D b_c(x)\zeta^{cn}.$$

Her er

$$b_c(x) = (a_n(x), f_c) = \frac{1}{D}\zeta^{-cx},$$

hvoraf

$$a_n(x) = \frac{1}{D}\sum_{c=1}^D \zeta^{c(n-x)} = \frac{1}{D}\sum_{c=1}^D \zeta^{c(x-n)}.$$

Vi har derfor

$$\begin{aligned} L(s,\chi) &= \sum_{x \pmod D} \chi(x) \sum_{n=1}^\infty \left(\frac{1}{D} \sum_{c=1}^D \zeta^{c(x-n)} \right) \frac{1}{n^s} \\ &= \frac{1}{D} \sum_{c=1}^D \left(\sum_{x \pmod D} \chi(x)\zeta^{cx} \right) \sum_{n=1}^\infty \zeta^{-cn} \frac{1}{n^s} \\ &= \frac{1}{D} \sum_{c=1}^D \tau_c(\chi) \sum_{n=1}^\infty \zeta^{-cn} \frac{1}{n^s}. \end{aligned}$$

Ved brug af relationen $\tau_c(\chi) = \overline{\chi(c)}\tau(\chi)$ fra sætning 100 og udeladelse af leddet svarende til $c = D$ reduceres udtrykket derfor til

$$L(s,\chi) = \frac{\tau(\chi)}{D}\sum_{c=1}^{D-1}\overline{\chi(c)}\sum_{n=1}^{\infty}\zeta^{-cn}\frac{1}{n^s}.$$

For $1 \le c \le D-1$ er den inderste række en Dirichlet række, som for $s = 0$ har begrænset men divergent afsnitsfølge. Ifølge sætning 102 har hver af disse Dirichlet rækker konvergensabscisse $\sigma_c = 0$, og de er derfor konvergente for $s = 1$. Altså er

$$L(1,\chi) = \frac{\tau(\chi)}{D}\sum_{c=1}^{D-1}\overline{\chi(c)}\sum_{n=1}^{\infty}\frac{1}{n}\zeta^{-cn}.$$

Vi benytter nu, at funktionen

$$\operatorname{Log} z = \log|z| + i\operatorname{Arg} z \quad \text{for} \quad \operatorname{Arg} z \in]-\pi,\pi[$$

er holomorf i den angivne opskårne $\mathbb{C}$-plan med

$$\frac{d}{dz}\operatorname{Log} z = \frac{1}{z}.$$

Endvidere er $\operatorname{Log} z$ en udvidelse af den sædvanlige logaritmefunktion $\log x$, $x > 0$, og

$$-\operatorname{Log}(1-z) = \sum_{n=1}^{\infty}\frac{z^n}{n} \quad \text{for} \quad |z| < 1.$$

Da rækkerne

$$\sum_{n=1}^{\infty}\frac{1}{n}\zeta^{-cn}, \quad 1 \le c \le D-1,$$

er konvergente, følger det nu af Abels's sætning, at

$$\sum_{n=1}^{\infty}\frac{1}{n}\zeta^{-cn} = -\operatorname{Log}(1-\zeta^{-c}) \quad \text{for} \quad 1 \le c \le D-1.$$

Dette giver nu

$$L(1,\chi) = -\frac{\tau(\chi)}{D}\sum_{c=1}^{D-1}\overline{\chi(c)}\operatorname{Log}(1-\zeta^{-c}), \tag{1}$$

som er det søgte endelige udtryk for $L(1,\chi)$.

I det følgende vil vi foretage nogle elementære omskrivninger af (1), og indfører til dette brug forkortelsen

$$S(\chi) = \sum_{c=1}^{D-1} \overline{\chi(c)} \mathrm{Log}\,(1-\zeta^{-c}).$$

Da $0 < c/D < 1$ og

$$1 - e^{-\frac{2\pi ic}{D}} = 2ie^{-\frac{\pi ic}{D}} \frac{e^{\frac{\pi ic}{D}} - e^{-\frac{\pi ic}{D}}}{2i} = 2ie^{-\frac{\pi ic}{D}} \sin\frac{\pi c}{D} = 2\sin\frac{\pi c}{D} e^{i\pi(\frac{1}{2}-\frac{c}{D})},$$

er

$$\mathrm{Log}\,(1-\zeta^{-c}) = \log(2\sin\frac{\pi c}{D}) + i\pi(\frac{1}{2} - \frac{c}{D}).$$

Ved konjugering heraf fås derfor

$$\mathrm{Log}\,(1-\zeta^{c}) = \log(2\sin\frac{\pi c}{D}) - i\pi(\frac{1}{2} - \frac{c}{D}).$$

Vi finder nu

$$\begin{aligned} S(\chi) &= \frac{1}{2}\sum_{c=1}^{D-1} \big(\overline{\chi(c)}\mathrm{Log}\,(1-\zeta^{-c}) + (\overline{\chi(-c)}\mathrm{Log}\,(1-\zeta^{c})\big) \\ &= \frac{1}{2}\sum_{c=1}^{D-1} \overline{\chi(c)}\big(\mathrm{Log}\,(1-\zeta^{-c}) + \chi(-1)\mathrm{Log}\,(1-\zeta^{c})\big). \end{aligned}$$

Ved at indsætte de fundne udtryk for $\mathrm{Log}\,(1-\zeta^{-c})$ og $\mathrm{Log}\,(1-\zeta^{c})$ heri fås endelig følgende:

$$L(1,\chi) = -\frac{\tau(\chi)}{D}\sum_{c=1}^{D-1} \overline{\chi(c)} \log\sin\frac{\pi c}{D} \quad \text{for} \quad \chi \text{ lige}, \tag{2}$$

$$L(1,\chi) = \frac{i\pi\tau(\chi)}{D^2}\sum_{c=1}^{D-1} \overline{\chi(c)}c \quad \text{for} \quad \chi \text{ ulige}. \tag{3}$$

Bemærk, at vi begge steder har simplificeret udtrykket ved brug af

$$\sum_{c=1}^{D-1} \overline{\chi(c)} = 0.$$

Klassetalsformler for kvadratiske tallegemer.

Sætning 110. *(Dirichlet's klassetalsformler). Lad $K = \mathbb{Q}(\sqrt{d})$ være et kvadratisk tallegeme med diskriminant d, og lad χ være den tilhørende Kronecker karakter modulo $D = |d|$. Idet w er antallet af enhedsrødder i K (når $d < 0$), og $\epsilon > 1$ fundamentalenhed (når $d > 0$), er klassetallet h for K givet ved:*

$$h = -\frac{1}{\log \epsilon} \sum_{0<c<\frac{D}{2}} \chi(c) \log \sin \frac{\pi c}{D} \quad \textit{for} \quad d > 0,$$

$$h = -\frac{w}{2D} \sum_{c=1}^{D-1} \chi(c) c \quad \textit{for} \quad d < 0.$$

Bevis. Ifølge Dedekind's klassetalsformel og sætningerne 103 og 108 er

$$h = \frac{w\sqrt{D}}{2^{r_1+r_2}\pi^{r_2}R} L(1,\chi).$$

For $d > 0$ er $w = 2$, $r_1 = 2$, $r_2 = 0$, $R = \log \epsilon$ og (jf sætning 100) $\tau(\chi) = \sqrt{D}$. Formlen følger derfor af (2) ovenfor, idet det yderligere er benyttet, at summen heri er symmetrisk, da χ er lige og $\sin(\pi c/D) = \sin\bigl(\pi(D-c)/D\bigr)$. Et evt. midterste led svarende til $c = D/2$ vil have $\chi(c) = 0$, og det kan derfor udelades.

For $d < 0$ er $r_1 = 0$, $r_2 = 1$, $R = 1$ og (jf sætning 100) $\tau(\chi) = i\sqrt{D}$. Formlen følger derfor af (3) ovenfor.

Hermed er sætningen bevist. □

Korollar. *Lad $K = \mathbb{Q}(\sqrt{d})$ være et reelt kvadratisk tallegeme med diskriminant d (> 0). Sæt*

$$\eta = \prod_{0<a,b<\frac{d}{2},\, \chi(a)=1,\, \chi(b)=-1} \frac{\sin \frac{\pi b}{d}}{\sin \frac{\pi a}{d}}.$$

Da er $\eta = \epsilon^h$, hvor $\epsilon > 1$ er fundamentalenhed i $O_K^\times$.

Eksempel 41. For $K = \mathbb{Q}(\sqrt{5})$, der har diskriminant $d = 5$, er $\chi(1) = 1$, $\chi(2) = (\frac{2}{5}) = -1$. Derfor er

$$\eta = \frac{\sin \frac{2\pi}{5}}{\sin \frac{\pi}{5}} = 2\cos\frac{\pi}{5} = \tfrac{1}{2}(1+\sqrt{5}).$$

Da $\epsilon = (1+\sqrt{5})/2 > 1$ tillige er fundamentalenhed i $O_K^\times$, er $h = 1$. (Jf sætning 79).

Sætning 111. *Lad $K = \mathbb{Q}(\sqrt{d})$ være et imaginært kvadratisk tallegeme med diskriminant $d < -4$, og lad χ være den tilhørende Kronecker karakter modulo $D = -d$. Da er*

$$h = \frac{1}{2 - \chi(2)} \sum_{0<c<\frac{D}{2}} \chi(c).$$

Bevis. Da $w = 2$ følger det af sætning 110, at

$$hD = -\sum_{0<c<D} \chi(c)c.$$

Vi skelner nu mellem to tilfælde 1° D lige og 2° D ulige.

