Kapitel 4. Analytiske metoder.

Lad k være et algebraisk tallegeme. Vi vil betragte Dedekinds zetafunktion

$$\zeta_k(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} ,$$

hvor summationen er over alle hele idealer ($\neq (0)$) i $\mathcal{O}_k$. Den variable $s = \sigma + it$, $\sigma, t \in \mathbb{R}$, er kompleks, og vi vil senere vise, at $\zeta_k(s)$ ved denne række fremstilling er defineret for $\sigma = \operatorname{Re} s > 1$ og der fremstiller en holomorf (analytisk) funktion af s. Funktionen har en entydig analytisk fortsættelse til hele $\mathbb{C}$ og bliver holomorf overalt, på nær for $s = 1$, hvor der er en pol af første orden med residuum

$$\lim_{s \to 1} (s-1)\, \zeta_k(s) > 0 .$$

Hovedsætning. For et vilkårligt algebraisk tallegeme k af grad $n = r_1 + 2r_2$ gælder klassetalsformlen

$$\lim_{s \to 1} (s-1)\, \zeta_k(s) = \frac{2^{r_1+r_2}\, \pi^{r_2}\, R}{w \sqrt{|d|}} \cdot h ,$$

hvor R er regulatoren, d diskriminanten og w ordenen af gruppen af enhedsrødder i $\mathcal{O}_k^*$.

Ved udnyttelsen af hovedsætningen er det derfor afgørende at finde andre udtryk for det omhandlede residuum af $\zeta_k(s)$. Da $\mathcal{O}_k$ er en Dedekindring gælder – i hvert fald formelt –

$$\zeta_k(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

$$= \prod_{\mathfrak{p}} \left(1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \cdots \right)$$

$$= \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \,,$$

hvor produktet er over alle primidealer $(\neq (0))$ i $\mathcal{O}_k$. Denne fremstilling kaldes <u>Euler-produktet</u> for $\zeta_k(s)$, idet specialtilfældet $k = \mathbb{Q}$:

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primtal}} \frac{1}{1 - \frac{1}{p^s}}$$

var kendt af Euler. Betegnelsen ζ skyldes Riemann (1859).

<u>Eksempel 39.</u> For $k = \mathbb{Q}$ er $r_1 = 1$, $r_2 = 0$, $R = 1$, $w = 2$, $d = 1$ og $h = 1$. Følgelig er ifølge hovedsætningen

$$\lim_{s \to 1} (s-1)\zeta(s) = 1 \,,$$

i overensstemmelse med at Riemann's ζ-funktion faktisk har en pol af 1. orden med residuum 1 i punktet $s = 1$.

Eksempel 40. For $k = \mathbb{Q}(i)$ (jvf. eksempel 18, pag. 88) er $r_1 = 0$, $r_2 = 1$, $R = 1$, $d = -4$, $w = 4$ og $h = 1$. Ifølge hovedsætningen er derfor

$$(*) \qquad \lim_{s \to 1} (s-1)\, \zeta_k(s) = \frac{\pi}{4}.$$

Her er

$$\zeta_k(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \prod_{\substack{p \\ \text{primtal}}} \prod_{\mathfrak{p} \mid p} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}.$$

Der er følgelig tre muligheder:

(i) p forgrenet, dvs. $p = 2$, $\mathfrak{p} = (1+i)$, $N(\mathfrak{p}) = 2$ i hvilket tilfælde vi får en faktor

$$\frac{1}{1 - \frac{1}{2^s}};$$

(ii) p opløst, dvs. $p \equiv 1 \ (4)$, $(p) = \mathfrak{p}_1 \mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$, i hvilket tilfælde vi får faktoren

$$\left(\frac{1}{1 - \frac{1}{p^s}} \right)^2;$$

(iii) p treg, dvs. $p \equiv 3 \ (4)$, $\mathfrak{p} = (p)$, $N(\mathfrak{p}) = p^2$, i hvilket tilfælde vi får faktoren

$$\frac{1}{1 - \frac{1}{p^{2s}}} = \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 + \frac{1}{p^s}}.$$

Følgelig er

$$\zeta_k(s) = \frac{1}{1-\frac{1}{2^s}} \prod_{p\equiv 1(4)} \frac{1}{\left(1-\frac{1}{p^s}\right)^2} \prod_{p\equiv 3(4)} \left(\frac{1}{1-\frac{1}{p^s}} \cdot \frac{1}{1+\frac{1}{p^s}}\right)$$

$$= \prod_p \frac{1}{1-\frac{1}{p^s}} \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}} ,$$

hvor

$$\chi(p) = \begin{cases} 1 & p\equiv 1(4) \\ -1 & p\equiv 3(4) \\ 0 & p = 2 \end{cases} .$$

Da χ kan udvides til en multiplikativ funktion på $\mathbb{N}$ ved

$$\chi(n) = \begin{cases} 1 & n\equiv 1\ (4) \\ -1 & n\equiv 3\ (4) \\ 0 & n\equiv 0\ (2) \end{cases}$$

finder vi

$$(**) \qquad \zeta_k(s) = \zeta(s)\cdot L(s,\chi) ,$$

hvor

$$L(s,\chi) = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} .$$

$L(s,\chi)$ er en såkaldt <u>Dirichlet'sk L-funktion</u> for <u>karakteren</u> χ. Det fremgår af (**), at $\zeta_k(s)$ har residuet $L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$ i $s=1$.

Da residuet ifølge hovedsætningen er $\frac{\pi}{4}$ (jvf (*)) er derfor

$$\frac{\pi}{4} = L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots,$$

hvilket er Leibniz velkendte rækkeudvikling for $\pi/4$.

Eksempel 41. For $k = \mathbb{Q}(\sqrt{2})$ (jvf. eksemplerne 19, 30, 36) er $r_1 = 2$, $r_2 = 0$, $R = \ln(1+\sqrt{2})$, $d = 8$, $w = 2$ og $h = 1$. I følge hovedsætningen er derfor

$$(*) \qquad \lim_{s \to 1} (s-1)\,\zeta_k(s) = \frac{1}{\sqrt{2}} \ln(1+\sqrt{2}).$$

I analogi med eksempel 40 fås her

$$(**) \qquad \zeta_k(s) = \zeta(s) \cdot L(s,\chi),$$

hvor

$$\chi(n) = \begin{cases} 1 & n \equiv \pm 1 \ (8) \\ -1 & n \equiv \pm 3 \ (8) \\ 0 & n \equiv 0 \ (2) \end{cases}$$

og

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Ved sammenligning af (*) og (**) fås derfor

$$(***) \qquad \frac{1}{\sqrt{2}} \ln(1+\sqrt{2}) = L(1,\chi) = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} + \frac{1}{15} + \cdots,$$

hvor der er skiftevis to minustegn og to plustegn.

Øvelse. Vis formel (***) i eksempel 1 ved elementære metoder. [Vink: betragt 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].

Øvelse. Betragt legemet $\mathbb{Q}(\sqrt{-2})$, og vis at den tilhørende L-funktion er givet ved karakteren

$$\chi(n) = \begin{cases} 1 & n \equiv 1, 3 \ (8) \\ -1 & n \equiv 5, 7 \ (8) \\ 0 & n \equiv 0 \ (2) \end{cases}$$

Vis, at

$$\frac{\pi}{\sqrt{8}} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11} - \frac{1}{13} - \frac{1}{15} + \cdots .$$

[I analogi med den foregående øvelse kan denne sum også findes ved elementære metoder].

—

De foregående eksempler har illustreret nødvendigheden af at studere karakterfunktioner χ på $\mathbb{N}$ og de tilhørende L-rækker nærmere. Vi betragter først karakterer på endelige abelske grupper.

Definition. Lad G være en endelig abelsk gruppe af orden $m = |G|$. En karakter på G er en afbildning $\chi : G \to \mathbb{C}^*$ for hvilken

$$\chi(ab) = \chi(a)\chi(b) \quad \text{for alle } a, b \in G.$$

χ er altså en homomorfi af $(G, \cdot)$ ind i $(\mathbb{C}^*, \cdot)$.

Da χ er en homomorfi er $\chi(e) = 1$, hvor e er gruppens etelement. Da $a^m = e$ for alle $a \in G$ gælder derfor $\chi(a)^m = \chi(a^m) = \chi(e) = 1$, dvs. χ's værdier er alle m'te enhedsrødder.

Lad $V = V_G$ være vektorrummet af alle komplekse funktioner definieret på G. V er da et m-dimensionalt kompleks vektorrum. I V indføres på naturlig måde et indre produkt ved

$$(f, g) = \frac{1}{m} \sum_{a \in G} f(a)\bar{g}(a) \quad \text{for vilkårlige } f, g \in V.$$

Hermed bliver V et komplekst Hilbertrum; den tilhørende norm $\| \ \|$ er givet ved

$$\|f\|^2 = \frac{1}{m} \sum_{a \in G} |f(a)|^2.$$

Vi vil vise, at mængden af karakterer på G udgør et ortonormalsystem i V. Da alle χ's værdier har absolutværdi 1 er

$$\|\chi\|^2 = \frac{1}{m} \sum_{a \in G} 1 = 1 \quad \text{for ethvert } \chi.$$

For at vise ortogonaliteten bemærkes først, at mængden af karakterer på G udgør en gruppe ved punktvis (sædvanlig) multiplikation. Enhedskarakteren er karakteren identisk 1. Denne kaldes hovedkarakteren på G. Endvidere ses, at den inverse karakter til en karakter χ er $\bar{\chi}$. Lad nu $\chi_1 \neq \chi_2$ være to vilkårlige karakterer på G, og betragt karakteren $\chi = \chi_1 \chi_2^{-1} = \chi_1 \bar{\chi}_2$. For at vise $(\chi_1, \chi_2) = 0$ skal vi altså vise, at middelværdien af χ

$$M(\chi) = \frac{1}{m} \sum_{a \in G} \chi(a) = 0.$$

Da $\chi_1 \neq \chi_2$, er χ ikke hovedkarakteren, hvorfor der findes et $b \in G$ med $\chi(b) \neq 1$. Vi finder nu

$$M(\chi) = \frac{1}{m} \sum_{a \in G} \chi(ab) = \frac{1}{m} \sum_{a \in G} \chi(a)\chi(b) = M(\chi) \cdot \chi(b),$$

hvoraf som ønsket $M(\chi) = 0$. Af dette resultat følger specielt, at karaktererne på G er lineært uafhængige funktioner i V; antallet af karakterer er derfor højst $m = \dim_{\mathbb{C}} V$.

Sætning 95 (Struktursætning for abelske grupper).

Enhver endeligt frembragt abelsk gruppe er isomorf med det (ydre) direkte produkt af endelig mange cykliske grupper.

Bevis: Ved beviset benyttes additiv skrivemåde. Lad derfor $(G, +)$ være en abelsk gruppe med frembringere $g_1, \dots, g_m$, og lad $E = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{m}$. E er da en fri abelsk gruppe af rang m og basis $(e_1^* = (1, \dots, 0), \dots, e_m^* = (0, \dots, 1))$. Lad $\varphi : E \to G$ være homomorfien givet ved $\varphi\left(\sum_1^n n_j e_j^*\right) = \sum_1^n n_j g_j$, $n_j \in \mathbb{Z}$.

Da φ er surjektiv er

$$G \cong E/F, \quad F = \ker \varphi.$$

Da F er en undergruppe i den fri abelske gruppe E,

kan vi anvende elementardivisorsætningen (sætning 51), hvorfor der findes en basis $(e_1, \dots, e_n)$ for E og en basis $(f_1, \dots, f_r)$, $r \leq n$, for F, så at

$f_j = m_j e_j$ for $1 \leq j \leq r$, $m_j \in \mathbb{N}$ for $1 \leq j \leq r$,

(og endda $m_1 \mid m_2 \mid \cdots \mid m_r$). Det er nu klart, at

$$G \cong \mathbb{Z}/(m_1\mathbb{Z}) \oplus \cdots \oplus \mathbb{Z}/(m_r\mathbb{Z}) \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-r}. \qquad \square$$

Korollar. En endelig abelsk gruppe er isomorf med det (ydre) direkte produkt af endelig mange endelige cykliske grupper.

Sætning 96. Lad G være en vilkårlig endelig abelsk gruppe af orden $|G| = m$. Der findes da præcis m forskellige karakterer på G, dvs. karaktererne udgør en ortonormal basis for vektorrummet $V = V_G$. Karaktergruppen for G er isomorf med G selv. For karaktererne på G gælder ortogonalitetsrelationerne:

$$(*) \qquad \frac{1}{m} \sum_{a \in G} \chi(a) = \begin{cases} 1 & \text{når } a = e \ (\chi = \chi_0) \\ 0 & \text{ellers} \end{cases},$$

$$(**) \qquad \frac{1}{m} \sum_{\chi} \chi(a) = \begin{cases} 1 & \text{når } a = e \ (\chi = \chi_0 \text{ (hovedk.)}) \\ 0 & \text{ellers} \end{cases}.$$

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 $(1 \leq j \leq r)$. Et vilkårligt element i G er da af formen

$$a = (a_1^{\alpha_1} \cdots, a_r^{\alpha_r}), \quad \alpha_j \in \mathbb{Z}/(m_j\mathbb{Z}), \ 1 \leq j \leq r,$$

og vi får øjensynlig definieret $m_1 \cdot \ldots \cdot m_r = m$ forskellige karakterer på G ved at sætte

$$\chi(a) = \xi_1^{\alpha_1} \cdot \ldots \cdot \xi_r^{\alpha_r},$$

hvor ξ_j er en vilkårlig m_j'te enhedsrod. Karaktergruppen er (indre) direkte produkt af de cykliske undergrupper $\langle \chi_j^{\alpha_j} \mid \alpha_j \in \mathbb{Z}/(m_j\mathbb{Z}) \rangle$, hvor $\chi_j(a) = e^{2\pi i \alpha_j / m_j}$, $1 \leq j \leq r$. Følgelig er karaktergruppen isomorf med G selv.

Vi har tidligere vist den første ortogonalitetsrelation (*), som jo siger at $M(\chi) = 1$ for $\chi = \chi_0$ og ellers 0. Relation (*) udtrykker derfor præcis, at matricen

$$\frac{1}{\sqrt{m}} \left(\chi_r(a_s) \right)_{r,s=1,\ldots,m},$$

hvor $\chi_1, \ldots, \chi_m$ er samtlige karakterer på G og $a_1, \ldots, a_m$ samtlige elementer i G, er en unitær matrix. Den anden ortogonalitetsrelation (**) følger

nu af at den transponerede til en unitær matrix er unitær. □

Eksempel 42. For abelske grupper af orden $m \leq 4$ har vi følgende karakterer, som bekvemt angives i såkaldte karaktertabeller:

$m = 1$:

	e
χ_0	1

$G \cong C_1$

$m = 2$:

	e	a
χ_0	1	1
χ_1	1	−1

$G \cong C_2$

$m = 3$:

	e	a	a^2
χ_0	1	1	1
χ_1	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_2	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$

$G \cong C_3$

$m = 4$:

	e	a	a^2	a^3
χ_0	1	1	1	1
χ_1	1	i	−1	$-i$
χ_2	1	−1	1	−1
χ_3	1	$-i$	−1	i

$G \cong C_4$

	$e = (e_1, e_2)$	(e_1, a_2)	(a_1, e_2)	(a_1, a_2)
χ_0	1	1	1	1
χ_1	1	1	−1	−1
χ_2	1	−1	1	−1
χ_3	1	−1	−1	1

$G \cong C_2 \times C_2$

Definition. En Dirichletkarakter modulo D, $D \in \mathbb{N}$, er en afbildning $\chi : \mathbb{Z} \to \mathbb{C}$ med egenskaberne

(a) χ er periodisk med periode D,

(b) $\chi(a) = 0$, når $\gcd(a, D) > 1$,

(c) restriktionen af χ til den primiske resthalsegruppe modulo D er en gruppekarakter.

Dirichletkarakteren, der er identisk 1 på alle primiske resthlasser modulo D kaldes hovedkarakteren modulo D, og den betegnes χ_0.

En Dirichletkarakter χ kaldes kvadratisk, såfremt $\chi \neq \chi_0$, $\chi^2 = \chi_0$.

En Dirichletkarakter χ modulo D kaldes lige (ulige), såfremt $\chi(-1) = 1$ ($\chi(-1) = -1$).

Eksempel 43. Vi vi angive Dirichletkarakterne modulo D for $D = 1, 2, 3, 4, 5, 6, 8$. På grund af periodiciteten er det i hvert tilfælde tilstrækkeligt at angive $\chi(a)$ for $0 \leq a < D$.

$D = 1$:

	0
χ_0	1

$D = 2$:

	0	1
χ_0	0	1

$D = 3$:

	0	1	2
χ_0	0	1	1
χ_1	0	1	-1

$D = 4$:

	0	1	2	3
χ_0	0	1	0	1
χ_1	0	1	0	-1

$D = 5$:

	0	1	2	3	4
χ_0	0	1	1	1	1
χ_1	0	1	i	$-i$	-1
χ_2	0	1	-1	-1	1
χ_3	0	1	$-i$	i	-1

$4 = 2^2$

$3 \equiv 2^3$

$D = 6$:

	0	1	2	3	4	5
χ_0	0	1	0	0	0	1
χ_1	0	1	0	0	0	-1

$D = 8$:

	0	1	2	3	4	5	6	7
χ_0	0	1	0	1	0	1	0	1
χ_1	0	1	0	1	0	-1	0	-1
χ_2	0	1	0	-1	0	1	0	-1
χ_3	0	1	0	-1	0	-1	0	1

Lad χ' være en Dirichletkarakter modulo D', og lad $D' \mid D$, $D \in \mathbb{N}$. Man kan da definere $\chi : \mathbb{Z} \to \mathbb{C}$ ved

$$\chi(a) = \begin{cases} 0, & \text{når } \gcd(a, D) > 1 \\ \chi'(a), & \text{når } \gcd(a, D) = 1 \ (\text{og } \gcd(a; D') = 1) \end{cases}$$

Det er klart, at χ er en Dirichletkarakter modulo D. χ siges at være <u>induceret</u> af χ'.

<u>Definition.</u> En Dirichletkarakter χ modulo D kaldes <u>primitiv</u>, såfremt χ ikke er induceret af en Dirichletkarakter χ' modulo D' for nogen ægte divisor D' i D.

<u>Bemærk.</u> Det fremgår af eksempel 43, at følgende af de anførte karakterer er primitive:
$\chi_0 \pmod 1$, $\chi_1 \pmod 3$, $\chi_1 \pmod 4$, $\chi_1, \chi_2, \chi_3 \pmod 5$, $\chi_1, \chi_3 \pmod 8$.
De øvrige karakterer ses let at være imprimitive.
Bemærk, at $\chi_1 \pmod 4$, $\chi_3 \pmod 8$, $\chi_1 \pmod 8$ optrådte i L-funktioner i henholdsvis eksempel 40 ($\mathbb{Q}(i)$) eksempel 41 ($\mathbb{Q}(\sqrt{2})$) og i øvelsen ($\mathbb{Q}(\sqrt{-2})$).

<u>Sætning 97.</u> Enhver Dirichletkarakter χ er induceret af en entydigt bestemt primitiv karakter. Modulus af denne primitive karakter betegnes f og kaldes χ's <u>minimale modulus</u> (tysk: <u>Führer</u>, engelsk: <u>conductor</u>).

Bevis: ① Hvis $\mathfrak{D}' \mid \mathfrak{D}$ indeholder enhver primisk restklasse a' mod $\mathfrak{D}'$ et element a som er primisk modulo $\mathfrak{D}$. Vi lader P være produktet af de primdivisorer i $\mathfrak{D}$, som ikke går op i $\mathfrak{D}'$, dvs. $\gcd(P, \mathfrak{D}') = 1$. Der findes da $x, y \in \mathbb{Z}$, så $xP + y\mathfrak{D}' = a' - 1$. Sæt $a = a' - y\mathfrak{D}' = 1 + xP$. Da er $\gcd(a, p) = 1$ for alle primdivisorer i $\mathfrak{D}$.

② Hvis χ mod $\mathfrak{D}$ er induceret af χ' mod $\mathfrak{D}'$ og af χ'' mod $\mathfrak{D}''$, er χ også induceret af $\tilde{\chi}$ mod $\tilde{\mathfrak{D}}$, hvor $\tilde{\mathfrak{D}} = \gcd(\mathfrak{D}', \mathfrak{D}'')$ og

$$\tilde{\mathfrak{D}}(\tilde{a}) = \begin{cases} 0, & \gcd(\tilde{a}, \tilde{\mathfrak{D}}) > 1 \\ \mathfrak{D}(a), & \gcd(a, \mathfrak{D}) = 1, \quad a \equiv \tilde{a} \pmod{\tilde{\mathfrak{D}}}. \end{cases}$$

Bemærk, at for $\gcd(a, \mathfrak{D}) = 1$ er $\chi(a) = \chi'(a) = \chi''(a)$, hvorfor χ's restriktion til sådanne a er periodisk med perioder $\mathfrak{D}'$ og $\mathfrak{D}''$ og dermed med periode $\tilde{\mathfrak{D}}$. Ifølge denne bemærkning og ① er $\tilde{\mathfrak{D}}$ da defineret på $\mathbb{Z}$, og $\tilde{\chi}$ inducerer tydeligvis $\mathfrak{D}$. Hvis specielt $\mathfrak{D}' = \mathfrak{D}''$ viser konstruktionen, at $\tilde{\mathfrak{D}} = \mathfrak{D}' = \mathfrak{D}''$ og $\tilde{\chi} = \chi' = \chi''$. Bemærk også, at $\tilde{\mathfrak{D}}$ inducerer $\mathfrak{D}'$ og $\mathfrak{D}''$.

③ Lad f være største fælles divisor for alle naturlige tal $\mathfrak{D}'$ for hvilke χ mod $\mathfrak{D}$ er induceret af en Dirichlet karakter modulo $\mathfrak{D}'$. Ifølge ② er χ da induceret af en entydig Dirichletkarakter mod f. Det er klart, at denne karakter er primitiv (jfl. definitionen af f), og at enhver karakter, som inducerer $\mathfrak{D}$, selv er induceret af denne (jvf. bemærkningerne i ②). □

Sætning 98. Samtlige primitive kvadratiske karakterer er angivet i følgende skema, hvor $m = p_1 \cdots p_r$ er et vilkårligt ulige kvadratfrit tal ($m = 1$ tilladt undtagen i første linie i skemaet), og

$$\left(\frac{x}{m}\right) = \left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_r}\right)$$

er produktet af Legendresymboler.
De primitive kvadratiske karakterer χ er i bijektiv forbindelse med de kvadratiske talllegemer, idet d er fastlagt ved betingelsen

$$\chi(p) = \left(\frac{d}{p}\right) \quad \text{for alle primtal } p.$$

f	$\chi(x)$	tilhørende kvadr. tallegeme	diskr. d	$\chi(-1)$
m	$\left(\frac{x}{m}\right)$	$\mathbb{Q}(\sqrt{m})$, $m \equiv 1\,(4)$	m	1
		$\mathbb{Q}(\sqrt{-m})$, $m \equiv -1\,(4)$	$-m$	-1
$4m$	$(-1)^{\frac{x-1}{2}}\left(\frac{x}{m}\right)$, x ulige	$\mathbb{Q}(\sqrt{-m})$, $m \equiv 1\,(4)$	$-4m$	-1
	0, x lige	$\mathbb{Q}(\sqrt{m})$, $m \equiv -1\,(4)$	$4m$	1
$8m$	$(-1)^{\frac{x^2-1}{8}}\left(\frac{x}{m}\right)$, x ulige	$\mathbb{Q}(\sqrt{2m})$, $m \equiv 1\,(4)$	$8m$	1
	0, x lige	$\mathbb{Q}(\sqrt{-2m})$, $m \equiv -1\,(4)$	$-8m$	-1
$8m$	$(-1)^{\frac{x-1}{2}+\frac{x^2-1}{8}}\left(\frac{x}{m}\right)$, x ulige	$\mathbb{Q}(\sqrt{-2m})$, $m \equiv 1\,(4)$	$-8m$	-1
	0, x lige	$\mathbb{Q}(\sqrt{2m})$, $m \equiv -1\,(4)$	$8m$	1

χ er lige (ulige), hvis og kun hvis det tilhørende kvadratiske tallegeme er reelt (imaginært).

Bevis: 1. Entydighed.

① Lad $D = 2^{\alpha} \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$; da er (jvf. sætning 43)

$G_D \cong G_{2^{\alpha}} \times G_{p_1^{\alpha_1}} \times \cdots \times G_{p_r^{\alpha_r}}$, hvor G_D er den primiske restklassegruppe modulo D. Enhver karakter χ mod D er da af formen $\chi = \chi' \chi_1 \cdots \chi_r$, hvor χ' er en karakter mod 2^{α} og χ_j en karakter modulo $p_j^{\alpha_j}$. Det er indirekte klart, at en nødvendig betingelse for at χ er primitiv, er at $\chi', \chi_1, \ldots, \chi_r$ alle er primitive.

② For $D = p^{\alpha}$, p ulige, $\alpha \geq 1$, er $\varphi(D) = p^{\alpha-1}(p-1)$, hvorfor $G_D \cong G' \times G''$, hvor $|G'| = p^{\alpha-1}$, $|G''| = p-1$. Da $|G'|$ er ulige, er ethvert element $\neq 1$ i G' af ulige orden, hvorfor den eneste reelle karakter på G' er hovedkarakteren. Heraf og af ① følger at der ikke findes nogen primitiv kvadratisk karakter mod p^{α} for $\alpha > 1$. For $\alpha = 1$, er $G_D \cong C_{p-1}$, hvorfor der er præcis to reelle karakterer mod D. Disse fremkommer ved at specificere $\chi(a) = \pm 1$ for en frembringer a i $G_D = G_p$. For $\chi(a) = 1$ er $\chi = \chi_0$ hovedkarakteren med $f = 1$. For $\chi(a) = -1$ er $f = p$, da $f \mid p$ og $f \neq 1$. Da Legendresymbolet $\left(\frac{a}{p}\right)$ er en Dirichletkarakter $\neq \chi_0$ (mod p) er $\chi(a) = \left(\frac{a}{p}\right)$ den eneste primitive kvadratiske karakter modulo p.

③ For $D = 2^\alpha$, $\alpha \geq 1$, er $\varphi(D) = 2^{\alpha-1}$. Det fremgår af eksempel 43, at der ikke er nogen primitiv kvadratisk karakter for $D = 2$. For $D = 4 = 2^2$ er der en primitiv kvadratisk karakter, nemlig

$$\chi(x) = \begin{cases} (-1)^{\frac{x-1}{2}}, & x \text{ ulige} \\ 0, & x \text{ lige} \end{cases}$$

For $D = 8 = 2^3$ er der to primitive kvadratiske karakterer, nemlig

$$\chi(x) = \begin{cases} (-1)^{\frac{x^2-1}{2}}, & x \text{ ulige} \\ 0, & x \text{ lige} \end{cases}, \qquad \frac{x^2-1}{8}$$

og

$$\chi(x) = \begin{cases} (-1)^{\frac{x-1}{2} + \frac{x^2-1}{2}}, & x \text{ ulige} \\ 0, & x \text{ lige} \end{cases}. \qquad \frac{x^2-1}{8}$$

④ Af ①, ② og ③ fremgår nu, at der højst er de i tabellens to første kolonner anførte primitive kvadratiske karakterer. Hermed er entydigheden vist.

2° Eksistens.

Vi må dertil eftervise, at de i tabellen anførte karakter er primitive med den i første kolonne anførte minimale modulus. Vi nøjes med beviset i tilfældet $f = m$, idet de øvrige tilfælde klares analogt. For $m = p_1 \cdots p_r$ findes præcis 2^r forskellige reelle Dirichletkarakterer modulo m, jvf. ① og ②, nemlig $\chi_{p_{j_1} \cdots p_{j_\ell}}(x) = \left(\frac{x}{p_{j_1}}\right) \cdots \left(\frac{x}{p_{j_\ell}}\right)$ for $\gcd(x, m) = 1$, hvor $\{p_{j_1}, \ldots, p_{j_\ell}\}$ er en vilkårlig delmængde af $\{1, \ldots, r\}$. Det er klart, at $\chi_{p_{j_1} \cdots p_{j_\ell}}$ også definerer en Dirichlet-

Indskud for (4):

For $D = 2^\alpha$, $\alpha > 3$, betragtes den primitive restklasse-gruppe $G_D = G_{2^\alpha}$ af orden $\varphi(2^\alpha) = 2^{\alpha-1}$.