1° D lige: Da er $\chi(D/2) = 0$, hvorfor

$$(*) \qquad hD = -\sum_{0<c<\frac{D}{2}} \chi(c)c - \sum_{0<c<\frac{D}{2}} \chi\left(c+\frac{D}{2}\right)\left(c+\frac{D}{2}\right).$$

I dette tilfælde er

$$\chi(x) = \chi_*(x)\left(\frac{x}{p_1}\right)\cdots\left(\frac{x}{p_r}\right),$$

hvor $\chi_* = \chi_4$, χ_8, $\chi_4\chi_8$ og $p_1, \ldots, p_r$ er de ulige primdivisorer i d. Da

$$\chi_*\left(x+\frac{D}{2}\right) = -\chi_*(x), \quad \left(\frac{x+\frac{D}{2}}{p_j}\right) = \left(\frac{x}{p_j}\right) \quad \text{for} \quad 1 \le j \le r,$$

er

$$\chi\left(x+\frac{D}{2}\right) = -\chi(x) \quad \text{for} \quad x \in \mathbb{Z}.$$

Formlen $(*)$ kan derfor omskrives til

$$hD = \sum_{0<c<\frac{D}{2}} \chi(c)\left(c+\frac{D}{2}-c\right) = \frac{D}{2}\sum_{0<c<\frac{D}{2}} \chi(c),$$

hvilket giver den angivne formel for h, da $\chi(2) = 0$ i dette tilfælde.

2° D ulige: Her benyttes blot, at $\chi(-1) = -1$, hvorfor $(*)$ nu kan omskrives til

$$hD = -\sum_{0<c<\frac{D}{2}} \chi(c)c - \sum_{0<c<\frac{D}{2}} \chi(D-c)(D-c) = \sum_{0<c<\frac{D}{2}} \chi(c)(D-2c),$$

dvs.

$$(**) \qquad hD = D\sum_{0<c<\frac{D}{2}} \chi(c) - 2\sum_{0<c<\frac{D}{2}} \chi(c)c.$$

Da D og χ er ulige, fås på den anden side

$$\begin{aligned} hD &= -\sum_{0<c<D,\, c \text{ lige}} \chi(c)c - \sum_{0<c<D,\, \text{lige}} \chi(D-c)(D-c) \\ &= \sum_{0<c<D,\, \text{lige}} \chi(c)(D-2c) = \chi(2)\sum_{0<c<\frac{D}{2}} \chi(c)(D-4c). \end{aligned}$$

Da $\chi(2) = \pm 1$ giver dette

$$(***) \qquad hD\chi(2) = D\sum_{0<c<\frac{D}{2}} \chi(c) - 4\sum_{0<c<\frac{D}{2}} \chi(c)c.$$

Af $(**)$ og $(***)$ fås nu

$$hD(2-\chi(2)) = D\sum_{0<c<\frac{D}{2}} \chi(c),$$

hvilket giver den angivne formel for h.

Hermed er sætningen bevist. □

Eksempel 42. For $K = \mathbb{Q}(\sqrt{-5})$, der har diskriminant $d = -20$, er Kronecker karakteren χ givet ved

$$\chi(x) = \begin{cases} (-1)^{\frac{x-1}{2}}\left(\frac{x}{5}\right), & x \text{ ulige}, \\ 0, & x \text{ lige}. \end{cases}$$

Altså er

$$h = \frac{1}{2}\sum_{0<c<10} \chi(x) = \frac{1}{2}\cdot 4 = 2.$$

Bemærk, at det også er muligt at bruge formlen

$$h = \frac{\sqrt{20}}{\pi} L(1, \chi)$$

til beregning af h. Det følger fx ved en simpel vurdering, at

$$1.3 < 1 + \frac{1}{3} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} - \frac{1}{17} - \frac{1}{19} < L(1, \chi) < 1 + \frac{1}{3} + \frac{1}{7} + \frac{1}{9} < 1.6,$$

hvorfor

$$1.8 < \frac{\sqrt{20}}{\pi} \cdot 1.3 < h < \frac{\sqrt{20}}{\pi} \cdot 1.6 < 2.3.$$

Konklusionen er derfor igen $h = 2$ (jf eksempel 26).

Bemærkning. Det medfølgende PARI-program CLASSNBS benytter sætningerne 110 og 111 til beregning af klassetal af kvadratiske tallegemer. Jf også opgave 17, der omtaler den såkaldte *genusteori* for imaginært kvadratiske tallegemer, og sætningerne 72 og 73 om imaginært kvadratiske tallegemer med klassetal 1.

Klassetalsformler for cirkeldelingslegemer. Vi anfører uden bevis en række vigtige resultater, der alle skyldes Kummer. I disse sætninger er $\zeta = e^{2\pi i/l}$, hvor l er et ulige primtal, og $K = \mathbb{Q}(\zeta)$ og $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$ er de tilhørende cirkeldelingslegemer.

Sætning 112. *I cirkeldelingslegemet K gælder følgende dekompositionsformler for opløsning af pO_K i primidealer i O_K, idet p betegner et vilkårligt primtal:*

For $p = l$ er

$$lO_K = \mathfrak{p}^{l-1},$$

hvor $\mathfrak{p} = (\lambda) = (1 - \zeta)$.

For $p \neq l$ er

$$pO_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g, \quad g = g_p,$$

hvor alle primidealer $\mathfrak{p}_j$ er uforgrenede og har samme grad f_p, dvs. $f_p g_p = [K : \mathbb{Q}] = l - 1$. Endvidere er f_p givet ved

$$f_p = \min\{r \in \mathbb{N} \mid p^r \equiv 1 \pmod{l}\}.$$

I cirkeldelingslegemet K_0 gælder tilsvarende:
For $p = l$ er

$$lO_{K_0} = \mathfrak{p}_0^{\frac{l-1}{2}},$$

hvor $\mathfrak{p}_0 = (\lambda_0) = (2 - 2\cos(2\pi/l))$.
For $p \neq l$ er

$$pO_{K_0} = \mathfrak{p}_1^0 \cdots \mathfrak{p}_{g^0}^0, \quad g^0 = g_p^0,$$

hvor alle primidealer $\mathfrak{p}_j^0$ er uforgrenede og har samme grad f_p^0, dvs. $f_p^0 g_p^0 = [K_0 : \mathbb{Q}] = (l-1)/2$. Endvidere er f_p^0 givet ved

$$f_p^0 = \min\{r \in \mathbb{N} \mid p^r \equiv \pm 1 \pmod{l}\}.$$

Sætning 113. *For cirkeldelingslegemerne K og K_0 gælder for $\Re s > 0$ følgende produktformler for Dedekind's zeta-funktion:*

$$\frac{\zeta_K(s)}{\zeta(s)} = \prod_{\chi \pmod{l},\ \chi \neq \chi_0} L(s, \chi),$$

$$\frac{\zeta_{K_0}(s)}{\zeta(s)} = \prod_{\chi \pmod{l},\ \chi \neq \chi_0,\ \chi \text{ lige}} L(s, \chi).$$

Sætning 114. *(Kummer's klassetalsformler). For cirkeldelingslegemerne K og K_0 gælder følgende formler for klassetallene $h = h(K)$ og $h_0 = h(K_0)$:*

$$h = \frac{l^{\frac{l}{2}}}{2^{\frac{l-3}{2}} \pi^{\frac{l-1}{2}} R} \prod_{\chi \pmod{l},\ \chi \neq \chi_0} L(1, \chi),$$

$$h_0 = \frac{l^{\frac{l-3}{4}}}{R} \prod_{\chi \pmod{l},\ \chi \neq \chi_0,\ \chi \text{ lige}} L(1, \chi),$$

hvor R er regulatoren for K.

Sætning 115. *For klassetallene $h = h(K)$ og $h_0 = h(K_0)$ er $h = h_0 h^*$, hvor $h^* \in \mathbb{N}$. Primtallet l er regulært, hvis og kun hvis $l \nmid h^*$.*

Bemærkning 1. Da $h^* = h/h_0$ gælder ifølge sætning 114

$$h^* = \frac{l^{\frac{l+3}{4}}}{2^{\frac{l-3}{2}}\pi^{\frac{l-1}{2}}} \prod_{\chi \pmod l,\ \chi \text{ ulige}} L(1,\chi).$$

Da

$$L(1,\chi) = \frac{i\pi\tau(\chi)}{l^2} \sum_{c=1}^{l-1} \overline{\chi(c)}c \quad \text{for} \quad \chi \text{ ulige},$$

kan formlen for h^* omskrives til

$$h^* = \frac{(-1)^{\frac{l-1}{2}}}{(2l)^{\frac{l-3}{2}}} \prod_{\chi \pmod l,\ \chi \text{ ulige}} \sum_{c=1}^{l-1} \overline{\chi(c)}c.$$

Ud fra denne formel kan derpå vises, at

$$l \,|\, h^* \Leftrightarrow l \,|\, B_2B_4\cdots B_{l-3},$$

som ved brug af sætning 115 giver Kummer's berømte betingelser for regularitet (jf 4.10).