Vi påstår nu, at der for alle $n \in \mathbb{N}_0$ gælder

$$(*) \qquad 5^{2^n} = 2^{n+2} \cdot h_n + 1 \quad , \quad h_n \text{ ulige}.$$

For $n = 0$ er

$$5^{2^0} = 5 = 2^2 \cdot 1 + 1 \quad ,$$

altså $h_0 = 1$. Antages $(*)$ at gælde for $n \in \mathbb{N}_0$, finder vi

$$5^{2^{n+1}} = (5^{2^n})^2 = (2^{n+2} \cdot h_n + 1)^2$$

$$= 2^{n+3} \cdot h_{n+1} + 1 \quad ,$$

hvor $h_{n+1} = 2^{n+1} \cdot h_n + h_n$ er ulige, dvs. formlen $(*)$ gælder også for $n+1$.

Af $(*)$ følger nu umiddelbart, at restklasse 5 mod 2^α har orden $2^{\alpha-2}$ i G_{2^α}, og følgelig er G_{2^α} enten isomorf med $C_{2^{\alpha-1}}$ eller med $C_{2^{\alpha-2}} \times C_2$.

Det bemærkes nu, at $C_{2^{\alpha-1}}$ har præcis 2 reelle karakterer (bestemt ved værdien ± 1 på en frembringer), og at $C_{2^{\alpha-2}} \times C_2$ af samme grund har præcis 4 reelle karakterer. Heraf følger igen, at der i første tilfælde er præcis 2 reelle Dirichlet karakterer modulo 2^α og i andet tilfælde præcis 4. Da de 4 primitive Dirichlet karakterer mod $f = 1, 4, 8$ inducerer 4 forskellige reelle Dirichlet karakterer modulo 2^α, er $G_{2^\alpha} \cong C_{2^{\alpha-2}} \times C_2$

og ingen af de 4 karakterer er primitive

karakter modulo $p_{j_1} \cdots p_{j_\ell}$, og at disse 2^r karakterer er samtlige mulige primitive karakterer modulo alle divisorerne i m. Da hver Dirichlet karakter modulo m er induceret af en primitiv karakter modulo en divisor i m, følger at samtlige 2^r karakterer er primitive modulo $p_{j_1} \cdots p_{j_\ell}$, altså specielt, at $\chi(x) = \left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_r}\right)$ er primitiv modulo m, dvs. $f = m$.

3. Korrespondance med kvadratisk tallegeme.

Vi nøjes igen med beviset i første tilfælde $f = m$, idet de øvrige tilfælde behandles analogt. Såfremt $p \mid m = \pm d$ er $\chi(p) = 0 = \left(\frac{d}{p}\right)$. I hovedtilfældet $p \nmid m$ fås ved brug af reciprocitetssætningen:

$$\chi(p) = \left(\frac{p}{m}\right) = \left(\frac{p}{p_1}\right) \cdot \cdots \cdot \left(\frac{p}{p_r}\right)$$

$$= (-1)^{\frac{p-1}{2} \cdot \left(\frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2}\right)} \left(\frac{p_1}{p}\right) \cdot \cdots \cdot \left(\frac{p_r}{p}\right)$$

$$= (-1)^{\frac{p-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{p}\right)$$

$$= \begin{cases} \left(\frac{m}{p}\right) = \left(\frac{d}{p}\right), & m \equiv 1 \pmod 4 \text{ for } \mathbb{Q}(\sqrt{m}) \\ (-1)^{\frac{p-1}{2}} \left(\frac{m}{p}\right) = \left(\frac{-m}{p}\right) = \left(\frac{d}{p}\right), & m \equiv -1 \pmod 4 \text{ for } \mathbb{Q}(\sqrt{-m}) \end{cases}$$

Bemærk: Enhver primisk restklasse modulo m indeholder uendelig mange primtal. Dette følger af Dirichlet's sætning om primtal i differensrækker, som vi vil se senere.

4. χ lige eller ulige.

Dette fremgår som anført ved beregning af $\chi(-1)$. Vi vil igen

nøjes med tilfældet $f = m$, hvor vi finder

$$\chi(-1) = \left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right)$$

$$= (-1)^{\frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2}}$$

$$= (-1)^{\frac{m-1}{2}}$$

Dette giver det ønskede resultat. □

Øvelse. Konstruer den primitive kvadratiske karakter for alle $f \leq 20$.

Definition. Lad χ være en Dirichlet karakter modulo D og lad $\zeta = e^{2\pi i/D}$. Summen

$$\tau_c(\chi) = \sum_{x \bmod D} \chi(x)\, \zeta^{cx}, \qquad c \bmod D,$$

hvor x gennemløber alle restklasser modulo D, kaldes en Gaussisk sum. τ_1 kaldes en normeret Gaussisk sum.

Sætning 99. Lad χ være en primitiv kvadratisk karakter med minimal modulus f, og lad $\zeta = e^{2\pi i/f}$. Der gælder da

$$\tau(\chi) = \tau_1(\chi) = \begin{cases} \sqrt{f} & \text{hvis } \chi \text{ er lige} \\ i\sqrt{f} & \text{hvis } \chi \text{ er ulige} \end{cases}.$$

Bevis: ① For $f = 2^\alpha$, $\alpha = 2, 3$, gælder formlen idet:

$$\tau(\chi) = 1 \cdot i + (-1)(-i) = 2i = \sqrt{4}\, i \quad \text{for } f = 4,$$

$$\tau(\chi) = 1 \cdot \left(\tfrac{1}{\sqrt{2}} + \tfrac{i}{\sqrt{2}}\right) - 1 \cdot \left(-\tfrac{1}{\sqrt{2}} + \tfrac{i}{\sqrt{2}}\right) - 1 \cdot \left(-\tfrac{1}{\sqrt{2}} - \tfrac{i}{\sqrt{2}}\right) + 1 \cdot \left(\tfrac{1}{\sqrt{2}} - \tfrac{i}{\sqrt{2}}\right)$$

$$= \sqrt{8} \quad \text{for } f = 8, \ \chi \text{ karakter for } \mathbb{Q}(\sqrt{2}).$$

$$\tau(\chi) = 1 \cdot \left(\tfrac{1}{\sqrt{2}} + \tfrac{i}{\sqrt{2}}\right) + 1 \cdot \left(-\tfrac{1}{\sqrt{2}} + \tfrac{i}{\sqrt{2}}\right) - 1 \left(-\tfrac{1}{\sqrt{2}} - \tfrac{i}{\sqrt{2}}\right) - 1 \cdot \left(\tfrac{1}{\sqrt{2}} - \tfrac{i}{\sqrt{2}}\right)$$

$$= \sqrt{8}\, i \quad \text{for } f = 8, \ \chi \text{ karakter for } \mathbb{Q}(\sqrt{-2}).$$

② Vi vil dernæst vise formlen for $f = p =$ ulige primtal, hvor følgelig $\chi(x) = \left(\frac{x}{p}\right)$ simpelthen er Legendre symbolet. Vi har da

$$\tau(\chi) = \sum_{x \bmod p} \left(\frac{x}{p}\right) \zeta^x, \qquad \zeta = e^{2\pi i/p}$$

$$= \sum_{\substack{\left(\frac{a}{p}\right) = 1 \\ a \bmod p}} \zeta^a - \sum_{\substack{\left(\frac{b}{p}\right) = -1 \\ b \bmod p}} \zeta^b$$

Da

$$1 + \sum \zeta^a + \sum \zeta^b = \sum_{j=0}^{p-1} \zeta^j = 0,$$

er

$$\tau(\chi) = 1 + 2 \sum_{\substack{\left(\frac{a}{p}\right) = 1 \\ a \bmod p}} \zeta^a = \sum_{x \bmod p} \zeta^{x^2}.$$

Vi finder

$$\overline{\tau}(\chi) = \sum_{x \bmod p} \left(\frac{x}{p}\right) \zeta^{-x}$$

$$= \sum_{x \bmod p} \left(\frac{-x}{p}\right) \zeta^{\Theta x},$$

altså

$$\overline{\tau}(\chi) = \left(\frac{-1}{p}\right) \tau(\chi).$$

Dette viser, at $\tau(\chi)$ er reel når $p \equiv 1\ (4)$ og rent imaginær når $p \equiv -1\ (4)$.

Vi ønsker dernæst at bestemme $|\tau(\chi)|$. Dertil betragtes vektorrummet V af komplekse funktioner på restklasserne modulo p, altså $\dim_{\mathbb{C}} V = p$, med indre produkt

$$(f, g) = \frac{1}{p} \sum_{x \bmod p} f(x)\, \overline{g(x)}.$$

Heri er funktionerne

$$\{ f_c : x \mapsto \zeta^{cx} \mid c \bmod p \}$$

en ortonormal basis, idet

$$(f_c, f_{c'}) = \frac{1}{p} \sum_{x \bmod p} \zeta^{(c-c')x} = \begin{cases} 1 & \text{for } c \equiv c'\ (p) \\ 0 & \text{for } c \not\equiv c'\ (p) \end{cases}$$

Følgelig kan $\chi \in V$ fremstilles som "Fourierrække"

$$\chi = \sum_{c \bmod p} \alpha_c f_c,$$

hvor

$$\alpha_c = (\chi, f_c) = \frac{1}{p} \sum_{x \bmod p} \chi(x)\, \zeta^{-cx},$$

dvs.

$$\alpha_c = \frac{1}{p}\, \tau_{-c}(\chi).$$

Det observeres nu, at

$$\tau_c(\chi) = \sum_{x \bmod p} \chi(x)\, \zeta^{cx} = \begin{cases} \sum_{x \bmod p} \chi(x) = 0 & \text{for } c \equiv 0 \ (p) \\ \sum_{x \bmod p} \chi\left(\frac{x}{c}\right) \zeta^{x} = \frac{\tau(\chi)}{\chi(c)} & \text{for } c \not\equiv 0 \ (p) \end{cases}$$

Heraf følger, at

$$|\alpha_c| = \begin{cases} 0 & \text{for } c \equiv 0 \ (p) \\ \frac{|\tau(\chi)|}{p} & \text{for } c \not\equiv 0 \ (p) \end{cases}$$

Vi vil nu på to forskellige måder beregne $\|\chi\|^2$. Dels er

$$\|\chi\|^2 = \frac{1}{p} \sum_{x \bmod p} |\chi(x)|^2 = \frac{p-1}{p},$$

dels er - da f_c'erne udgør et ortonormalsystem -

$$\|\chi\|^2 = \Big\| \sum_{c \bmod p} \alpha_c f_c \Big\|^2 = \sum_{c \bmod p} |\alpha_c|^2 = \frac{p-1}{p^2} |\tau(\chi)|^2.$$

Ved at sammenholde de to udtryk for $\|\chi\|^2$ fås derfor

$$|\tau(\chi)| = \sqrt{p}\,.$$

Sammenholdes dette endelig med at $\tau(\chi)$ er reel (rent imaginær) når $p \equiv 1\,(4)$ ($p \equiv -1\,(4)$) fås

$$(*) \qquad \tau(\chi) = \begin{cases} \pm\sqrt{p} & \text{når } p \equiv 1\,(4) \\ \pm i\sqrt{p} & \text{når } p \equiv -1\,(4) \end{cases}.$$

Vi mangler derfor "blot" at vise, at fortegnet i (*) er plus begge steder. Denne fortegnsbestemmelse er den egentlige vanskelighed ved bestemmelsen af $\tau(\chi)$, og der findes en række smukke beviser herfor (jvf. E. Landau: Vorlesungen über Zahlentheorie (1927), Vol I, der indeholder 4 forskellige beviser). Vi fremstrækker det mest algebraiske af de kendte beviser. Det skyldes I. Schur. Udgangspunktet er matricen

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix},$$

for hvilken

$$\operatorname{tr} A = \sum_{x=0}^{p-1} \zeta^{x^2} = \tau(\chi).$$

Det observeres ved en simpel udregning, at

$$A^2 = \begin{pmatrix} p & 0 & \cdots & 0 \\ 0 & 0 & \cdots & p \\ \vdots & \vdots & \ddots & \vdots \\ 0 & p & \cdots & 0 \end{pmatrix},$$

idet det benyttes, at

$$\sum_{x=0}^{p-1} \zeta^{cx} = \begin{cases} p & \text{når } c \equiv 0 \pmod p \\ 0 & \text{når } c \not\equiv 0 \pmod p \end{cases}.$$

Endelig følger heraf at

$$A^4 = \begin{pmatrix} p^2 & 0 & \cdots & 0 \\ 0 & p^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p^2 \end{pmatrix}.$$

Lad $\lambda_1, \cdots, \lambda_p$ være de karakteristiske rødder for A.

Da

$$\begin{aligned} \det (A^2 - t^2 I) &= \det (A - tI)(A + tI) \\ &= \det (A - tI) \cdot \det (A + tI) \\ &= (\lambda_1 - t) \cdots (\lambda_p - t)(\lambda_1 + t) \cdots (\lambda_p + t) \\ &= (\lambda_1^2 - t^2) \cdots (\lambda_p^2 - t^2) \end{aligned}$$

har A^2 de karakteristiske rødder $\lambda_1^2, \cdots, \lambda_p^2$ og følgelig A^4 de karakteristiske rødder $\lambda_1^4, \cdots, \lambda_p^4$. Imidlertid er det klart, at $\lambda_1^4 = \cdots = \lambda_p^4 = p^2$, således at $\lambda_j^2 = \pm p$ for $1 \le j \le p$. Da

$$\sum_1^p \lambda_j^2 = \operatorname{tr} A^2 = p,$$

når

$$\lambda_j^2 = \begin{cases} p & \text{for } \frac{p+1}{2} \text{ værdier af } j \in \{1,\cdots,p\} \\ -p & \text{for } \frac{p-1}{2} \text{ værdier af } j \in \{1,\cdots,p\}. \end{cases}$$

De karakteristiske rødder $\lambda_1, \cdots, \lambda_p$ for A er derfor

$$\varepsilon\sqrt{p} \quad \text{med multiplicitet } r_\varepsilon, \quad \varepsilon \in \{\pm 1, \pm i\},$$

og hvor

$$(**) \qquad r_1 + r_{-1} = \frac{p+1}{2}, \quad r_i + r_{-i} = \frac{p-1}{2}.$$

Da

$$\operatorname{tr} A = \sum_1^p \lambda_j = (r_1 - r_{-1} + i(r_i - r_{-i}))\sqrt{p}$$

$$= \tau(\chi) = \begin{cases} \pm\sqrt{p} & \text{når } p \equiv 1 \ (4) \\ \pm i\sqrt{p} & \text{når } p \equiv -1 \ (4) \end{cases}$$

ifølge (*), er

$$r_1 - r_{-1} = \pm 1, \quad r_i - r_{-i} = 0 \quad \text{for } p \equiv 1 \ (4),$$

$$r_1 - r_{-1} = 0, \quad r_i - r_{-i} = \pm 1 \quad \text{for } p \equiv -1 \ (4).$$

Sammenholdt med (**) giver dette

$$(***) \begin{cases} r_1 = \frac{p+1\pm 2}{4}, \ r_{-1} = \frac{p+1-(\pm 2)}{4}, \ r_i = r_{-i} = \frac{p-1}{4}, & p \equiv 1 \ (4), \\ r_1 = r_{-1} = \frac{p+1}{4}, \ r_i = \frac{p-1\pm 2}{4}, \ r_{-i} = \frac{p-1-(\pm 2)}{4}, & p \equiv -1 \ (4), \end{cases}$$

hvor fortegnene $\pm$ følger fortegnene i (*).