Bemærkning 2. Et af hovedemnerne i algebraisk talteori i det 20. århundrede har været studiet af absolut abelske tallegemer K, dvs. algebraiske tallegemer, som er galoiske over $\mathbb{Q}$ og med abelsk Galoisgruppe. Et berømt resultat af Kronecker/Weber udsiger, at de absolut abelske tallegemer præcist er alle cirkeldelingslegemer og deres dellegemer. For ethvert sådant tallegeme kan der (som vi har set det for kvadratiske tallegemer og visse cirkeldelingslegemer) knyttes en gruppe $\mathfrak{X}$ af primitive Dirichlet karakterer med den egenskab, at

$$\zeta_K(s) = \prod_{\chi\in\mathfrak{X}} L(s,\chi).$$

Denne karaktergruppes egenskaber kan benyttes til at udtrykke egenskaber for legemet K. Fx gælder:

(i) $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq \mathfrak{X}$.

(ii) Diskriminanten d for K er givet ved formlen

$$d = \prod_{\chi\in\mathfrak{X}} \chi(-1)\mathfrak{f}_\chi.$$

(*iii*) Det mindste cirkeldelingslegeme $\mathbb{Q}(e^{2\pi i/\mathfrak{f}})$, som indeholder K, er bestemt ved $\mathfrak{f} = \mathrm{lcm}_{\chi\in\mathfrak{X}}\mathfrak{f}_\chi$.

Fundamentale bidrag til denne teori er givet af H. Hasse og H. W. Leopoldt. Et interessant led i denne teori er anvendelsen af *p-adiske L-funktioner*, der blev indført af Kubota-Leopoldt i 1964. Det er herved muligt at opstille en *p-adisk klassetalsformel* i fuldstændig analogi med Dedekind's klassetalsformel. Se fx K. Iwasawa: *Lectures on p-adic L-Functions*, 1972 eller S. Lang: *Cyclotomic Fields*, 1980.

Mere generelt har man i den såkaldte *klasselegemeteori* med stor succes studeret relativt abelske udvidelser K/k, hvor k og K er algebraiske tallegemer. Fundamentale bidrag til denne teori er givet af bl.a. H. Weber, D. Hilbert, P. Furtwängler, T. Takagi, H. Hasse, E. Artin og C. Chevalley.

Opgaver:

Opgave 1. Bestem alle Dirichlet karakterer modulo 10, 12 og 16. Angiv for hver af disse karakterer den primitive karakter, som inducerer den.

Opgave 2. Gennemfør beviset for sætning 99 i de oversprungne tilfælde.

Opgave 3. Vis ved brug af Gauss' formel

$$\sum_{x=0}^{p-1} \zeta^{x^2} = (\zeta - \zeta^{-1})(\zeta^3 - \zeta^{-3}) \cdots (\zeta^{p-2} - \zeta^{-(p-2)}),$$

at

$$\tau(\chi) = \begin{cases} \sqrt{p} & \text{hvis} \quad p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{hvis} \quad p \equiv -1 \pmod 4, \end{cases}$$

når p er et ulige primtal, $\zeta = e^{2\pi i/p}$ og $\chi = (\frac{\cdot}{p})$.

Opgave 4. Betragt en vilkårlig primitiv kvadratisk karakter χ med minimal modulus $\mathfrak{f}_\chi = \mathfrak{f}$. Vis på grundlag af resultatet i opgave 3, at

$$\tau(\chi) = \begin{cases} \sqrt{\mathfrak{f}} & \text{hvis} \quad \chi \quad \text{er lige}, \\ i\sqrt{\mathfrak{f}} & \text{hvis} \quad \chi \quad \text{er ulige}, \end{cases}$$

Vink: Betragt først tilfældene $\chi = \chi_4$, χ_8, $\chi_4\chi_8$, samt $\chi = (\frac{\cdot}{p})$, hvor p er et ulige primtal. Benyt dernæst i tilfældet $\mathfrak{f} = p_1 \cdots p_r$ den gaussiske sum $\tau_c(\chi)$, hvor

$$c = \sum_{j=1}^{r} \frac{\mathfrak{f}}{p_j}$$

til beregning af $\tau(\chi)$.

Opgave 5. For $K = \mathbb{Q}(\sqrt{2})$ er

$$\zeta_K(s) = \zeta(s)L(s,\chi), \quad \text{hvor} \quad \chi = \chi_8.$$

Slut heraf, at

$$\frac{1}{\sqrt{2}} \log(1+\sqrt{2}) = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} + \frac{1}{15} + \cdots .$$

Vis dernæst denne formel direkte. Vink: Benyt funktionen

$$F(x) = x - \frac{x^3}{3} - \frac{x^5}{5} + \frac{x^7}{7} + \frac{x^9}{9} - \frac{x^{11}}{11} - \frac{x^{13}}{13} + \frac{x^{15}}{15} + \cdots$$

og dens afledede.

Opgave 6. For $K = \mathbb{Q}(\sqrt{-2})$ er

$$\zeta_K(s) = \zeta(s)L(s,\chi), \quad \text{hvor} \quad \chi = \chi_4\chi_8.$$

Slut heraf, at

$$\frac{\pi}{\sqrt{8}} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11} - \frac{1}{13} - \frac{1}{15} + \cdots .$$

Vis dernæst denne formel direkte. Vink: Benyt funktionen

$$F(x) = x + \frac{x^3}{3} - \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} + \frac{x^{11}}{11} - \frac{x^{13}}{13} - \frac{x^{15}}{15} + \cdots$$

og dens afledede.

Opgave 7. Lad $K = \mathbb{Q}(\sqrt{d})$ være et vilkårligt kvadratisk tallegeme af diskriminant d. Lad χ være den tilhørende Kronecker karakter, og sæt $D = |d| = \mathfrak{f}_\chi$. Vis, at

$$L(1,\chi) = \int_0^1 \frac{\sum_{r=1}^{D-1} \chi(r)x^{r-1}}{1-x^D}\,.$$

Vink: Benyt funktionen

$$F(x,\chi) = \sum_1^\infty \frac{\chi(n)}{n}x^n$$

og dens afledede. Vis dernæst, at integranden har en dekomposition af formen

$$\frac{\sum_{r=1}^{D-1} \chi(r)x^{r-1}}{1-x^D} = \sum_{0<j<\frac{D}{2}} \frac{a_j x + b_j}{1 - 2\cos\frac{2\pi j}{D}\cdot x + x^2}\,,$$

hvor $a_j, b_j \in \mathbb{R}$ for $1 < j < D/2$. Vis specielt, at $a_j = 0$ for $0 < j < D/2$, hvis χ er ulige.

Opgave 8. Vis, at $K = \mathbb{Q}(\sqrt{-23})$ har klassetal $h = 3$.

Opgave 9. Vis, at $K = \mathbb{Q}(\sqrt{-14})$ har klassetal $h = 4$. Vis dernæst, at klassegruppen $\mathrm{Cl}(K) \simeq C_4$. Vink: Vis, at idealklassen, der indeholder idealet $(3, 1 + \sqrt{-14})$ er af 4. orden.

Opgave 10. Kontrollér, at de imaginært kvadratiske tallegemer $K = \mathbb{Q}(\sqrt{d})$, hvor

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163,$$

alle har klassetal $h = 1$.

Opgave 11. Vis sætning 114 på grundlag af sætning 113. Vink: Benyt specielt resultaterne fra opgaverne 2 og 4 i kapitel 4.

Gennemfør derpå udledningen af den angivne formel

$$h^* = \frac{(-1)^{\frac{l-1}{2}}}{(2l)^{\frac{l-3}{2}}} \prod_{\chi \pmod l,\ \chi \text{ ulige}} \sum_{c=1}^{l-1} \overline{\chi(c)} c.$$

Vink: Vis først formlen $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)}$, og tag hensyn til en eventuel reel Dirichlet karakter.

Opgave 12. Benyt formlen for h^* (jf opgave 11) til at vise, at $h^* = 1$ for $l = 3, 5, 7$.

Opgave 13. Betragt *Maillet's determinant*, der for et ulige primtal l er givet ved

$$D_l = \det\left(R(rs^{-1})\right)_{r,s=1,\ldots,(l-1)/2},$$

hvor s^{-1} er en vilkårlig repræsentant for den inverse restklasse modulo l til restklassen repræsenteret ved s, og hvor $R : \mathbb{Z} \to \{0, 1, \ldots, l-1\}$ er defineret ved $R(x) \equiv x \pmod l$.

Vis, at

$$|D_l| = l^{\frac{l-3}{2}} M(l),$$

hvor $M(l) \in \mathbb{N}_0$.

E. Maillet antog (1913), at $M(l) \neq 0$ for alle l. På grundlag af beregninger (for $l \leq 13$) formodede E. Malo, at $M(l) = 1$ for alle l. Men som vist af L.

Carlitz og F. R. Olson (1955), gælder der faktisk $M(l) = h^*(l)$ for alle l, hvor $h^*(l) = h^*$ for cirkeldelingslegemet $K = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/l}$. Det var kendt af Kummer, at $h^*(l) = 1$ for $l \leq 19$, og at $h^*(23) = 3$. Maillet determinanter har været benyttet af D. H. Lehmer og J. M. Masley (1976) til beregning af $h^*(l)$ for $200 < l < 512$.

Opgave 14. Lad $\mathfrak{X}^{prim}$ betegne mængden af alle primitive Dirichlet karakterer. Heri defineres produktet $\chi_1 \cdot \chi_2$ som den primitive Dirichlet karakter, der inducerer Dirichlet karakteren $\chi_1\chi_2$ (punktvis multiplikation).

1) Vis, at $\left(\mathfrak{X}^{prim}, \cdot\right)$ er en gruppe.

2) Bestem alle undergrupper af denne gruppe, som er isomorfe med C_2 og $C_2 \times C_2$.

Opgave 15. Betragt cirkeldelingslegemet $K = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/20}$. Vis, at $G = \mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$, hvor σ, τ er bestemt ved

$$\sigma : \zeta \mapsto \zeta^3, \quad \tau : \zeta \mapsto \zeta^{-1}.$$

Vis, at G har følgende undergrupper ($\neq E, G$):

$$\langle \sigma \rangle, \quad \langle \sigma\tau \rangle, \quad \langle \sigma^2, \tau \rangle, \quad \langle \sigma^2 \rangle, \quad \langle \tau \rangle.$$

Angiv de tilsvarende fixpunktlegemer K', hvor $Q \subset K' \subset K$ i henhold til Galoisteoriens hovedsætning.

Illustrér derpå den anførte sammenhæng mellem absolut abelske udvidelser og grupper af Dirichlet karakterer (jf også opgave 14) ved for hvert dellegeme $K' \subseteq K$ at angive den tilsvarende karaktergruppe $\mathfrak{X} = \mathfrak{X}_{K'}$.

Betragt nu specielt dellegemet

$$K' = \mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(\sqrt{5}, \sqrt{-5}).$$

Vis, at

$$O_{K'} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\tfrac{1}{2}(1 + \sqrt{5}) + \mathbb{Z}i\tfrac{1}{2}(1 + \sqrt{5}).$$

Vis herved, at diskriminanten for K' er $d = 400$, og verificér i dette tilfælde gyldigheden af formlen

$$d = \prod_{\chi \in \mathfrak{X}} \chi(-1)\mathfrak{f}_\chi.$$

Vis endvidere, at

$$O_{K'}^{\times} = \left\{ i^m \left(\tfrac{1}{2}(1+\sqrt{5})\right)^n \mid 0 \le m < 4,\ n \in \mathbb{Z} \right\}.$$

Vis herved, at antallet enhedsrødder og regulatoren for K' er givet ved

$$w = 4, \quad R = 2\log\left(\tfrac{1}{2}(1+\sqrt{5})\right).$$

Vis endelig, at klassetallet for K' er $h = 1$.

Opgave 16. Lad G være en endelig abelsk gruppe, og betragt

$$G^2 = \{x^2 \mid x \in G\} \quad \text{og} \quad G_2 = \{x \in G \mid x^2 = e\}.$$

Vis, at G^2 og G_2 er undergrupper i G. Vis derpå, at

$$G/G^2 \simeq G_2 \simeq C_2^r.$$

Vink: Benyt struktursætningen for abelske grupper til at skrive G som direkte produkt af cykliske grupper af primtalspotensorden, og karakterisér herved r.

Opgave 17. Dennne opgave omhandler den såkaldte *genusteori* for imaginært kvadratiske tallegemer. En tilsvarende teori findes også for reelt kvadratiske tallegemer, men den er noget mere kompliceret.

Betragt det imaginært kvadratiske tallegeme $K = \mathbb{Q}(\sqrt{d})$ af diskriminant $d < 0$. Lad $d = -d_0 p_1 \cdots p_g$, hvor $d_0 = 1, 4, 8$, og $p_1, \ldots, p_g$ er de ulige primdivisorer i d. Kronecker karakteren χ for K er da $\chi = \chi_0\chi_1 \cdots \chi_g$, hvor χ_0 er den tilhørende primitive kvadratiske Dirichlet karakter modulo 1, 4 eller 8, medens

$$\chi_j = \left(\frac{\cdot}{p_j}\right) \quad \text{for} \quad 1 \le j \le g.$$

Endvidere er $G = \mathrm{Cl}(K)$ klassegruppen for K.

1) Vis, at enhver idealklasse $C \in G$ indeholder et helt ideal $\mathfrak{a}$, som er primisk med (d), dvs. med $\mathfrak{a} + (d) = O_K$. Vink: Benyt sætning 39, korollar 3.

Vis tillige, at $\mathfrak{a}$ er primisk med (d) netop hvis $\gcd(N(\mathfrak{a}), d) = 1$.

2) Lad $\mathfrak{a}$ være et helt ideal i O_K, som er primisk med (d). Vis, at

$$\prod_{j=0}^{g} \chi_j(N(\mathfrak{a})) = \chi(N(\mathfrak{a})) = 1.$$

3) Lad $\alpha \in O_K$ med $\gcd(N(\alpha), d) = 1$. Vis, at

$$\chi_j(N(\alpha)) = 1 \quad \text{for} \quad 0 \leq j \leq g.$$

Vink: Begynd med $1 \leq j \leq g$.

4) Lad $C \in G$, og definér for $0 \leq j \leq g$:

$$\chi_j(C) = \chi_j(N(\mathfrak{a})),$$

hvor $\mathfrak{a} \in C$ er et helt ideal, som er primisk med (d).

Vis, at χ_j herved er veldefineret, dvs. uafhængig af valget af $\mathfrak{a}$.

5) Vis, at

$$\prod_{j=0}^{g} \chi_j(C) = 1 \quad \text{for ethvert} \quad C \in G.$$

6) Vis, at

$$\chi_j(C) = \chi_j(C') \quad \text{for} \quad 0 \leq j \leq g,$$

når $C = X^2 C'$ med $X \in G$.

Karaktererne χ_j kaldes *genus karakterer*. Indholdet af punkt 6 er derfor, at genus karaktererne lever på $G/G^2 \simeq G_2$, der kaldes *genus klassegruppen* (jf opgave 16).

7) Vis, at relationen i punkt 5 er den eneste relation mellem genus karaktererne. Med andre ord: til enhver fortegnskombination $(\delta_0, \delta_1, \ldots, \delta_g)$ med $\delta_0 \delta_1 \cdots \delta_g = 1$ og $\delta_0 = 1$, hvis $d_0 = 1$, findes en idealklasse $C \in G$ med

$$\chi_j(C) = \delta_j \quad \text{for} \quad 0 \leq j \leq g.$$

Vink: Benyt Dirichlet's sætning om primtal i differensrækker til at vise, at der findes et primtal p med $\chi_j(p) = \delta_j$ for $0 \leq j \leq g$. Udnyt derpå, at der findes et helt ideal $\mathfrak{p}$ med $N(\mathfrak{p}) = p$.

8) Vis, at der for genus klassegruppen G_2 gælder

$$|G_2| \geq \begin{cases} 2^{g-1}, & \text{hvis} \quad d_0 = 1, \\ 2^g, & \text{hvis} \quad d_0 = 4, 8. \end{cases}$$

Bemærkning: Der gælder faktisk altid lighedstegn i disse uligheder. Af denne formel for $|G_2|$ følger fx, at $h = |G|$ er ulige, hvis og kun hvis $g = 0$ og $d_0 = 4, 8$, dvs. $d = -4, -8$ eller $g = 1$ og $d_0 = 1$, dvs. $d = -p$, hvor $p \equiv -1 \pmod 4$ er et primtal. Sammenlign dette resultat med de medfølgende tabeller over klassetal for imaginært kvadratiske tellegemer.

B. Blandede opgaver

Opgave 1. Lad $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $k = \mathbb{Q}$, Find udtryk for

$$S_{K/k}(a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6}), \;\; N_{K/k}(a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6})$$

for $a_0, a_1, a_2, a_3 \in k$.

Udregn minimalpolynomiet for $\sqrt{2} + \sqrt{3}$.

Udregn $D(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ og $D(1, \sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3)$, og lav en sammenligning mellem de to diskriminanter, der illustrerer transformationsformlen for diskriminanter på side 1.10.

Opgave 2. Lad $f \in \mathbb{Q}[x]$ være et normeret irreducibelt polynomium af grad n og med en rod $\vartheta \in \mathbb{C}$. Vis, at fortegnet for $D(1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1})$ er givet ved formlen $(-1)^{r_2}$, hvor r_2 er antallet af kompleks konjugerede par af ikke reelle rødder for f.

Opgave 3. Lad $K = k(\vartheta)$ være en endelig separabel udvidelse af grad n over k. Lad K^* være et spaltningslegeme for minimalpolynomiet f af grad n, og lad

$$\vartheta = \vartheta^{(1)}, \vartheta^{(2)}, \cdots, \vartheta^{(n)} \tag{1}$$

være de n forskellige rødder i f. Lad G være Galois gruppen for K^*/k. Da G opererer transitivt på mængden (1) findes der automorfier

$$\{\sigma_j \mid 1 \leqq j \leqq n\}\,, \tag{2}$$

så at $\sigma_j(\vartheta) = \vartheta^{(j)}$ for $1 \leqq j \leqq n$. Der er derfor præcis n forskellige virkninger af G på K, nemlig virkningerne af (2). For et vilkårligt element $\omega \in K$ defineres $\omega^{(j)} = \sigma_j(\omega)$ for $1 \leqq j \leqq n$. Lad ω have grad l, hvor $lm = n$, og lad de konjugerede til ω være

$$\omega = \omega_1, \omega_2, \ldots, \omega_l\,. \tag{3}$$

Vis, at

$$\{\omega^{(j)} = \sigma_j(\omega) \mid 1 \leqq j \leqq n\} \tag{4}$$

består af tallene (3), hver m gange, eller sagt på en anden måde, at

$$(-1)^n \prod_{j=1}^{n} (x - \omega^{(j)})$$

er det karakteristiske polynomium for ω.