For at fiksere disse fortegn udregnes $\det A$ eller rettere $\arg \det A$ på to forskellige måder. For det første fås af (***)

$$\det A = \prod_1^p \lambda_j = (\sqrt{p})^p (-1)^{r_{-1}} i^{r_i} (-i)^{r_{-i}} ,$$

hvor for

$$\arg \det A = (-1)^{r_{-1}} i^{r_i} (-i)^{r_{-i}} = \begin{cases} (-1)^{\frac{p+1-(\pm 2)}{4}} , & p \equiv 1 (4) \\ (-1)^{\frac{p+1}{4}} (\pm i) , & p \equiv -1 (4) \end{cases} .$$

For det andet er $\det A$ en Vandermonde determinant, dvs.

$$\det A = \prod_{0 \le r < s \le p-1} (\zeta^s - \zeta^r)$$

$\zeta = e^{\pi i/p}$

$$= \prod_{r<s} \eta^{r+s} (\eta^{s-r} - \eta^{-(s-r)}) , \quad \eta = e^{2\pi i/p}$$

$$= \prod_{r<s} \eta^{r+s} \prod_{r<s} 2i \sin \frac{(s-r)\pi}{p} .$$

$$= \left(\prod_{r<s} \eta^{r+s} \right) i^{\frac{p(p-1)}{2}} \cdot 2^{\frac{p(p-1)}{2}} \cdot \prod_{r<s} \sin \frac{(s-r)\pi}{p} .$$

Her er

$$\sum_{0 \le r < s \le p-1} (r+s) = \sum_{s=1}^{p-1} \left(\frac{s(s-1)}{2} + s^2 \right) = 2p \left(\frac{p-1}{2} \right)^2 ,$$

idet man benytter den velkendte formel (vises ved induktion):

$$\sum_{1}^{n} s^2 = \frac{1}{6} n(n+1)(2n+1).$$

Følgelig er

$$\prod_{r<s} \eta^{r+s} = \eta^{\sum_{r<s}(r+s)} = (\eta^{2p})^{\left(\frac{p-1}{2}\right)^2} = 1.$$

Endvidere bemærkes at

$$\sin \frac{(s-r)\pi}{p} > 0 \quad \text{for} \quad 0 \le r < s \le p-1.$$

Vi finder derfor

$$\overset{\text{sgn}}{\arg} \det A = i^{\frac{p(p-1)}{2}}.$$

Ved at sammenholde de to udtryk for $\overset{\text{sgn}}{\arg} \det A$ fås

$$i^{\frac{p(p-1)}{2}} = (-1)^{\frac{p+1-(\pm 2)}{4}} = i^{\frac{p+1-(\pm 2)}{2}} \quad \text{for } p \equiv 1\ (4),$$

$$i^{\frac{p(p-1)}{2}} = (-1)^{\frac{p+1}{4}} (\pm i) = \pm i^{\frac{p+3}{2}} \quad \text{for } p \equiv -1\ (4).$$

Dette viser, at

$$\frac{p-1}{2} \equiv p \cdot \frac{p-1}{2} \equiv \frac{p+1-(\pm 2)}{2} \pmod 4 \quad \text{for } p \equiv 1\ (4),$$

$$-\frac{p-1}{2} \equiv p \cdot \frac{p-1}{2} \equiv \pm \frac{p+3}{2} \pmod 4 \quad \text{for } p \equiv -1\ (4).$$

Heraf følger umiddelbart, at fortegnene er + begge steder.

③ Vi vil endelig vise formlen almost, dvs. for $f = m$, $4m$, $8m$, hvor $m = p_1 \cdots p_r$ er produkt af forskellige ulige primtal. Vi nøjes igen med at vise tilfældet $f = m = p_1 \cdots p_r$, idet de øvrige tilfælde opnås ved små modifikationer.

Lad

$$c = \sum_1^r \frac{f}{p_j} = p_2 \cdots p_r + p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1}.$$

Da er $\gcd(c, p_j) = 1$ for $1 \leq j \leq r$, altså $\gcd(c, f) = 1$.

Der gælder derfor

$$\tau(\chi) = \chi(c)\, \overline{\tau}_c(\chi),$$

hvor χ er den primitive kvadratiske karakter mod f.

I det g er antallet af primtal $p_j \equiv -1 (4)$, $1 \leq j \leq r$, fås

$$\chi(c) = \left(\frac{c}{f}\right) = \prod_1^r \left(\frac{c}{p_j}\right) = \prod_{j=1}^r \prod_{i \neq j} \left(\frac{p_i}{p_j}\right)$$

$$= \prod_{1 \leq i < j \leq r} \left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right)$$

$$= (-1)^{\frac{g(g-1)}{2}}.$$

Endvidere finder vi

$$\overline{\tau}_c(\chi) = \sum_{x \bmod f} \chi(x)\, \zeta^{cx}, \qquad \zeta = e^{2\pi i/f},$$

$$= \sum_{x \bmod f} \left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_r}\right) \zeta^{\frac{f}{p_1}x} \cdots \zeta^{\frac{f}{p_r}x}$$

$$= \prod_{j=1}^{r} \left(\sum_{x \bmod p_j} \left(\frac{x}{p_j}\right) \zeta_j^{\,x} \right), \quad \zeta_j = \zeta^{\frac{f}{p_j}} = e^{\frac{2\pi i}{p_j}},$$

$$= \prod_{j=1}^{r} \varepsilon_j \sqrt{p_j}, \quad \text{hvor } \varepsilon_j = \begin{cases} 1, & p_j \equiv 1 \,(4) \\ i & p_j \equiv -1 \,(4) \end{cases}$$

$$= i^g \sqrt{f}.$$

Sammenfattende får vi derfor

$$\tau(\chi) = (-1)^{\frac{g(g-1)}{2}} i^g \sqrt{f}$$

$$= i^{g^2} \sqrt{f}$$

$$= \begin{cases} \sqrt{f} & \text{for } g \text{ lige} \leftrightarrow m \equiv 1 \,(4) \leftrightarrow \chi \text{ lige} \\ i\sqrt{f} & \text{for } g \text{ ulige} \leftrightarrow m \equiv -1 \,(4) \leftrightarrow \chi \text{ ulige} \end{cases}.$$

Hermed er sætning 99 bevist. □

Som en første anvendelse af Gaussiske summer vil vise reciprocitetssætningen og 2. supplement til denne (sætning 61), idet det huskes, at 1. supplement var en direkte følge af Eulers kriterium.

Lad p være et ulige primtal og χ en primitiv kvadratisk karakter af minimal modulus f, hvor $p \nmid f$. Vi betragter for $\zeta = e^{2\pi i/f}$ de Gaussiske summer

$$\tau(\chi) = \sum_{x \bmod f} \chi(x)\, \zeta^x \quad , \quad \tau_p(\chi) = \sum_{x \bmod f} \chi(x)\, \zeta^{px}.$$

Da p er primisk med f er

$$\tau_p(\chi) = \frac{1}{\chi(p)}\, \tau(\chi) = \chi(p)\, \tau(\chi).$$

Endvidere er ifølge sætning 99

$$\tau(\chi)^2 = \chi(-1)\, f.$$

Vi vil midlertidigt regne i ringen $\mathbb{Z}[\zeta]$, som er en delring af ringen af hele elementer i cirkeldelingslegemet $\mathbb{Q}(\zeta)$. Da p er et ulige primtal er

$$\tau(\chi)^p \equiv \sum_{x \bmod f} \chi(x)^p\, \zeta^{px} \qquad (\bmod p)$$

$$= \sum_{x \bmod f} \chi(x)\, \zeta^{px}$$

$$= \tau_p(\chi)$$

$$= \chi(p)\, \tau(\chi).$$

Heraf følger

$$\tau(\chi)^2 \left(\chi(p) - (\bar{\tau}(\chi)^2)^{\frac{p-1}{2}} \right) \equiv 0 \pmod{p}$$

eller

$$\chi(-1) f \left(\chi(p) - \chi(-1)^{\frac{p-1}{2}} f^{\frac{p-1}{2}} \right) \equiv 0 \pmod{p}.$$

Da $\mathbb{Z}[\zeta] \cap \mathbb{Q} = \mathbb{Z}$, gælder sidstnævnte kongruens også i $\mathbb{Z}$, og da $p \nmid f$ er følgelig

$$\chi(p) \equiv \chi(-1)^{\frac{p-1}{2}} f^{\frac{p-1}{2}} \pmod{p}.$$

Heraf fås ved brug af Eulers kriterium (sætning 57)

$$\chi(p) \equiv \chi(-1)^{\frac{p-1}{2}} \left(\frac{f}{p}\right) \pmod{p}.$$

Da begge sider af kongruensen har værdien ± 1 og $p > 2$ gælder følgelig

$$(*) \qquad \chi(p) = \chi(-1)^{\frac{p-1}{2}} \left(\frac{f}{p}\right).$$

For $f = q$ et ulige primtal forskelligt fra p er $\chi(x) = \left(\frac{x}{q}\right)$, og formlen (*) specialiserer derfor til

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{q}{p}\right),$$

som ved brug af Eulers kriterium (el. 1. supplement) giver

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

For $f = 8$ og χ den lige primitive kvadratiske karakter modulo 8, for hvilken $\chi(x) = (-1)^{\frac{x^2-1}{8}}$ for x ulige og $\chi(x) = 0$ for x lige, specialiserer formlen (*) til

$$\left(\frac{2}{p}\right) = \left(\frac{8}{p}\right) = \chi(p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{for } p \equiv \pm 1 \ (8) \\ -1 & \text{for } p \equiv \pm 3 \ (8) \end{cases},$$

hvilket netop er 2. supplement til reciprocitetssætningen.

Det bemærkes, at vi kun benyttede værdien af $\tau(\chi)^2$, dvs. det præcise fortegn for $\tau(\chi)$ er uden betydning for dette bevis for reciprocitetssætningen og 2. supplement til denne.

Bemærk også, at da

$$\sqrt{\chi(-1) f} = \tau(\chi) \in \mathbb{Q}(\zeta), \quad \zeta = e^{2\pi i/f},$$

indeholder cirkeldelingslegemet $\mathbb{Q}(\zeta)$ det kvadratiske tallegeme $\mathbb{Q}(\sqrt{\chi(-1) f})$. Denne omstændighed blev vist direkte i sætning 87 i specialtilfældet $f = l =$ ulige primtal.

—

Genusteori for kvadratiske tallegemer.

Sætning 100. Lad G være en endelig abelsk gruppe, og

$$G^2 = \{ x^2 \mid x \in G \},$$

$$G_2 = \{ x \in G \mid x^2 = e \}, \text{ hvor } e \text{ er } G\text{'s etelement.}$$

Da er G^2 og G_2 undergrupper i G, og

$$G/G^2 \cong G_2 \cong \underbrace{C_2 \times C_2 \times \cdots \times C_2}_{g}, \quad g \geq 0.$$

Bevis: Da G er en endelig gruppe er en delmængde $H \subset G$ en undergruppe i G, netop hvis $e \in H$ og $x, y \in H \Rightarrow xy \in H$. Det er klart, at G^2 og G_2 opfylder disse betingelser, dvs. G^2 og G_2 er undergrupper i G.

Det bemærkes dernæst, at for $n = n_1 n_2$, $\gcd(n_1, n_2) = 1$, er $C_n \cong C_{n_1} \times C_{n_2}$; thi er a_1 og a_2 frembringere for henholdsvis C_{n_1} og C_{n_2} er $(a_1, a_2) \in C_{n_1} \times C_{n_2}$ af orden $n = n_1 n_2 =$ mindste fælles multiplum af n_1 og n_2.

Kombineres denne bemærkning med sætning 95, korollar, følger at

$$G \cong C_{2^{\alpha_1}} \times \cdots \times C_{2^{\alpha_g}} \times C_{p_1^{\beta_1}} \times \cdots \times C_{p_r^{\beta_r}},$$

hvor $\alpha_j \in \mathbb{N}$, $\beta_s \in \mathbb{N}$ og $p_1, \ldots, p_r$ er ulige primtal.

Lad $a_1, \ldots, a_g, b_1, \ldots, b_r$ være frembringere for de cykliske komponenter i denne fremstilling af G. Da er

$$G^2 \cong C_{2^{\alpha_1 - 1}} \times \cdots \times C_{2^{\alpha_g - 1}} \times C_{p_1^{\beta_1}} \times \cdots \times C_{p_r^{\beta_r}},$$

altså

$$G/G^2 \cong C_2 \times \cdots \times C_2 \qquad (g \text{ faktorer}).$$

På den anden side er

$$G_2 \cong C_2 \times \cdots \times C_2 \qquad (g \text{ faktorer}).$$

Vi skal her bemærke, at

$$\left(C_{2^{\alpha_j}}\right)^2 = \{q_j^2, q_j^4, \cdots, q_j^{2^{\alpha_j}}\} \cong C_{2^{\alpha_j-1}},$$

$$\left(C_{p_s^{\beta_s}}\right)^2 = \{b_s^2, b_s^4, \cdots b_s^{p_s^{\beta_s}-1}, b_s^{p_s^{\beta_s}+1}, \cdots b_s^{2p_s^{\beta_s}}\} = C_{p_s^{\beta_s}},$$

$$\left(C_{2^{\alpha_j}}\right)_2 = \{q_j^{2^{\alpha_j-1}}, q_j^{2^{\alpha_j}}\} \cong C_2,$$

$$\left(C_{p_s^{\beta_s}}\right)_2 = \{b_s^{p_s^{\beta_s}}\} \cong C_1. \qquad \square$$

<u>Definition.</u> Lad $k = \mathbb{Q}(\sqrt{d})$ være et kvadratisk tallegeme af diskriminant d. For brudne ideler $\mathfrak{a}, \mathfrak{b} \neq (0)$ i k definerer vi:

(i) $\mathfrak{a} \sim \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} = (\alpha)$, $\alpha \in k$,

(ii) $\mathfrak{a} \approx \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} = (\alpha)$, $\alpha \in k$ med $N(\alpha) > 0$,

(iii) $\mathfrak{a} \approx\!\!\approx \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} = (\alpha)\mathfrak{M}^2$, $\alpha \in k$ med $N(\alpha) > 0$ og $\mathfrak{M}$ et brudent ideal i k.