Vis derved, at

$$S_{K/k}(\omega) = \sum_{j=1}^{n} \omega^{(j)}, \quad N_{K/k}(\omega) = \prod_{j=1}^{n} \omega^{(j)},$$

Bemærk, at formlen $D(\omega) = (\det M)^2$ i Sætning 9 gælder for en vilkårlig basis ω, og opskriv M.

Opgave 4. Lad $K = \mathbb{Q}(\vartheta)$, hvor $\vartheta = \sqrt[3]{28}$. Vis, at $\alpha = \frac{1}{3}(1 - \vartheta)^2$ er et helt algebraisk tal, og angiv minimalpolynomiet for α over $\mathbb{Q}$. Opgaven kan løses på (mindst) to forskellige måder.

Opgave 5. Betragt ringen $R = \mathbb{Z}[x]$ med brøklegeme $K = \mathbb{Q}(x)$. Vis, at idealet $\mathfrak{a} = (2, x)$ ikke er et hovedideal. Bestem strukturen af $R/\mathfrak{a}$.

Vis, at de to idealer $\mathfrak{a}$ og $\mathfrak{b} = (x)$ har den samme tilordnede følge af idealer i $\mathbb{Z}$ jvf. beviset for Sætning 19.

Vis, at R er UFD. Vink: Giv en beskrivelse af de irreducible polynomier i R ved de irreducible normerede polynomier i $\mathbb{Q}[x]$.

Vis, at R er noethersk og helt afsluttet, og at der findes et primideal $\mathfrak{p} \neq (0)$ som ikke er maksimalt.

Opgave 6. Lad R og $\mathfrak{a}$ være som i Opgave 5. Vis, at $R : \mathfrak{a} = R$ (Vink: Benyt, at $\mathfrak{a} \supseteq (2)$.) Begrund dernæst, at idealet $\mathfrak{a}$ ikke er invertibelt.

Opgave 7. Vis, at $R = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$ er noethersk og at ethvert primideal $\mathfrak{p} \neq (0)$ er maksimalt, men at R ikke er helt afluttet. Vink: I beviset for den anden betingelse er det en god ide først at vise, at ethvert helt ideal $\mathfrak{a} \neq (0)$ af R er et 2-dimensionalt delgitter af det 2-dimensionale gitter R i $\mathbb{C}$, og at derfor $R/\mathfrak{a}$ er endelig.

Opgave 8. Vis, at $R = \overline{\mathbb{Z}}$ tilfredsstiller Noether betingelserne, at ethvert primideal $\mathfrak{p} \neq (0)$ er maksimalt, og at R er helt afsluttet. Vink: Den første

påstand kan vises indirekte ved at antage $\mathfrak{p} \subset \mathfrak{m}$ og $\vartheta \in \mathfrak{m} \setminus \mathfrak{p}$, og derpå betragte $O_K \cap \mathfrak{p}$ og $O_K \cap \mathfrak{m}$ for det algebraiske tallegeme $K = \mathbb{Q}(\vartheta)$.

At R ikke er noethersk blev betragtet i kapitel 2, Opgave 1.

Opgave 9. Denne og den efterfølgende opgave handler om valuationer, p-adiske tal and p-adisk analyse. Dette er en meget vigtig del af algebraisk talteori og mange forfattere af bøger i algebraisk talteori (e.g. Artin, Borevich and Safarevich, Cassels and Fröhlich, Edwards, Hasse, Lang, Weiss) har baseret fremstillingen på valuationer fremfor idealer.

For ethvert primtal p defineres for $x \in \mathbb{Q}$ tallet $n_p(x) \in \mathbb{Z} \cup \{\infty\}$ på følgende måde:

$$n_p(x) = \begin{cases} \infty \text{ hvis } x = 0 \\ n \text{ hvis } x \neq 0 \text{ og } x = \pm p^n y, \text{ hvor } y \text{ ikke indeholder } p\,. \end{cases}$$

Vis, at n_p er en additive ikke-arkimedisk valuation på $\mathbb{Q}$ (benyt definitionen på side 2.40).

En følge (x_n), $x_n \in \mathbb{Q}$ for $n \in \mathbb{N}$ er konvergent med grænseværdi x mht. n_p, hvis $n_p(x - x_n) \to \infty$ for $n \to \infty$.

Vis, at (p^n) er konvergent, og angiv grænseværdien.

Prøv også at definere at en følge (x_n) er en Cauchy (eller fundamental) følge, og vis, at en konvergent følge er en Cauchy følge.

Opgave 10. For ethvert primtal p defineres $\mathbb{Z}_p$ og $\mathbb{Q}_p$ på følgende måde:

$$(*) \qquad \mathbb{Z}_p = \{x = \sum_{n=0}^{\infty} a_n p^n\}, \;\; \mathbb{Q}_p = \{x = \sum_{n=n_0}^{\infty} a_n p^n\}\,,$$

hvor $a_n \in \{0, 1, \cdots, p-1\}$ for alle n, og $n_0 \in \mathbb{Z}$ er vilkårligt.

I $\mathbb{Q}_p$ (og derfor i $\mathbb{Z}_p$) defineres

$$n_p(x) = \begin{cases} \infty \text{ hvis } x = 0 \\ n_0 \text{ hvis } x = \sum_{n=n_0}^{\infty} a_n p^n \text{ med } a_{n_0} \neq 0\,. \end{cases}$$

Vi vil accepere indtil videre, at $\mathbb{Q}_p$ er et legeme, og at n_p er en additiv ikke-arkimedisk valuation på $\mathbb{Q}_p$. Vis, at

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid n_p(x) \geqq 0\}\,,$$

og at derfor $\mathbb{Z}_p$ er en ring. $\mathbb{Z}_p$ kaldes ringen af hele tal i $\mathbb{Q}_p$.

Vis, at $\mathbb{Q}$ kan indlejres i $\mathbb{Q}_p$ på en natural måde. Vink: Betragt først, hvordan $x = -1$, $x \in \mathbb{N}$, $x = 1/q, q > 1$ kan udtrykkes som en sum $(*)$. Det tilrådes at betragte en specifik værdi af p og et specifikt x af de to sidste typer for at blive fortrolig med problemstillingen. Vis også, at ved denne indlejring af $\mathbb{Q}$ vil de to betydninger af n_p stemme overens, og at $\mathbb{Q}$ er tæt i $\mathbb{Q}_p$ og $\mathbb{Z}$ er indeholdt i og er tæt i $\mathbb{Z}_p$. Med andre ord: $\mathbb{Q}_p$ er kompletteringen (fuldstændiggørelsen) af $\mathbb{Q}$ mht. n_p og $\mathbb{Z}_p$ er afslutningen af $\mathbb{Z}$.

Opgave 11. Lad p være et ulige primtal, og $a \in \mathbb{Z}$ en kvadratisk rest modulo p. Vis, at ligningen $x^2 = a$ har præcis to løsninger i $\mathbb{Z}_p$. Vink: Vis først, at kongruensen

$$x^2 \equiv a \pmod{p^n}$$

har præcis to løsninger af formen

$$x = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \ ,$$

når $a_j \in \{0, 1, \cdots, p-1\}$ for $0 \leqq j < n$.

Bestem a_0, a_1, a_2, a_3, når $p = 5$ og $a = 11$.

Opgave 12. I $\mathbb{Q}_p$ kan man lave analyse meget i stil med real analyse, specielt vedrørende udvikling i potensrække. Man kan således definere

$$\ln_p(1+x) = \sum_{m=1}^{\infty} (-1)^{m-1} \frac{x^m}{m}, \ \text{ når } \ n_p(x) > 0 \ ,$$

$$\exp_p(x) = \sum_{m=0}^{\infty} \frac{x^m}{m!}, \ \text{ når } \ n_p(x) > 1/(p-1) \ ,$$

$$(1+x)^y = \sum_{m=0}^{\infty} \binom{y}{m} x^m, \ \text{ når } \ n_p(x) > 1/(p-1), \ \ n_p(y) \geqq 0 \ .$$

Prøv at løse det sidste spørgsmål i Opgave 11 ved hjælp af binomial formlen. Vink: Det kan være nyttigt at bemærke, at

$$\tfrac{1}{2} = 3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + \cdots \ .$$

Opgave 13. Lad R være et integritetsområde og K dets brøklegeme. Lad $\mathfrak{B} \neq (0)$ være et invertibelt brudent ideal. Vis, at $\mathfrak{A} : \mathfrak{B} = \mathfrak{A}\mathfrak{B}^{-1}$ for ethvert brudent ideal $\mathfrak{A}$.