De tre ækvivalensrelationer kaldes <u>ækvivalens</u> ($\sim$), <u>streng</u> (eller egentlig) <u>ækvivalens</u> ($\approx$) og <u>genus ækvivalens</u> ($\approx\!\!\approx$).

Det er klart, at $\mathfrak{a} \approx \mathfrak{b} \Rightarrow \mathfrak{a} \sim \mathfrak{b}$ og at $\mathfrak{a} \approx \mathfrak{b}$ $\Rightarrow \mathfrak{a} \approx \mathfrak{b}$ (brug $\mathfrak{m} = (1)$). Lad $\mathcal{D}$ være gruppen af brudne idealer, $\mathcal{D}_1 = \{\mathfrak{a} \in \mathcal{D} \mid \mathfrak{a} \sim (1)\}$, $\mathcal{D}_1^+ = \{\mathfrak{a} \in \mathcal{D} \mid \mathfrak{a} \approx (1)\}$, $\mathcal{D}_1^{gen} = \{\mathfrak{a} \in \mathcal{D} \mid \mathfrak{a} \approx (1)\}$. Det er da klart, at $\mathcal{D}_1$, $\mathcal{D}_1^+$, $\mathcal{D}_1^{gen}$ er undergrupper i $\mathcal{D}$, og vi betragter kvotientgrupperne (klassegrupperne):

$$H = \mathcal{D}/\mathcal{D}_1, \quad H^+ = \mathcal{D}/\mathcal{D}_1^+, \quad H^{gen} = \mathcal{D}/\mathcal{D}_1^{gen},$$

der kaldes henholdsvis <u>klassegruppen</u>, <u>den egentlig klassegruppe</u> og <u>genus klassegruppen</u>.

Det viser sig at være nyttigt at inddele de kvadratiske tallegemer $\mathbb{Q}(\sqrt{d})$ i 3 typer.

Type <u>I</u>: består af samtlige imaginær kvadratiske tallegemer.

Type <u>II</u>: består af sidstnævnte reelle kvadratiske tallegemer, for hvilke fundamentalenheden $\varepsilon_1 > 1$ har $N(\varepsilon_1) = -1$,

Type <u>III</u>: består af sidstnævnte kvadratiske tallegemer, for hvilke fundamentalenheden $\varepsilon_1 > 1$ har $N(\varepsilon_1) = +1$.

<u>Sætning 101.</u> $H = H^+$, såfremt k er af type <u>I</u> el. <u>II</u>. H er undergruppe af index 2 i H^+, såfremt k er af type <u>III</u>.

<u>Bevis:</u> Hvis k er af type <u>I</u> har alle $\alpha \in k^*$, $N(\alpha) > 0$, dvs. der er ingen forskel på $\sim$ og $\approx$, og følgelig er $H = H^+$. Hvis k er af type <u>II</u> gælder: $\mathfrak{a} \in \mathcal{D}_1 \Rightarrow \mathfrak{a} = (\alpha)$, $\alpha \in k^*$, $\Rightarrow \mathfrak{a} = (\alpha\varepsilon_1)$, og da $N(\alpha\varepsilon_1) = N(\alpha)N(\varepsilon_1) = -N(\alpha)$ gælder

$\mathfrak{A} \sim (1)$, altså $\mathfrak{A} \in \mathcal{D}_1^+$. Igen er $\sim$ og $\approx$ samme relation, dvs. $H = H^+$. Lad endelig k være af type III. Da $\mathcal{D}_1^+$ er en undergruppe af $\mathcal{D}_1$ og $H^+/H = \mathcal{D}/\mathcal{D}_1^+ / \mathcal{D}/\mathcal{D}_1$ $\cong \mathcal{D}_1/\mathcal{D}_1^+$, skal vi blot vise, at $\mathcal{D}_1$ består af præcis to egentlige ækvivalensklasser. Hertil bemærkes, at $\mathfrak{A} \in \mathcal{D}_1$ $\Rightarrow \mathfrak{A} = (\alpha) \Rightarrow \mathfrak{A} \sim (1)$ hvis $N(\alpha) > 0$ og $\mathfrak{A} \sim (\sqrt{d})$ hvis $N(\alpha) < 0$, idet $N(\sqrt{d}) = -d < 0$. Heraf følger, at $\mathcal{D}$ højst består af to egentlige ækvivalensklasser, repræsenteret ved (1) og $(\sqrt{d})$. Antag endelig at $(1) \sim (\sqrt{d})$. Da eksisterer et $\alpha \in k^*$ med $N(\alpha) > 0$, så $(\sqrt{d}) = (\alpha)$, men følgelig er $\frac{\sqrt{d}}{\alpha} = \varepsilon \in \mathcal{O}_k^*$ og $N(\varepsilon) < 0$, i modstrid med at k er af type III. □

<u>Sætning 102.</u> Lad $k = \mathbb{Q}(\sqrt{d})$ af diskriminant $d = d_0 d_1 \cdots d_g$, hvor $g+1$ er antallet af forskellige primdivisorer i d og $d_0 = -4, 8, -8$ således at d er lige og $d_j = (-1)^{\frac{p_j - 1}{2}} p_j$, $j \geq 1$, hvor p_j er et ulige primtal. Da er

$$H^{gen} \cong H^+ / H^{+2} \cong H_2^+ \cong C_2^{\,g}.$$

Der gælder

$$2^g \mid h^+ = |H^+|,$$

og

$$h^+ \text{ ulige} \iff g = 0.$$

Beviset for sætning 102, kræver nogle forberedende sætninger og definitioner.

Definition. Lad $k = \mathbb{Q}(\sqrt{d})$ og lad $'$ angive konjugeringen givet ved $\sqrt{d} \mapsto -\sqrt{d}$, og udstrakt til element i k, delmængde af k og system af delmængder af k på naturlig måde.

Et helt ideal $\mathfrak{A}$ i k kaldes ambisk, hvis

(i) $\mathfrak{A} = \mathfrak{A}'$,

(ii) $\mathfrak{A}$ er primitiv, dvs. ikke deleelig med idealet (n) for noget $n > 1$, $n \in \mathbb{N}$.

En egentlig idealklasse C kaldes ambisk, hvis $C = C'$. [ambisk (latin) = tvetydig].

Sætning 103. Lad $k = \mathbb{Q}(\sqrt{d})$. Da gælder (med betegnelserne i sætning 102): Der findes præcis 2^{g+1} ambisk idealer, nemlig

$$\{ \mathfrak{p}_0^{n_0} \cdots \mathfrak{p}_g^{n_g} \mid n_0, \dots, n_g \in \{0,1\} \},$$

hvor $\mathfrak{p}_0, \dots, \mathfrak{p}_g$ er samtlige forgrenede primidealer i $\mathfrak{O}_k$ fx fastlagt så $\mathfrak{p}_j \mid (d_j)$ for $0 \leq j \leq g$.

Bevis: Det bemærkes først, at $\mathfrak{p} = \mathfrak{p}'$, når $\mathfrak{p}$ er et forgrenet eller trægt primideal, men $\mathfrak{p} \neq \mathfrak{p}'$, når $\mathfrak{p}$ er et opløst primideal (jvf. øvelsen efter sætning 60).

Et helt ideal

$$\mathfrak{A} = \prod \mathfrak{p}^{n_\mathfrak{p}}$$

opfylder derfor $\mathfrak{A} = \mathfrak{A}'$, hvis og kun hvis $n_\mathfrak{p} = n_{\mathfrak{p}'}$ for alle oplyste primidealer. Hvis $\mathfrak{A}$ også skal være primitiv resterer kun de angivne muligheder. □

Sætning 104. (Specialtilfælde af "Hilbert 90").
Antag, at $\alpha \in k = \mathbb{Q}(\sqrt{d})$ har $N(\alpha) = \alpha\alpha' = 1$.
Da kan α skrives på formen

$$\alpha = \frac{\rho}{\rho'}, \qquad \rho \in k^*,$$

og ρ er bestemt på nær en faktor i $\mathbb{Q}^*$.

Bevis: Eksistens. Hvis $\alpha = -1$ er $\rho = \sqrt{d}$ brugbar.
Hvis $\alpha \neq -1$ er $\rho = 1+\alpha$ brugbar, idet

$$\frac{\rho}{\rho'} = \frac{1+\alpha}{1+\alpha'} = \frac{\alpha\alpha'+\alpha}{1+\alpha'} = \alpha.$$

Entydighed. Hvis $\rho/\rho' = \sigma/\sigma'$ er
$\rho/\sigma = \rho'/\sigma' = (\rho/\sigma)'$, dvs $\rho/\sigma \in \mathbb{Q}^*$. □

Sætning 105. Lad $k = \mathbb{Q}(\sqrt{d})$. Da gælder (med betegnelserne i sætning 102):

(i) En egentlig idealklasse C er ambisk $\Leftrightarrow$ $C^2 = 1$ (= etelementet i H^+).

(ii) Der findes præcis 2^g ambiske egentlige idealklasser, idet hver ambisk egentlig idealklasse indeholder præcis to ambiske idealer.

(i) Det bemærkes først, at enhver egentlig idealklasse C indeholder et helt ideal; thi er $\mathfrak{b} \in C$ og $b \in \mathbb{N}$ en fællesnævner for $\mathfrak{b}$ er $(b)\mathfrak{b} \sim \mathfrak{b}$ et helt ideal i C. Lad nu C være en vilkårlig egentlig idealklasse og $\mathfrak{A}$ et helt ideal heri. Da følger, at

$$\mathfrak{A}\mathfrak{A}' = (N(\mathfrak{A})) \sim (1),$$

hvoraf $CC' = 1$. Dette viser påstanden i (i).

(ii) Ifølge sætning 103 skal vi vise:

(a) Ethvert ambish ideal tilhører en ambish egentlig idealklasse.

(b) Enhver ambish egentlig idealklasse indeholder præcis to ambishe idealer.

Lad $\mathfrak{A} = \mathfrak{A}' \in C$. Da er $\mathfrak{A}' = \mathfrak{A} \in C'$, og følgelig er $C \cap C' \neq \emptyset$, altså $C = C'$. Dette viser (a).

Lad dernæst $\mathfrak{A} \in C = C'$ være et helt ideal i en given ambish egentlig idealklasse C. Da er også $\mathfrak{A}' \in C$, altså $\mathfrak{A}\mathfrak{A}'^{-1} \sim (1)$, dvs. $\mathfrak{A}\mathfrak{A}'^{-1} = (\alpha)$, hvor $N(\alpha) > 0$. Da tillige $|N(\alpha)| = N(\mathfrak{A})/N(\mathfrak{A}') = 1$, er $N(\alpha) = 1$. Ifølge sætning 104 er $\alpha = \frac{\rho}{\rho'}$, hvor $\rho \in k^*$, men hvor vi om fornødent ved forlængelse kan opnå, at $\rho \in \mathcal{O}_k \setminus \{0\}$. Idealet $\mathfrak{A}(\rho') = \mathfrak{A}'(\rho) = \mathfrak{d}$ er derfor helt og $\mathfrak{b} = \mathfrak{b}'$. C vil derfor

indeholde $\mathfrak{C}$ eller $\mathfrak{C}\cdot(\sqrt{d})$ afhængigt af om $N(\mathfrak{p}')>0$ eller $N(\mathfrak{p}')<0$. Ved at forkorte det relevante af disse idealer med et passende (n), $n\in\mathbb{N}$, findes et ambisk ideal i $\mathfrak{C}$.

På grund gruppestrukturen vil vi derfor have vist (b), hvis vi kan godtgøre:

(b_1) Den egentlige idealklasse $\mathfrak{D}_1^+$ (etalematet i H^+) indholder præcis to ambiske idealer.

Lad $\mathfrak{A}$ være et ambisk ideal i $\mathfrak{D}_1^+$. Da er $\mathfrak{A}=(\alpha)=(\alpha')$ og $N(\alpha)=N(\alpha')(>0)$. Følgelig er

$$(*)\qquad \frac{\alpha}{\alpha'}=\varepsilon\in O_k^* \quad\text{og}\quad N(\varepsilon)=+1.$$

Vi må nu skelne mellem de tre typer af k.

<u>Type I.</u> Hvis $-d>4$ er $|O_k^*|=2$ og $\frac{\alpha}{\alpha'}=\pm 1$, dvs. $\alpha=\alpha'$ eller $\alpha=-\alpha'$. Vi har da enten $\alpha\in\mathbb{Q}^*$, altså $(\alpha)=(1)$, eller $\alpha\in\mathbb{Q}^*\sqrt{d}$, altså $(\alpha)=\mathfrak{p}_t\cdots\mathfrak{p}_g=(\sqrt{d^*})$, hvor $d^*=\begin{cases} d & ,\ d\text{ulige} \\ \frac{1}{4}d & ,\ d\text{lige}\end{cases}$ og $t=\begin{cases}1 & ,\ \frac{d}{4}\text{ulige}\\ 0 & ,\ \text{ellers}\end{cases}$.

For $d=-3,-4$ er $h^+=h=1$. I begge tilfælde er $g=0$, dvs. der findes præcis to ambiske idealer, nemlig (1), $\left(\frac{3+\sqrt{-3}}{2}\right)$ og (1), $(1+i)$. I alle tilfælde ligger de fundne ambiske idealer i $\mathfrak{D}_1^+=\mathfrak{D}_1$.