Opgave 14. Lad X være et lattice mht. ordningen $\leqq$, og lad $x \vee y$ være det mindste element i X med $x \leqq x \vee y$ og $y \leqq x \vee y$, and tilsvarende $x \wedge y$ være det største element i X med $x \wedge y \leqq x$ og $x \wedge y \leqq y$. Vis, at de to egenskaber

$$\forall x, y, z \in X : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \ , \tag{1}$$

$$\forall x, y, z \in X : x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \tag{2}$$

er ækvivalente.

Opgave 15. Det antages bekendt, at

$$x^9 - 1 = (x^6 + x^3 + 1)(x^2 + x + 1)(x - 1) \ ,$$

og at de tre faktorer er irreducible i $\mathbb{Q}[x]$. Lad $K = \mathbb{Q}(\zeta)$, hvor $\zeta = e^{2\pi i/9}$.
Angiv minimalpolynomiet for ζ^ℓ over $\mathbb{Q}$ for $0 \leqq \ell \leqq 10$.
Vis, at $\mathbb{Q}$-basen $(1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5)$ for K har diskriminanten

$$D(1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5) = -3^9 \ .$$

Hvad kan der på dette grundlag siges om diskriminanten d for legemet K.

Opgave 16. Vis, at den diophantiske ligning

$$x^3 = y^2 + 11$$

netop har løsningerne $(x, y) = (3, \pm 4), (15, \pm 58)$.

Opgave 17. Lad $K = \mathbb{Q}(\sqrt{-39})$. Vis, at klassetallet $h = 4$, og at klassegruppen er isomorf med C_4.

Opgave 18. Betragt det kubiske legeme $K = \mathbb{Q}(\alpha)$, hvor α er en vilkårlig rod i polynomiet $x^3 - x - 1$. Det kan benyttes (jvf. Opgave 12, Kapitel 3), at

$$O_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2, \ \ d = -23.$$

Udregn $N(a_0 + a_1\alpha)$ for $a_0, a_1 \in \mathbb{Z}$, og vis herved, at $N(3 + 2\alpha) = N(3 - \alpha) = 23$.

Vis, at

$$23 = (3+2\alpha)^2(3-\alpha)\varepsilon, \quad \text{hvor } \varepsilon \in {O_K}^{\times},$$

og bestem ε. Vis endelig, at $3+2\alpha$ og $3-\alpha$ er ikke associerede elementer i O_K.

Opgave 19. For det kvadratiske tallegeme $K = \mathbb{Q}(\sqrt{-23})$ siger Dedekind's klassetalsformel, at

$$L(1,\chi) = \frac{2^{r_1+r_2}\pi^{r_2}R}{w\sqrt{|d|}}h\ .$$

Angiv værdierne af r_1, r_2, R, w, d, og opstil på nemmeste måde en tabel over Kronecker karakteren χ, der hører til K. Find tilnærmede værdier for h ved at beregne afsnit i rækken

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$$

for eksempel ved afskæring af rækken efter første og anden periode for χ.

P. Programmer

I dette kapitel gengives de tre PARI-programmer UNITS, KUMMER og CLASSNBS, der er omtalt i kapitlerne 3, 4 og 5. Endvidere gengives det output (let redigeret), som programmerne genererer.

PARI-programmet UNITS.

```
\\ Enheder i legemet Q(2 cos 2*pi/7)
f(A,B)=x^3-A*x^2+B*x-1;
D(A,B)=A^2*B^2-4*A^3-4*B^3+18*A*B-27;
\precision=5;
\l
print("  A   ","   B   ","   D   ",\
"   log(abs(roots(f(A,B))))")
for(A=-5,5,for(B=-8,8,if(((D(A,B)%49)==0)&&(D(A,B)>0)\
&&(issquare(D(A,B)\49)),\
print("  ",A,"     ",B,"     ",D(A,B),"     ",\
log(abs(roots(f(A,B))))),)))
```

```
  A      B      D       log(abs(roots(f(A,B))))

 -4      3      49     [1.0303, 0.36813, -1.3984]
 -2     -1      49     [0.80958, -0.58886, -0.22072]
 -1     -2      49     [0.58886, -0.80959, 0.22072]
  3     -4      49     [-0.36813, -1.0303, 1.3984]
  5     -8    2401     [0.14741, -1.9873, 1.8399]
  5      6      49     [-1.6191, 0.44144, 1.1777]
```

PARI-programmet KUMMER.

```
\\ Bernoullital og ikke regulære primtal
b=bernvec(250);
bern(x)=if(x==1,-1/2,if((x<0)||(x%2),0,b[x/2+1]));
\l
print("Tabel over Bernoullital:");
print("  n   ","   B_2n");
for(n=0,20,print("  ",n,"     ",bern(2*n)));
print("Tabel over ikke regulære primtal < 500");
for(p=3,500,if(isprime(p),for(n=1,(p-3)/2,\
if((numer(bern(2*n))%p)==0,print(p," er irregulær, da "\
,p," er divisor i B_",2*n),)),));
```

```
Tabel over Bernoullital:

  n      B_2n

  0      1
  1      1/6
  2     -1/30
  3      1/42
  4     -1/30
  5      5/66
  6     -691/2730
  7      7/6
  8     -3617/510
  9      43867/798
  10    -174611/330
  11     854513/138
  12    -236364091/2730
  13     8553103/6
  14    -23749461029/870
  15     8615841276005/14322
  16    -7709321041217/510
  17     2577687858367/6
  18    -263152715530534773373/1919190
  19     2929993913841559/6
  20    -2610827184964491220 51/13530
```

```
Tabel over ikke regulære primtal < 500:

37 er irregulær, da 37 er divisor i B_32
59 er irregulær, da 59 er divisor i B_44
67 er irregulær, da 67 er divisor i B_58
101 er irregulær, da 101 er divisor i B_68
103 er irregulær, da 103 er divisor i B_24
131 er irregulær, da 131 er divisor i B_22
149 er irregulær, da 149 er divisor i B_130
157 er irregulær, da 157 er divisor i B_62
157 er irregulær, da 157 er divisor i B_110
233 er irregulær, da 233 er divisor i B_84
257 er irregulær, da 257 er divisor i B_164
263 er irregulær, da 263 er divisor i B_100
271 er irregulær, da 271 er divisor i B_84
283 er irregulær, da 283 er divisor i B_20
293 er irregulær, da 293 er divisor i B_156
307 er irregulær, da 307 er divisor i B_88
311 er irregulær, da 311 er divisor i B_292
347 er irregulær, da 347 er divisor i B_280
353 er irregulær, da 353 er divisor i B_186
353 er irregulær, da 353 er divisor i B_300
379 er irregulær, da 379 er divisor i B_100
379 er irregulær, da 379 er divisor i B_174
389 er irregulær, da 389 er divisor i B_200
401 er irregulær, da 401 er divisor i B_382
409 er irregulær, da 409 er divisor i B_126
421 er irregulær, da 421 er divisor i B_240
433 er irregulær, da 433 er divisor i B_366
461 er irregulær, da 461 er divisor i B_196
463 er irregulær, da 463 er divisor i B_130
467 er irregulær, da 467 er divisor i B_94
467 er irregulær, da 467 er divisor i B_194
491 er irregulær, da 491 er divisor i B_292
491 er irregulær, da 491 er divisor i B_336
491 er irregulær, da 491 er divisor i B_338

i alt 28 irregulære primtal
```

PARI-programmet CLASSNBS.

```
\\ Klassetal for kvadratiske tallegemer
c(x)=classno(x);
\l
print("Klassetal for imaginært kvadratiske \
tallegemer med -d<200:");
print("  d  "," h  ");
for(d=1,200,if(isfund(-d),print(-d,"    ",classno(-d)),));
print("Klassetal for reeelt kvadratiske \
tallegemer med d<200:");
print("  d  "," h  ");
for(d=2,200,if(isfund(d),print(d,"    ",classno(d)),));
print("Klassetal for imaginært kvadratiske \
tallegemer med -d=p<1000:");
print("  d  "," h  ");
for(d=1,1000,if(isfund(-d)&&isprime(-d),\
print(-d,"    ",classno(-d)),));
print("Klassetal for reelt kvadratiske \
tallegemer med d=p<1000:");
print("  d  "," h  ");
for(d=2,1000,if(isfund(d)&&isprime(d),\
print(d,"    ",classno(d)),));
```