Type II. Da $\varepsilon = \pm \varepsilon_1^n$, $\varepsilon_1 > 1$, ε_1 fundamentalenhed med $N(\varepsilon_1) = -1$ og $N(\varepsilon) = +1$, er n lige, dvs. $\varepsilon = \pm \varepsilon_0^2$, hvor $\varepsilon_0 \in O_k^*$. I følge (*) er derfor

$$\frac{\alpha}{\alpha'} = \pm \varepsilon_0^2 = \pm N(\varepsilon_0) \frac{\varepsilon_0}{\varepsilon_0'}.$$

Af entydighedsdelen af sætning 104 fås nu:

hvis $\pm N(\varepsilon_0) = +1$ er $\frac{\alpha}{\varepsilon_0} \in \mathbb{Q}^* \Rightarrow (\alpha) = (1)$;

hvis $\pm N(\varepsilon_0) = -1$ er $\frac{\alpha}{\sqrt{d}\,\varepsilon_0} \in \mathbb{Q}^* \Rightarrow$

$(\alpha) = \mathfrak{p}_t \cdots \mathfrak{p}_g = (\sqrt{d^*})$, hvor d^* og t er som i type I.
De fundne ambigue idealer ligger i $\mathfrak{D}_1^+ = \mathfrak{D}_1$.

Type III. Her er $\varepsilon = \pm \varepsilon_1^n$, $\varepsilon_1 > 1$, ε_1 fundamentalenhed med $N(\varepsilon_1) = +1$, og alle $n \in \mathbb{Z}$ er derfor mulige. I følge sætning 104 har vi

$$(**) \qquad \varepsilon_1 = \frac{\rho}{\rho'}, \quad \rho = 1 + \varepsilon_1 \in O_k \setminus \{0\},$$

og vi har derfor

$$\frac{\alpha}{\alpha'} = \varepsilon = \begin{cases} \dfrac{\rho^n}{(\rho^n)'}, & \text{hvis } \varepsilon = +\varepsilon_1^n \\ \dfrac{(\sqrt{d}\,\rho^n)}{(\sqrt{d}\,\rho^n)'}, & \text{hvis } \varepsilon = -\varepsilon_1^n. \end{cases}$$

I følge sætning 104 er følgelig

$$(***) \qquad \frac{\alpha}{\rho^n} \in \mathbb{Q}^* \text{ eller } \frac{\alpha}{\sqrt{d}\,\rho^n} \in \mathbb{Q}^*, \quad n \in \mathbb{Z}.$$

Det følger af (**), at $(\rho) = (\rho') = (\rho)'$, og at (ρ) er et

helt ideal ($\neq (0)$). Sæt $\lambda = \rho/q$, hvor q er det største naturlige tal, for hvilket $q \mid \rho$. Da er

$$(\lambda) = (\rho/q) = \mathfrak{p}_0^{n_0} \cdots \mathfrak{p}_g^{n_g}, \quad n_0, \ldots, n_g \in \{0,1\}$$

et ambisk hovedideal. Bemærk, at λ og dermed $n_0, \ldots, n_g$ er entydigt bestemt ved k.

Vi vil vise, at $(\lambda) \neq (1)$ og $(\lambda) \neq (\sqrt{d^*})$. Hvis nemlig $(\lambda) = (1)$ eller $(\lambda) = (\sqrt{d^*})$, da er $\rho = \tilde{\varepsilon} q$ eller $\rho = \tilde{\varepsilon} q \sqrt{d^*}$, hvor $\tilde{\varepsilon} \in O_k^*$, og følgelig er

$$\varepsilon_1 = \frac{\rho}{\rho'} = \pm \frac{\tilde{\varepsilon}}{\tilde{\varepsilon}'} = \pm \frac{\tilde{\varepsilon}^2}{N(\tilde{\varepsilon})} = \pm \tilde{\varepsilon}^2,$$

i strid med at ε_1 er en fundamentalenhed.

Da $(\rho)^2 = (\rho)(\rho') = (N(\rho))$ fremgår af (***), at der højst er følgende ambiske idealer i $\mathfrak{D}_1^+$:

$$(1), \quad (\lambda), \quad (\sqrt{d^*}), \quad (\delta\sqrt{d^*}/\lambda),$$

hvor $\delta = 1, 2$ ($\delta = 2$ hvis $t = 1$ og $n_0 = 1$).

Da $(\sqrt{d^*}) \notin \mathfrak{D}_1^+$, er der præcis to ambiske idealer i $\mathfrak{D}_1^+$, nemlig

(1), (λ), når $N(\rho) > 0$,

(1), $(\delta\sqrt{d^*}/\lambda)$, når $N(\rho) < 0$. □

Bevis for sætning 102: Da H_2^+ ifølge sætning 105 (i) præcis består af de ambiske egentlige idealklasser, og antallet af disse ifølge sætning 105 (ii) er 2^g, er H^+/H^{+2}

$\cong H^+_2 \cong C_2^g$ ifølge sætning 100. Endelig er

$$H^+/H^{gen} = \mathcal{D}/\mathcal{D}_1^+/\mathcal{D}/\mathcal{D}_1^{gen} \cong \mathcal{D}_1^{gen}/\mathcal{D}_1^+ = H^{+2}.$$

Da $H^+/H^{+2} \cong C_2^g$ er det klart, at $2^g \mid h^+$.

Endelig fremgår af sætning 100, at $h^+ = |H^+|$ er ulige

$\iff |H_2^+| = 1 \iff g = 0$. □

Eksempel 44. $k = \mathbb{Q}(\sqrt{-5})$. Her er $d = -20 = -4 \cdot 5$, altså $g = 1$. Følgelig er $H^{gen} \cong C_2$. Da k er af type I er $h = h_+$ altså delelig med 2. Vi fandt i eksempel 29, at $h = 2$, idet klasserne er repræsenteret ved (1) og $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$. I dette tilfælde er $\mathcal{D}_1 = \mathcal{D}_1^+ = \mathcal{D}_1^{gen}$ mængden af alle hovedidealer. Der er to ambishe hovedidealer, nemlig (1) og $(\sqrt{-5})$. Samtlige ambishe idealer er

$$(1),\ \mathfrak{p}_2,\ (\sqrt{-5}),\ \mathfrak{p}_2(\sqrt{-5}).$$

Eksempel 45. $k = \mathbb{Q}(\sqrt{10})$. Her er $d = 40 = 8 \cdot 5$, altså $(\varepsilon_1 = 3+\sqrt{10})$ $g = 1$. Følgelig er $H^{gen} \cong C_2$. Da k er af type II er $h = h^+$ altså delelig med 2. De eneste primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{d} = \sqrt{40} < 7$ er divisorerne i 2, 3, 5. Da 2 og 5 går op i $d = 40$ er (2) og (5) forgrenede. Ifl. sætn. 60 (øvelse) er

$$(2) = \mathfrak{p}_2^2,\ \mathfrak{p}_2 = (2, \sqrt{10}),\quad N(\mathfrak{p}_2) = 2,$$
$$(5) = \mathfrak{p}_5^2,\ \mathfrak{p}_5 = (5, \sqrt{10}),\quad N(\mathfrak{p}_5) = 5.$$

Da $\left(\frac{40}{3}\right) = \left(\frac{1}{3}\right) = 1$, er $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, $\mathfrak{p}_3 = (3, 1+\sqrt{10})$, $\mathfrak{p}_3' = (3, 1-\sqrt{10})$ hvor $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$.

Idealklassene i $H = H^+$ er derfor representert ved

$$\{(1),\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \mathfrak{p}_3',\ \mathfrak{p}_5,\ \mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_2\mathfrak{p}_3'\}.$$

Da

$$\mathfrak{p}_2\mathfrak{p}_5 = (2, \sqrt{10})(5, \sqrt{10}) = (2\sqrt{10}, 5\sqrt{10}, 10) = (\sqrt{10}) \sim (1),$$

$$\mathfrak{p}_2\mathfrak{p}_3 = (2, \sqrt{10})(3, 1+\sqrt{10}) = (6, 3\sqrt{10}, 2+2\sqrt{10}, 10+10\sqrt{10})$$

$$= (4+\sqrt{10}) \sim (1),$$

er

$$\mathfrak{p}_3 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2,\ \mathfrak{p}_3' \sim \mathfrak{p}_3^{-1} \sim \mathfrak{p}_2,\ \mathfrak{p}_5 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2,$$

og idealklassene er følgelig representert ved $\{(1), \mathfrak{p}_2\}$.
Da $2 \mid h = h^+$, er derfor $h = h^+ = 2$. Igen er
$D_1 = D_1^+ = D_1^{\text{gen}}$. De to ambiske hovedidealer er (1) og $(\sqrt{10})$.
Samtlige ambiske idealer er

$$(1),\ \mathfrak{p}_2,\ \mathfrak{p}_5,\ (\sqrt{10}) = \mathfrak{p}_2\mathfrak{p}_5.$$

<u>Eksempel 46.</u> $k = \mathbb{Q}(\sqrt{79})$. Her er $d = (-4)(-79)$, altså $g = 1$. Følgelig er $H^{\text{gen}} \cong C_2$. Da k har fundamentalenheden $\varepsilon_1 = 80 + 9\sqrt{79}$ (idet $\sqrt{79} = [8, \overline{1, 7, 1, 16}]$) og $N(\varepsilon_1) = +1$, er k af type <u>III</u>, og vi har altså $h^+ = 2h$. Vi finder $\mathfrak{g} = 1 + \varepsilon_1 = 81 + 9\sqrt{79} = 9\lambda$, $\lambda = 9 + \sqrt{79}$, og (λ) er derfor et ambisk ideal og $N(\lambda) = 2$. Samtlige ambiske idealer er derfor hovedidealer:

$$(1),\ \mathfrak{p}_2 = (\lambda) = (9+\sqrt{79}),\ (\sqrt{d^*}) = (\sqrt{79}) = \mathfrak{p}_{79},$$

$$\mathfrak{p}_2\mathfrak{p}_{79} = (79 + 9\sqrt{79}).$$

Af disse er (1) og (λ) i $\mathfrak{D}_1^+$. Vi søger primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{d} = 2\sqrt{79} < 18$, og $\mathfrak{p}$ må derfor være divisor i 2, 3, 5, 7, 11, 13, 17. Her er

$$\left(\frac{d}{2}\right) = 0, \quad (2) = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (\lambda) = (9+\sqrt{79}) \sim (1);$$

$$\left(\frac{d}{3}\right) = \left(\frac{4}{3}\right)\left(\frac{79}{3}\right) = \left(\frac{1}{3}\right) = 1, \quad (3) = \mathfrak{p}_3\mathfrak{p}_3', \quad \mathfrak{p}_3 = (3, 1+\sqrt{79}),$$

$$\mathfrak{p}_3' = (3, 1-\sqrt{79});$$

$$\left(\frac{d}{5}\right) = \left(\frac{4}{5}\right)\left(\frac{79}{5}\right) = \left(\frac{4}{5}\right) = 1, \quad (5) = \mathfrak{p}_5\mathfrak{p}_5', \quad \mathfrak{p}_5 = (5, 2+\sqrt{79}),$$

$$\mathfrak{p}_5' = (5, 2-\sqrt{79});$$

$$\left(\frac{d}{7}\right) = \left(\frac{4}{7}\right)\left(\frac{79}{7}\right) = \left(\frac{9}{7}\right) = 1, \quad (7) = \mathfrak{p}_7\mathfrak{p}_7', \quad \mathfrak{p}_7 = (7, 3+\sqrt{79}),$$

$$\mathfrak{p}_7' = (7, 3-\sqrt{79});$$

$$\left(\frac{d}{11}\right) = \left(\frac{4}{11}\right)\left(\frac{79}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1, \quad (11) \text{ treg}, \quad N((11)) > \sqrt{d};$$

$$\left(\frac{d}{13}\right) = \left(\frac{4}{13}\right)\left(\frac{79}{13}\right) = \left(\frac{1}{13}\right) = 1, \quad 13 = \mathfrak{p}_{13}\mathfrak{p}_{13}', \quad \mathfrak{p}_{13} = (13, 1+\sqrt{79}),$$

$$\mathfrak{p}_{13}' = (13, 1-\sqrt{79});$$

$$\left(\frac{d}{17}\right) = \left(\frac{4}{17}\right)\left(\frac{79}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = -1, \quad (17) \text{ treg}, \quad N((17)) > \sqrt{d}.$$

Idealklasserne i H er derfor repræsenteret ved

$$\{(1), \mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_5, \mathfrak{p}_5', \mathfrak{p}_7, \mathfrak{p}_7', \mathfrak{p}_{13}, \mathfrak{p}_{13}', \mathfrak{p}_3\mathfrak{p}_5, \mathfrak{p}_3\mathfrak{p}_5', \mathfrak{p}_3'\mathfrak{p}_5, \mathfrak{p}_3'\mathfrak{p}_5', \mathfrak{p}_3^2, \mathfrak{p}_3'^2\}.$$

Da

$\mathfrak{p}_3\mathfrak{p}_5 = (3, 1+\sqrt{79})(5, 2+\sqrt{79}) = (8-\sqrt{79})$, $\mathfrak{p}_3'\mathfrak{p}_5' = (8+\sqrt{79})$,

$\mathfrak{p}_3\mathfrak{p}_7 = (3, 1+\sqrt{79})(7, 3+\sqrt{79}) = (10+\sqrt{79})$, $\mathfrak{p}_3'\mathfrak{p}_7' = (10-\sqrt{79})$,

$\mathfrak{p}_5\mathfrak{p}_{13}' = (5, 2+\sqrt{79})(13, 1-\sqrt{79}) = (12+\sqrt{79})$, $\mathfrak{p}_5'\mathfrak{p}_{13} = (12-\sqrt{79})$,

følger derfor, at idealklasserne i H er repræsenteret ved

$$\{(1), \mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_3^2, \mathfrak{p}_3'^2\}.$$

Endelig bemærkes, at hovedidealerne $(5-\sqrt{79})$ og $(5+\sqrt{79})$ er konjugerede og har norm $54 = 2\cdot 3^3$. Det ene ideal er derfor $\mathfrak{p}_2\mathfrak{p}_3^3$ og det andet $\mathfrak{p}_2\mathfrak{p}_3'^2$. Da $\mathfrak{p}_2 \sim (1)$ følger at $\mathfrak{p}_3^3 \sim \mathfrak{p}_3'^3 \sim (1)$, og derfor at $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1} \sim \mathfrak{p}_3^2$.