Klassetal for imaginært kvadratiske tallegemer med -d<200:

d	h	d	h	d	h	d	h	d	h
-3	1	-4	1	-7	1	-8	1	-11	1
-15	2	-19	1	-20	2	-23	3	-24	2
-31	3	-35	2	-39	4	-40	2	-43	1
-47	5	-51	2	-52	2	-55	4	-56	4
-59	3	-67	1	-68	4	-71	7	-79	5
-83	3	-84	4	-87	6	-88	2	-91	2
-95	8	-103	5	-104	6	-107	3	-111	8
-115	2	-116	6	-119	10	-120	4	-123	2
-127	5	-131	5	-132	4	-136	4	-139	3
-143	10	-148	2	-151	7	-152	6	-155	4
-159	10	-163	1	-164	8	-167	11	-168	4
-179	5	-183	8	-184	4	-187	2	-191	13
-195	4	-199	9						

i alt 62 diskriminanter

Klassetal for reelt kvadratiske tallegemer med d<200:

d	h	d	h	d	h	d	h	d	h
5	1	8	1	12	1	13	1	17	1
21	1	24	1	28	1	29	1	33	1
37	1	40	2	41	1	44	1	53	1
56	1	57	1	60	2	61	1	65	2
69	1	73	1	76	1	77	1	85	2
88	1	89	1	92	1	93	1	97	1
101	1	104	2	105	2	109	1	113	1
120	2	124	1	129	1	133	1	136	2
137	1	140	2	141	1	145	4	149	1
152	1	156	2	157	1	161	1	165	2
168	2	172	1	173	1	177	1	181	1
184	1	185	2	188	1	193	1	197	1

i alt 60 diskriminanter

Klassetal for imaginært kvadratiske tallegemer med -d=p<1000:

d	h	d	h	d	h	d	h	d	h
-3	1	-7	1	-11	1	-19	1	-23	3
-31	3	-43	1	-47	5	-59	3	-67	1
-71	7	-79	5	-83	3	-103	5	-107	3
-127	5	-131	5	-139	3	-151	7	-163	1
-167	11	-179	5	-191	13	-199	9	-211	3
-223	7	-227	5	-239	15	-251	7	-263	13
-271	11	-283	3	-307	3	-311	19	-331	3
-347	5	-359	19	-367	9	-379	3	-383	17
-419	9	-431	21	-439	15	-443	5	-463	7
-467	7	-479	25	-487	7	-491	9	-499	3
-503	21	-523	5	-547	3	-563	9	-571	5
-587	7	-599	25	-607	13	-619	5	-631	13
-643	3	-647	23	-659	11	-683	5	-691	5
-719	31	-727	13	-739	5	-743	21	-751	15
-787	5	-811	7	-823	9	-827	7	-839	33
-859	7	-863	21	-883	3	-887	29	-907	3
-911	31	-919	19	-947	5	-967	11	-971	15
-983	27	-991	17	-1019	13	-1031	35	-1039	23
-1051	5	-1063	19	-1087	9	-1091	17	-1103	23
-1123	5	-1151	41	-1163	7	-1171	7	-1187	9
-1223	35	-1231	27	-1259	15	-1279	23	-1283	11
-1291	9	-1303	11	-1307	11	-1319	45	-1327	15
-1367	25	-1399	27	-1423	9	-1427	15	-1439	39
-1447	23	-1451	13	-1459	11	-1471	23	-1483	7
-1487	37	-1499	13	-1511	49	-1523	7	-1531	11
-1543	19	-1559	51	-1567	15	-1571	17	-1579	9
-1583	33	-1607	27	-1619	15	-1627	7	-1663	17
-1667	13	-1699	11	-1723	5	-1747	5	-1759	27
-1783	17	-1787	7	-1811	23	-1823	45	-1831	19
-1847	43	-1867	5	-1871	45	-1879	27	-1907	13
-1931	21	-1951	33	-1979	23	-1987	7	-1999	27

i alt 155 diskriminanter

Klassetal for reelt kvadratiske tallegemer med d=p<1000:

d	h	d	h	d	h	d	h	d	h
5	1	13	1	17	1	29	1	37	1
41	1	53	1	61	1	73	1	89	1
97	1	101	1	109	1	113	1	137	1
149	1	157	1	173	1	181	1	193	1
197	1	229	3	233	1	241	1	257	3
269	1	277	1	281	1	293	1	313	1
317	1	337	1	349	1	353	1	373	1
389	1	397	1	401	5	409	1	421	1
433	1	449	1	457	1	461	1	509	1
521	1	541	1	557	1	569	1	577	7
593	1	601	1	613	1	617	1	641	1
653	1	661	1	673	1	677	1	701	1
709	1	733	3	757	1	761	3	769	1
773	1	797	1	809	1	821	1	829	1
853	1	857	1	877	1	881	1	929	1
937	1	941	1	953	1	977	1	997	1
1009	7	1013	1	1021	1	1033	1	1049	1
1061	1	1069	1	1093	5	1097	1	1109	1
1117	1	1129	9	1153	1	1181	1	1193	1
1201	1	1213	1	1217	1	1229	3	1237	1
1249	1	1277	1	1289	1	1297	11	1301	1
1321	1	1361	1	1373	3	1381	1	1409	1
1429	5	1433	1	1453	1	1481	1	1489	3
1493	1	1549	1	1553	1	1597	1	1601	7
1609	1	1613	1	1621	1	1637	1	1657	1
1669	1	1693	1	1697	1	1709	1	1721	1
1733	1	1741	1	1753	1	1777	1	1789	1
1801	1	1861	1	1873	1	1877	1	1889	1
1901	3	1913	1	1933	1	1949	1	1973	1
1993	1	1997	1						

i alt 147 diskriminanter

A. Alfabeter

Det græske alfabet:

A,α: alfa	B,β: beta	Γ, γ: gamma	Δ, δ: delta
E,ϵ, ε: epsilon	Z,ζ: zeta	H, η: eta	$\Theta, \theta, \vartheta$: theta
I,ι: iota	K,κ: kappa	Λ, λ: lambda	M,μ: my
N,ν: ny	Ξ, ξ: ksi	Π, π, ϖ: pi	R,ρ, ϱ: ro
$\Sigma, \sigma, \varsigma$: sigma	T,τ: tau	Υ, υ: ypsilon	Φ, ϕ, φ: fi
X,χ: ki	Ψ, ψ: psi	Ω, ω: omega	

Det gotiske alfabet:

$\mathfrak{A}, \mathfrak{a}$: A, a	$\mathfrak{B}, \mathfrak{b}$: B, b	$\mathfrak{C}, \mathfrak{c}$: C, c	$\mathfrak{D}, \mathfrak{d}$: D, d	$\mathfrak{E}, \mathfrak{e}$: E, e
$\mathfrak{F}, \mathfrak{f}$: F, f	$\mathfrak{G}, \mathfrak{g}$: G, g	$\mathfrak{H}, \mathfrak{h}$: H, h	$\mathfrak{I}, \mathfrak{i}$: I, i	$\mathfrak{J}, \mathfrak{j}$: J, j
$\mathfrak{K}, \mathfrak{k}$: K, k	$\mathfrak{L}, \mathfrak{l}$: L, l	$\mathfrak{M}, \mathfrak{m}$: M, m	$\mathfrak{N}, \mathfrak{n}$: N, n	$\mathfrak{O}, \mathfrak{o}$: O, o
$\mathfrak{P}, \mathfrak{p}$: P, p	$\mathfrak{Q}, \mathfrak{q}$: Q, q	$\mathfrak{R}, \mathfrak{r}$: R, r	$\mathfrak{S}, \mathfrak{s}$: S, s	$\mathfrak{T}, \mathfrak{t}$: T, t
$\mathfrak{U}, \mathfrak{u}$: U, u	$\mathfrak{V}, \mathfrak{v}$: V, v	$\mathfrak{W}, \mathfrak{w}$: W, w	$\mathfrak{X}, \mathfrak{x}$: X, x	$\mathfrak{Y}, \mathfrak{y}$: Y, y
$\mathfrak{Z}, \mathfrak{z}$: Z, z				

L. Litteratur

T. M. Apostol: *Introduction to Analytic Number Theory*. 1976.

E. Artin: *Algebraic Numbers and Functions*. 1967.

E. Artin, J. Tate: *Class Field Theory*. 1951-52.

E. Artin: *Theory of Algebraic Numbers*. 1959.

E. Artin: *Galoische Theorie*. 1959.

A. Baker: *Transcendental Number Theory*. 1975.

Z. I. Borevich, I. R. Safarevich: *Number Theory*. 1966.

J. W. S. Cassels: *An Introduction to the Geometry of Numbers*. 1959.

J. W. S. Cassels, A. Fröhlich /ed.: *Algebraic Number Theory*. Symposium (England), 1967.

C. Chevalley: *Class Field Theory*. 1953-54.

S. Chowla: *The Riemann Hypothesis and Hilbert's Tenth Problem*. 1965.

H. Cohen: *A Cource in Computational Algebraic Number Theory*. 1993.

H. Cohn: *A Second Cource in Number Theory*. 1962.

H. Cohn: *A Classical Invitation To Algebraic Numbers and Class Fields*. 1978.

H. Cohn: *Introduction to the Construction of Class Fields*. 1985.

G. Cornell, J. H. Silverman: *Modular Forms and Fermat's Last Theorem*. 1997.

M. Deuring: *Klassenkörpertheorie*. 1965-66.

L. E. Dickson: *Introduction to the Theory of Numbers*. 1929.

G. L. Dirichlet: *Vorlesungen über Zahlentheorie* (med 11. supplement af R. Dedekind). 1879.

G. L. Dirichlet: *Werke*. I (1889), II (1897).

H. M. Edwards: *Fermat's Last Theorem*. 1977.

H. M. Edwards: *Divisor Theory*. 1990.

M. Eichler: *Introduction to the Theory of Algebraic Numbers and Functions*. 1963.

T. Estermann: *Introduction to Modern Prime Number Theory*. 1961.

R. Fueter: *Synthetische Zahlentheorie*. 1950.

C. F. Gauss: *Disquisitiones Arithmeticae*. 1801.

H. Hasse: *"Klassenkörperbericht"*. I (1926), Ia (1927), II (1930).

H. Hasse: *Vorlesungen über Zahlentheorie*. 1950.

H. Hasse: *Über die Klassenzahl abelscher Zahlkörper*. 1952.

H. Hasse: *Zahlentheorie*. 1969.

E. Hecke: *Vorlesungen über die Theorie der algebraischen Zahlen*. 1923.

K. Hensel: *Theorie der algebraischen Zahlen*. 1908.

D. Hilbert: *Die Theorie der algebraischen Zahlkörper*. 1897. (Se Gesammelte Abhandlungen I).

L. Holzer: *Zahlentheorie*. I (1958), II (1959), III (1965).

L. Holzer: *Klassenkörpertheorie*. (1966).

A. E. Ingham: *Distribution of Prime Numbers*. 1932.

K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory*. 1993.

K. Iwasawa: *Lectures on p-adic L-Functions*. 1972.

N. Koblitz: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. 1984.

H. Koch: *Algebraic Number Theory*. 1997.

E. E. Kummer: *Collected Papers*. I, 1975.

E. Landau: *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*. 1918.

E. Landau: *Vorlesungen über Zahlentheorie* I-III. 1927.

S. Lang: *Algebraic Number Theory*. 1994.

S. Lang: *Cyclotomic Fields*. 1978.

S. Lang: *Cyclotomic Fields II*. 1980.

D. A. Marcus: *Number Fields*. 1995.

C. Meyer: *Die Berechnung der Klassezahl abelscher Körper über quadratischen Zahlkörpern*. 1957.

H. Minkowski: *Geometrie der Zahlen*. 1896.

H. Minkowski: *Diophantische Approximationen*. 1907.

L. J. Mordell: *Diophantine Equations*. 1969.

W. Narkiewich: *Elementary and Analytic Theory of Algebraic Numbers*. 1974.

J. Neukirch: *Class Field Theory*. 1986.

P. Ribenboim: *Algebraic Numbers*. 1972.

P. Ribenboim: 13 *Lectures on Fermat's Last Theorem*. 1995.

P. Samuel: *Theorie Algébrique des Nombres*. 1967.

L. C. Washington: *Introduction to Cyclotomic Fields*. 1997.

H. Weber: *Lehrbuch der Algebra* I-III. 1896.

A. Weil: *Basic Number Theory*. 1995.

E. Weiss: *Algebraic Number Theory*. 1963.

H. G. Zimmer: *Computational Problems, Methods, and Results in Algebraic Number Theory*. Springer Lecture Notes 262, 1972.

I. Indeks

Abels sætning 1.16
abelske grupper, struktursætning for 5.13
absolut udvidelse 1.1
ACC 2.2
algebraisk afslutning 1.6
algebraisk afsluttet 1.6
algebraisk element 1.1
algebraisk tallegeme 1.1
algebraisk udvidelse 1.1
algebraiske tal, legemet af 1.6
approksimationssætning, stærke 2.41

Baker's metode 3.33
basis 2.6
Bernoullital 0.3, 4.13
brudent ideal 2.12

cirkeldelingslegeme 1.5, 4.1
cirkeldelingslegeme, reelt 4.3
cirkeldelingspolynomium 1.5
CLASSNBS 5.43, P.4

Dedekind's diskriminantsætning 3.23
Dedekind's klassetalsformel 5.1
Dedekind's zetafunktion 0.3, 5.1
Dedekindring 2.1
Dedekindring, karakterisering af 2.1, 2.16
Dedekindring, klassisk 3.1
Dedekindring, udvidelser af 2.2, 2.24
dekomposition 3.11, 3.13, 3.15
dekomposition, forgrenet 3.11, 3.13, 3.15
dekomposition, opløst 3.11, 3.13, 3.15
dekomposition, træg 3.11, 3.13, 3.15
Dirichlet karakter 0.2, 5.15
Dirichlet karakter, induceret 5.16
Dirichlet karakter, kvadratisk 5.15

Dirichlet karakter, lige 5.15
Dirichlet karakter, primitiv 5.16
Dirichlet karakter, ulige 5.15
Dirichlet række 5.26
Dirichlet's enhedssætning 0.2, 3.42
Dirichlet's primtalssætning 0.2
diskriminant 1.10, 3.1
distributivt lattice 2.31
divisor teori 0.4

Eisenstein's kriterium 1.4, 1.20
elementardivisorsætningen 3.6
endelig udvidelse 1.1
endeligt frembragt 2.3, 2.6
enhed 2.2
euklidisk funktion 3.37
euklidisk funktion, minimal 3.38
euklidisk funktion, ækvivalens af 3.37
euklidisk ring 3.37
Euler's formel 4.13
Euler-produkt 5.32, 5.33
Eulers kriterium 3.10

Fermat problem 0.1
Fermat-primtal 1.18
forgreningsindex, for primideal 3.8
fri R-modul 2.6
Frobenius-automorfi 1.19
fundamentalenheder 3.56
fundamentalområde 3.19
funktionalligning 0.3
fællesnævner 2.11, 2.12

Galoisgruppe 1.14
galois udvidelse 1.14
Galoisteori 1.13
Galoisteori, hovedsætning 1.15
Gauss' lemma 1.4, 1.20
gaussisk sum 5.22
gaussisk sum, normeret 5.22

genus karakter 5.52
genus klassegruppe 5.52
genusteori 0.1, 5.43, 5.52
geometrisk talteori 0.4, 3.18
gitter 3.18
gitter, fuldt 3.18
gitter, kritisk 3.65
gitter, punkt 3.18
gitter, tilladeligt 3.65
gitterdeteriminant 3.18
grad, af element 1.2
grad, af primideal 3.8
grad, af udvidelse 1.1
grundlegeme 1.1

hel afslutning 2.10
helt afsluttet 2.11
helt element 2.9
hovedkarakter 5.13, 5.15

ideale tal 0.2
idealklasser 3.25
idealkvotient 2.12
idealprodukt 2.12
ikke-Pell'ske ligning 3.56
imaginært kvadratisk tallegeme 1.4, 3.33, 3.40
invertibelt element 2.2
invertibelt ideal 2.13
irreducibelt element 2.2

k-automorfi 1.14
karakter 5.12
karaktergruppe 5.13
karakteristisk polynomium 1.6, 1.8
kinesisk restklassesætning 2.34
klassegruppe 0.1, 3.25
klasselegemeteori 5.46
klassetal 0.1, 3.25
klassetalsformel, cirkeldelingslegemer 5.43, 5.44, 5.45
klassetalsformel, kvadratiske tallegemer 5.40, 5.41

klassetalsformel, p-adisk 5.46
konjugerede legemer 3.2
konjugeret 1.9
konvergensabscisse 5.27
konvergensabscisse, absolut 5.27
konvergenshalvplan 5.27
Kreiseinheiten 4.16
kritisk determinant 3.65
Kronecker karakter 5.21
kubisk tallegeme, 3.44, 3.45, 3.58, 3.59, 3.67, 3.68, 3.69
kubisk tallegeme, rent 3.67,
KUMMER 4.13, P.2
Kummer's enhedssætning 4.6
Kummer's sætning 4.8
kvadratisk ikke rest 3.10
kvadratisk rest 3.10
kvadratisk tallegeme 1.4

L-funktion 5.30
L-funktion, p-adisk 5.46
L-række 5.29
L-rækker, summation af 5.37
lattice 2.31
Legendre symbol 3.10
logaritmisk afbildning 3.53

Möbius omvendingsformel 5.19
Möbius produkt 5.19
Maillet's determinant 5.49
maksimalt ideal 2.1
mindste fælles multiplum 2.32
minimalpolynomium 1.2
Minkowski's gitterpunktsætning 3.20
Minkowski's linearformsætning 3.20, 3.21
Minkowski's ulighed 3.66
modulus, minimal 5.16
Mordell's ligning 3.30, 3.32
Motzkin's sætning 3.38

naturlig indlejring 3.48

Noether betingelser 2.1
noethersk, modul 2.6
noethersk, ring 2.3
norm 1.7
normal udvidelse 1.13
normalt hylster 1.16, 3.1

Ordnung 3.1
ortogonalitetsrelationer 5.14

Pell's ligning 3.56
PID 2.2
PIR 2.33
primelement 2.2
primelement, for primideal 2.38
primideal 2.1
primiske idealer 2.33
primitivt element 1.12
primlegeme 1.1
primtalssætningen 5.36

R-modul 2.5
Rabinowitsch' sætning 3.34
rang 2.9
reciprocitetssætningen 0.1, 3.11, 5.24
reelt kvadratisk tallegeme 1.4, 3.44, 3.56
regulatoren 3.62
regulært primtal 0.3, 4.8
Riemanns zeta-funktion 0.3, 5.27

separabel udvidelae 1.14
separabelt polynomium 1.14
Siegel-Brauers sætning 3.63
spaltningslegeme 1.13
spor 1.7
Stickelberger's sætning 3.2
største fælles divisor 2.32

tallegeme 1.1
totalt imaginært 3.56, 4.2

totalt reelt 4.2
transcendent, element 1.2

UFD 2.2
undermodul 2.5
UNITS 3.61, P.1

valuation 2.39
valuation, additiv 2.40
valuation, diskret 2.40
valuation, ikke-arkimedisk 2.40
valuation, multiplikativ 2.39
valuation, normeret 2.40
valuationer, ækvivalens af 2.40
valuationsring 2.40
valuationsteori 0.4
Vandermonde determinant 1.13, 2.27
von Staudt/Clausens formel 4.13