Idealklasserne i H er altså repræsenteret ved

$$\{(1), \mathfrak{p}_3, \mathfrak{p}_3^2\}.$$

$\mathfrak{p}_3$ er imidlertid ikke nogen hovedideal; thi $\mathfrak{p}_3 = (a+b\sqrt{79})$

$\Rightarrow N(\mathfrak{p}_3) = 3 = \pm N(a+b\sqrt{79})$, dvs. ligningen

$$(*) \qquad x^2 - 79y^2 = \pm 3,$$

vil have en heltalsløsning $(x, y) = (a, b)$. Lad (x_0, y_0) være en løsning i $\mathbb{N}^2$, hvor $x_0+\sqrt{79}\,y_0$ er mindst mulig. Da $N(80+9\sqrt{79}) = 1$ er

$$(x_1, y_1) = (80x_0 - 9\cdot 79\, y_0, -9x_0 + 80y_0)$$

givet ved

$$x_1 + y_1\sqrt{79} = \frac{x_0 + y_0\sqrt{79}}{80 + 9\sqrt{79}}$$

ligeledes en løsning til $(*)$, og $|x_1 + y_1\sqrt{79}| < |x_0 + y_0\sqrt{79}|$.

Følgelig er enten

$$80x_0 - 9\cdot 79 y_0 < 0 \quad \text{eller} \quad -9x_0 + 80y_0 < 0,$$

dvs.

$$\text{enten} \quad \frac{x_0}{y_0} < \frac{9\cdot 79}{80} = 8,8875$$

$$\text{eller} \quad \frac{x_0}{y_0} > \frac{80}{9} = 8,8888\ldots,$$

altså i begge tilfælde (idet $\sqrt{79} = 8.888819\ldots$)

$$(**) \qquad \left| \frac{x_0}{y_0} - \sqrt{79} \right| > 0.0006.$$

På den anden side følger af (*), at

$$\left| \frac{x_0}{y_0} - \sqrt{79} \right| = \frac{3}{y_0^2 \left(\frac{x_0}{y_0} + \sqrt{79} \right)} < \frac{3}{\sqrt{79}\, y_0^2}.$$

Dette sammenlignet med (**) giver

$$0.0006 < \frac{3}{\sqrt{79}\, y_0^2}$$

eller

$$y_0 < \sqrt{\frac{3}{0.0006 \cdot \sqrt{79}}} < 24.$$

Da (*) ingen løsninger har med $x_0 > 0$, $0 < y_0 < 24$, har vi dermed godtgjort at $y_3 \neq (1)$. Da $y_3^3 \sim (1)$ følger heraf at $y_3^2 \neq 1$, altså $h = 3$, og dermed $h_+ = 6$.

Idealklasserne i H^+ er repræsenteret ved

$$\{(1),\ \varepsilon_3,\ \varepsilon_3^2,\ (\sqrt{79}),\ (\sqrt{79})\varepsilon_3,\ \sqrt{79}\,\varepsilon_3^2\}.$$

Der gælder derfor $H \cong C_3$, $H^+ \cong C_6$. Da

$$\{\varepsilon_3^3;\ \varepsilon_3'^3\} = \left\{\left(\frac{5-\sqrt{79}}{9-\sqrt{79}}\right), \left(\frac{5+\sqrt{79}}{9+\sqrt{79}}\right)\right\}$$

$$= \{(-17-2\sqrt{79}),\ (-17+2\sqrt{79})\},$$

og

$$N(-17-2\sqrt{79}) = N(-17+2\sqrt{79}) = -27,$$

er

$$\varepsilon_3^3 \neq (1), \quad \varepsilon_3'^3 \neq (1).$$

En fænkninger for H^+ er derfor ε_3 eller $(\sqrt{79})\varepsilon_3^2$. Endelig fremgår, at de 6 klasser i H^+ fordeler sig således på genusklasser:

$$\mathfrak{D}_1^{gen} \supset \{(1),\ \varepsilon_3^2,\ (\sqrt{79})\varepsilon_3\},$$

$$\{\varepsilon_3,\ (\sqrt{79}),\ (\sqrt{79})\varepsilon_3^2\}.$$

—

<u>Sætning 106.</u> Lad $k = \mathbb{Q}(\sqrt{d})$, hvor $d = d_0 d_1 \cdots d_g$, som i sætning 101. Lad χ_j være den primitive kvadratiske karakter mod $|d_j|$ hørende til det kvadratiske talleg. me $\mathbb{Q}(\sqrt{d_j})$. Da gælder

(i) Enhver egentlig idealklasse C indeholder et helt ideal $\mathfrak{A}$ med $\gcd(N(\mathfrak{A}), d) = 1$.

(ii) Sættet

$$\left(\chi_j(N(\mathfrak{A})) \mid j = 0, \cdots, g \right) \in (\pm 1)^{g+1},$$

hvor $\mathfrak{A}$ er et vilkårlig helt ideal i C med $\gcd(N(\mathfrak{A}), d) = 1$, afhænger kun af C. Vi skriver herefter $\chi_j(C) = \chi_j(\mathfrak{A})$.

(iii) $\forall C : \prod_{j=0}^{g} \chi_j(C) = 1.$

(iv) For $C \approx \bar{C}$ (dvs. $C\bar{C}^{-1} \in \mathfrak{D}_1^{gen}$) gælder

$$\chi_j(C) = \chi_j(\bar{C}) \text{ for } 0 \leq j \leq g.$$

(v) For enhver fortegnskombination $(\delta_0, \cdots, \delta_g) \in \{\pm 1\}^{g+1}$ med $\delta_0 \cdots \delta_g = 1$ findes en egentlig idealklasse C med $\chi_j(C) = \delta_j$ for $0 \leq j \leq g$. For $C \not\approx \bar{C}$ er $\chi_j(C) \neq \chi_j(\bar{C})$ for mindst et $j = 0, \cdots, g$.

Bemærkning. Karaktererne χ_j, $0 \leq j \leq g$, kaldes genus karaktererne for $k = \mathbb{Q}(\sqrt{d})$, idet disse ifølge (iv), (v) præcis er i stand til at skelne mellem genusklasserne.

Bevis: (i) Ifølge sætning 38, korollar 3, findes et helt ideal $\mathfrak{A}$ med $\mathfrak{A} + (d) = (1)$ og $\mathfrak{A} \in \tilde{C}$, hvor $\tilde{C}$ er idealklassen indeholdende C. Såfremt k er af type I, II er $\tilde{C} = C$, og $\mathfrak{A}$ er derfor et brugbart ideal. Er k af type III, består $\tilde{C}$ foruden af C af endnu en egentlig idealklasse. Imidlertid er $N(1+\sqrt{d}) = 1 - d < 0$ i dette tilfælde og $N(1+\sqrt{d})$ er primisk med d. Følgelig vil enten $\mathfrak{A}$ eller $\mathfrak{A}(1+\sqrt{d})$ være brugbart.

(ii) Vi viser først: For ethvert helt ideal $\mathfrak{A}$ med $\gcd(N(\mathfrak{A}), d) = 1$ gælder

$$(*) \qquad \prod_{j=0}^{g} \chi_j(N(\mathfrak{A})) = +1.$$

Lad

$$\mathfrak{A} = \mathfrak{P}_1 \cdots \mathfrak{P}_s$$

være primidealopløsningen af $\mathfrak{A}$.

$$N(\mathfrak{P}_i) = q_i^{f_i}, \qquad 1 \leq i \leq s,$$

hvor

$$f_i = \begin{cases} 1, & \text{hvis } \left(\frac{d}{q_i}\right) = 1 \\ 2, & \text{hvis } \left(\frac{d}{q_i}\right) = -1 \end{cases}.$$

Da $\chi = \chi_0 \cdots \chi_g$ er den primitive kvadratiske karakter hørende til $\mathbb{Q}(\sqrt{d})$ gælder ifølge sætning 98, $\left(\frac{d}{q_i}\right) = \chi(q_i)$. Vi finder derfor

$$\prod_{j=0}^{g} \chi_j(N(\mathfrak{A})) = \chi(N(\mathfrak{A})) = \prod_{i=1}^{s} \chi(N(\mathfrak{P}_i))$$

$$= \prod_{i=1}^{s} \chi(q_i^{f_i}) = \prod_{i=1}^{s} \chi(q_i)^{f_i}$$

$$= \prod_{i=1}^{s} \left(\frac{d}{q_i}\right)^{f_i} = 1.$$

Vi viser dernæst: For ethvert $\alpha \in \mathcal{O}_k$ med $N(\alpha) > 0$ og $\gcd(N(\alpha), d) = 1$ gælder

$$(**) \qquad \chi_j(N((\alpha))) = +1 \quad \text{for} \quad 0 \leq j \leq g.$$

På grund af (*) er det tilstrækkeligt at vise for $1 \leq j \leq g$. For disse j er $d_j = (-1)^{\frac{p_j-1}{2}} p_j$ ulige og $\chi_j(x) = \left(\frac{x}{p_j}\right)$. Da $\alpha = \frac{1}{2}(a + b\sqrt{d^*})$, $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$, og $N(\alpha) > 0$ finder vi

$$\chi_j(N((\alpha))) = \chi_j(N(\alpha)) = \left(\frac{\frac{1}{4}(a^2 - b^2 d^*)}{p_j}\right)$$

$$= \left(\frac{a^2 - b^2 d^*}{p_j}\right) = \left(\frac{a^2}{p_j}\right) = +1.$$

Lad nu $\mathfrak{A}_1, \mathfrak{A}_2$ være hele idealer i samme egentlige idealklasse C, hvor $\gcd(N(\mathfrak{A}_1), d) = \gcd(N(\mathfrak{A}_2), d) = 1$. Da er

$$\mathfrak{A}_1 \mathfrak{A}_2^{-1} = \left(\frac{\alpha_2}{\alpha_1}\right),$$

hvor $\alpha_1, \alpha_2 \in \mathcal{O}_k$ med $N(\alpha_2/\alpha_1) > 0$ yderligere kan vælges så

$$\gcd(N(\alpha_1), d) = \gcd(N(\alpha_2), d) = 1$$

og

$$N(\alpha_1) > 0, \quad N(\alpha_2) > 0.$$

Vi finder nu ved hjælp af (**)

$$\chi_j(N(\mathfrak{O}_1)) = \chi_j(N(\mathfrak{O}_1(\alpha_1))) = \chi_j(N(\mathfrak{O}_2(\alpha_2))) = \chi_j(N(\mathfrak{O}_2))$$

(iii) Dette følger nu umiddelbart af (*).

(iv) Dette følger af (**), og den omstændighed, at der for ethvert helt ideal $\mathfrak{M}$ med $\gcd(N(\mathfrak{M}), d) = 1$, gælder

$$\chi_j(N(\mathfrak{M}^2)) = \chi_j(N(\mathfrak{M})^2) = \chi_j(N(\mathfrak{M}))^2 = +1.$$

(v) Vi vil benytte Dirichlet's sætning om at enhver primisk restklasse indeholder uendelig mange primtal. For hvert j vælges $a_j \bmod |d_j|$, så $\chi_j(a_j) = \delta_j$, hvilket er muligt da χ_j antager begge værdier ± 1. Da $d_0, d_1, \dots, d_g$ er parvis indbyrdes primiske, findes en restklasse $a \bmod |d|$ (og kun én), så $a \equiv a_j \pmod{|d_j|}$ for $0 \le j \le g$. Da hvert a_j er primisk $\bmod |d_j|$, er a også primisk $\bmod |d|$. Følgelig findes et primtal $p \equiv a \pmod{|d|}$. For et sådant p gælder da

$$\chi_j(p) = \chi_j(a) = \chi_j(a_j) = \delta_j \quad \text{for} \quad 0 \le j \le g,$$

og følgelig er

$$\chi(p) = \prod_{j=0}^{g} \chi_j(p) = \prod_{j=0}^{g} \delta_j = +1.$$

p er derfor opløst, $p = \mathfrak{p}\mathfrak{p}'$, hvor $p = N(\mathfrak{p})$.

For klassen C indeholdende $\mathfrak{p}$ er nu

$$\chi_j(C) = \chi_j(N(\mathfrak{p})) = \chi_j(\mathfrak{p}) = \delta_j \quad , \quad 0 \leq j \leq g.$$

Afbildningen

$$C \mapsto (\chi_0(C), \dots, \chi_g(C))$$

er ifølge det viste en surjektiv afbildningen af de 2^g genusklasser på de 2^g fortegns kombinationer $(\delta_0, \dots, \delta_g) \in \{\pm 1\}^{g+1}$ med $\delta_0 \cdots \delta_g = 1$. Denne afbildning er derfor også injektiv. □

Definition. Et kvadratisk tallegeme $\mathbb{Q}(\sqrt{d})$, $d < 0$, kaldes idonisk (latin: idoneus = egnet, passende) såfremt $(H^+ =) H = H^{gen}$.

Bemærk: Det følger af definitionen på H^{gen}, at $\mathbb{Q}(\sqrt{d})$ er idonisk, hvis og kun hvis $\mathcal{O}^2 \sim (1)$ for ethvert helt ideal $\mathcal{O}$.

Eksempel 47. $\mathbb{Q}(\sqrt{-420})$ er et idonisk tallegeme. Vi søger alle primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{-d} = \sqrt{420} < 21$. Da

$$d = -420 = (-4)(-3)\,5\,(-7),$$

er

$$(2) = \mathfrak{p}_2^2, \quad (3) = \mathfrak{p}_3^2, \quad (5) = \mathfrak{p}_5^2, \quad (7) = \mathfrak{p}_7^2.$$

Endvidere er

$$(11) = \mathfrak{p}_{11} \cdot \mathfrak{p}_{11}', \text{ da } \left(\frac{-420}{11}\right) = \left(\frac{9}{11}\right) = +1,$$

$$(13) = \mathfrak{p}_{13} \cdot \mathfrak{p}_{13}', \text{ da } \left(\frac{-420}{13}\right) = \left(\frac{-4}{13}\right) = \left(\frac{-1}{13}\right) = +1,$$

$$(17) = \text{treg}, \text{ da } \left(\frac{-420}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

$$(19) = \mathfrak{p}_{19} \cdot \mathfrak{p}_{19}', \text{ da } \left(\frac{-420}{19}\right) = \left(\frac{-2}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right) = (-1)(-1) = +1.$$

Imidlertid er

$$N(x + y\sqrt{-105}) = x^2 + 105y^2,$$

og følgelig

$$N(4 \pm \sqrt{-105}) = 11^2, \quad N(8 \pm \sqrt{-105}) = 13^2, \quad N(16 \pm \sqrt{-105}) = 19^2.$$

Heraf sluttes, at

$$\{\mathfrak{p}_{11}^2, \mathfrak{p}_{11}'^2\} = \{(4 + \sqrt{-105}), (4 - \sqrt{-105})\},$$

$$\{\mathfrak{p}_{13}^2, \mathfrak{p}_{13}'^2\} = \{(8 + \sqrt{-105}), (8 - \sqrt{-105})\},$$

$$\{\mathfrak{p}_{19}^2, \mathfrak{p}_{19}'^2\} = \{(16 + \sqrt{-105}), (16 - \sqrt{-105})\}.$$

For samtlige primidealer $\mathfrak{p}$ med $N(\mathfrak{p}) < \sqrt{-d}$ gælder altså, at $\mathfrak{p}^2 \sim (1)$. Da enhver idealklasse C indeholder et helt ideal $\mathfrak{A}$ med $N(\mathfrak{A}) < \sqrt{-d}$, er $\mathfrak{A}$ produkt af primidealer $\mathfrak{p}$, som alle opfylder $\mathfrak{p}^2 \sim (1)$. Derfor er også $\mathfrak{A}^2 \sim (1)$, og dermed $C^2 = 1$. Dette viser, at $\mathbb{Q}(\sqrt{-420})$ er idonisk. Da der er 4 forskellige primdivisorer i $d = -420$, er

$$H = H^+ = H^{gen} \cong C_2^3.$$

Bemærkning. Man kender ialt 65 idoniske legemer $\mathbb{Q}(\sqrt{d})$, $d<0$, $d = d_0 \cdots d_g$, nemlig:

med $g=0$: $-d = 3, 4, 7, 8, 11, 19, 43, 67, 163$;

med $g=1$: $-d = 15, 20, 24, 35, 40, 51, 52, 88, 91,$
$115, 123, 148, 187, 232, 235, 267, 403, 427$;

med $g=2$: $-d = 84, 120, 132, 168, 195, 228, 280, 312,$
$340, 372, 408, 435, 483, 520, 532, 555,$
$595, 627, 708, 715, 760, 795, 1012, 1435$;

med $g=3$: $-d = 420, 660, 840, 1092, 1155, 1320, 1380,$
$1428, 1540, 1848, 1995, 3003, 3315$;

med $g=4$: $-d = 5460$.

Det er bevist (P. J. Weinberger, Acta Arithmetica XXII (1972-73), 117-124), at der højst er endnu et idonisk legeme; eksistensen af et sådant er dog yderst tvivlsom.

Bemærk, at $h(\mathbb{Q}(\sqrt{d})) = 1 \iff \mathbb{Q}(\sqrt{d})$ idonisk og $g=0$. For $g=0$ er det vist (jvf noten pp. 110-111), at ovenstående 9 legemer er samtlige idoniske.

Bemærk endvidere, at $h(\mathbb{Q}(\sqrt{d})) = 2 \iff \mathbb{Q}(\sqrt{d})$ idonisk og $g=1$. Også for $g=1$ er det vist (se A. Baker: Transcendental Number Theory (1975), pp. 52-54), at ovenstående 18 legemer er samtlige idoniske. Et tilsvarende resultat er ikke vist for $g \geq 2$.

Dirichletrækker.

Definition. En **Dirichletrække** er en række af formen

$$(*) \qquad \sum_{n=1}^{\infty} a_n n^{-s}, \qquad a_n \in \mathbb{C}, \quad s = \sigma + it,$$

hvor $n^{-s} = e^{-s \ln n}$.

De Dirichletrækker vi fortrinsvis vil interessere os for er:

$$\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$ hvor $\mathfrak{a}$ gennemløber alle hele idealer i et algebraisk tallegeme k,

og

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$ hvor χ er en Dirichletkarakter.

Sætning 107. Hvis Dirichletrækken $(*)$ er absolut konvergent for $s = s_0 = \sigma_0 + it_0$, da er den absolut konvergent i halvplanen $\sigma \geqq \sigma_0$.
Der findes et entydigt bestemt $\sigma_a \in \mathbb{R} \cup \{\pm\infty\}$, kaldet den **absolutte konvergensabscisse** med egenskaben, at Dirichletrækken $(*)$ er absolut konvergent for $\sigma > \sigma_a$ og ikke absolut konvergent for $\sigma < \sigma_a$ [modificeret, når $\sigma_a = \pm\infty$].

Bevis: For $s = \sigma + it$ med $\sigma \geqq \sigma_0$ gælder for $n \in \mathbb{N}$:

$$|a_n n^{-s}| = |a_n n^{-\sigma}| \leqq |a_n n^{-\sigma_0}| = |a_n n^{-s_0}|.$$

Den absolutte konvergens af (*) følger nu af Weierstrass' majorantkriterium. Definér

$$\sigma_a = \inf \left\{ \sigma \in \mathbb{R} \mid \sum_1^\infty |a_n| n^{-\sigma} < \infty \right\} \in \mathbb{R} \cup \{\pm\infty\}.$$

Det er klart, at σ_a har den postulerede egenskab og er det eneste tal i $\mathbb{R} \cup \{\pm\infty\}$ med egenskaben.

Sætning 108. Hvis Dirichletrækken (*) er konvergent for $s = s_0 = \sigma_0 + it_0$, da er den uniformt konvergent i enhver kompakt delmængde af halvplanen $\sigma > \sigma_0$. Der findes et entydigt bestemt $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$, kaldet konvergensabscissen med egenskaben, at Dirichletrækken (*) er konvergent for $\sigma > \sigma_c$ og divergent for $\sigma < \sigma_c$ [modificeret, når $\sigma_c = \pm\infty$]. Dirichletrækken (*) fremstiller en holomorf funktion i konvergenshalvplanen $\sigma > \sigma_c$.

Der gælder altid $\sigma_a - \sigma_c \leqq 1$ [$\sigma_a = \sigma_c$, hvis en af dem er $\pm\infty$].

Bevis: Sæt

$$b_n = a_n n^{-s_0}, \qquad B(x) = \sum_{n \leq x} b_n = \sum_{n \leq x} a_n n^{-s_0}$$

Da gælder summationsformlen (partiel summation):

$$\sum_{n=M+1}^{N} a_n n^{-s} = \sum_{n=M+1}^{N} b_n n^{-(s-s_0)}$$

$$= B(N) N^{-(s-s_0)} - B(M) M^{-(s-s_0)} + (s-s_0) \int_M^N B(x) x^{s_0-s-1} \, dx.$$

Formlen vises umiddelbart ved induktion efter $N (\geq M)$.

Da $B(x) \to \sum_1^\infty a_n n^{-s_0}$ for $x \to \infty$ er $B(x)$ begrænset:

$$(*) \qquad \exists\ B \in \mathbb{R}_+ \text{, så} \quad |B(x)| \leq B \text{ for } x \geq 1.$$

Dette giver

$$\left| \sum_{M+1}^{N} a_n n^{-s} \right| \leq B N^{-(\sigma-\sigma_0)} + B M^{-(\sigma-\sigma_0)} + |s-s_0| B \int_M^N x^{\sigma_0-\sigma-1}\, dx$$

$$\leq 2B M^{-(\sigma-\sigma_0)} + |s-s_0| B \frac{M^{\sigma_0-\sigma} - N^{\sigma_0-\sigma}}{\sigma-\sigma_0},$$

altså

$$(**) \qquad \left| \sum_{M+1}^{N} a_n n^{-s} \right| \leq 2B M^{-(\sigma-\sigma_0)} \left(1 + \tfrac{1}{2} \cdot \frac{|s-s_0|}{\sigma-\sigma_0}\right).$$

En given kompakt delmængde K af halvplanen $\sigma > \sigma_0$ er indeholdt i et rektangel

$$R = \left\{ s = \sigma + it \mid \sigma_0 < a \leq \sigma \leq b,\ c \leq t \leq d \right\}.$$

Det følger derfor af $(**)$, at

$$\left| \sum_{M+1}^{N} a_n n^{-s} \right| \leq C M^{-(a-\sigma_0)}, \qquad C \in \mathbb{C},$$

uniformt i $s \in R$ (og dermed i $K \subset R$).

Da $M^{-(a-\sigma_0)} \to 0$ for $M \to \infty$ konvergerer $(*)$ altså uniformt i enhver kompakt delmængde af halvplanen $\sigma > \sigma_0$.

Defineres

$$\sigma_c = \inf \left\{ \sigma \in \mathbb{R} \mid \sum_1^\infty a_n n^{-\sigma} \text{ konvergent} \right\} \in \mathbb{R} \cup \{\pm\infty\},$$

er det igen klart, at σ_c har den postulerede egenskab og er det eneste tal i $\mathbb{R} \cup \{\pm\infty\}$ med egenskaben.
Af første del af sætningen følger nu, at Dirichletrækken (*) konvergerer uniformt i enhver kompakt delmængde K af konvergenshalvplanen $\sigma > \sigma_c$. Da hvert led i Dirichletrækken er holomorf i $\mathbb{C}$ følger (af en velkendt sætning af Weierstrass), at Dirichletrækken i konvergenshalvplanen fremstiller en holomorf funktion.
For at vise den sidste påstand er det tilstrækkeligt at vise:

$$\sum_1^\infty a_n n^{-\sigma_0} \text{ konvgt.} \Rightarrow \sum_1^\infty a_n n^{-\sigma} \text{ abs. konvgt.}$$

for ethvert σ med $\sigma > \sigma_0 + 1$. Imidlertid er

$$|a_n n^{-\sigma}| \leqq |a_n n^{-\sigma_0}| \, n^{-(\sigma-\sigma_0)} \leqq B\, n^{-(\sigma-\sigma_0)},$$

hvor B er en konstant (jvf. (*)). Da $\sigma > \sigma_0 + 1$ er

$$\sum_1^\infty B\, n^{-(\sigma-\sigma_0)}$$

derfor en konvergent majorantrække for $\sum_1^\infty a_n n^{-\sigma}$. □

Korollar. Hvis Dirichletrækken (*) har begrænset afsnit men er divergent for $s = s_0$, er $\sigma_c = \sigma_0$.

Bevis: Det er givet, at der findes en konstant B, så ulighederne (*) ovenfor er opfyldt. Resultatet følger nu af sætning 108.

Eksempel 48. Dirichletrækken

$$\sum_1^\infty (-1)^{n-1} n^{-s}$$

har $\sigma_c = 1$, idet

$$\sum_1^\infty n^{-\sigma}$$

er konvergent for $\sigma > 1$ og divergent for $\sigma \leqq 1$.
Da Dirichletrækken har begrænsede spring men er divergent for $s = 0$ er $\sigma_c = 0$ ifølge sætning 108, korollar.
Dette eksempel viser derfor, at $\sigma_a - \sigma_c = 1$ kan forekomme.
Den ved Dirichletrækken fremstillede funktion

$$\eta_2(s) = \sum_1^\infty (-1)^{n-1} n^{-s}$$

er ifølge sætning 108 holomorf for $\sigma > 0$.

Eksempel 49. Dirichletrækken

$$\sum_1^\infty n^{-s}$$

har åbenbart $\sigma_a = \sigma_c = 1$, idet rækken er divergent for $s = 1$ og absolut konvergent for $\sigma > 1$. Den ved Dirichletrækken fremstillede funktion

$$\zeta(s) = \sum_1^\infty n^{-s}$$

er ifølge sætning 108 holomorf for $\sigma > 1$. Funktionen kaldes Riemann's ζ-funktion (B. Riemann: Über die Anzahl der Primzahlen unter einer gegebenen Grösse, Monatsberichte der Berliner Akademie, November 1859).

For $\sigma > 1$ gælder nu

$$(1 - 2^{-s+1})\,\zeta(s) = \sum_1^\infty n^{-s} - 2\sum_1^\infty (2n)^{-s}$$

$$= \sum_1^\infty (-1)^{n-1} n^{-s}$$

$$= \eta_2(s).$$

Man kan derfor udvide definitionen af ζ-funktionen ved at sætte

$$\zeta(s) = (1 - 2^{-s+1})^{-1}\,\eta_2(s).$$

Hermed bliver $\zeta(s)$ defineret og holomorf i halvplanen $\sigma > 0$, dog med undtagelse af nulpunkterne for funktionen $1 - 2^{-s+1}$.

Da

$$2^{-s+1} = 1 \iff (1-s)\ln 2 = 2n\pi i\,, \quad n \in \mathbb{Z}$$

$$\iff s = 1 + \frac{2n\pi i}{\ln 2}\,, \quad n \in \mathbb{Z}, \tag{*1}$$

må vi derfor i første omgang undtage disse punkter fra definitionsmængden for ζ-funktionen.

Vi betragter endvidere Dirichletrækken

$$\sum_1^\infty a_n n^{-s} \quad , \quad a_n = \begin{cases} 1 & n \equiv \pm 1 \ (3) \\ -2 & n \equiv 0 \ (3) \end{cases}$$

Da $\sum_{n \le x} a_n$ er begrænset er Dirichletrækken

konvergent for $\sigma > 0$ og følgelig er

$$\eta_3(s) = \sum_1^\infty a_n n^{-s}$$

holomorf i halvplanen $\sigma > 0$.

For $\sigma > 1$ gælder nu

$$(1 - 3^{-s+1}) \zeta(s) = \sum_1^\infty n^{-s} - 3 \sum_1^\infty (3n)^{-s}$$

$$= \sum_1^\infty a_n n^{-s}$$

$$= \eta_3(s)$$

Man kan derfor også udvide definitionen af $\zeta(s)$ ved

$$\zeta^*(s) = (1 - 3^{-s+1})^{-1} \eta_3(s).$$

Hermed bliver ζ-funktionen defineret og holomorf i halvplanen $\sigma > 0$, dog med undtagelse af nulpunkterne for funktionen $1 - 3^{-s+1}$, dvs. for

$$s = 1 + \frac{2m\pi i}{\ln 3} \quad , \quad m \in \mathbb{Z}.$$

(**)

Da

$$\zeta(s) - \zeta^*(s)$$

er holomorf i halvplanen $\sigma > 0$ påtrods-mængderne (*) og (**) og $\zeta(s) - \zeta^*(s)$ er ml i halvplanen $\sigma > 1$ følger af identitetssætningen for holomorfe funktioner, at $\zeta(s) = \zeta^*(s)$ for $\sigma > 0$ påtrods foreningsmængden af (*) og (**).

Vi påstår nu, at

$$\left\{ 1 + \frac{2n\pi i}{\ln 2} \mid n \in \mathbb{Z} \right\} \cap \left\{ 1 + \frac{2m\pi i}{\ln 3} \mid m \in \mathbb{Z} \right\} = \{1\}.$$

Thi antag

$$1 + \frac{2n\pi i}{\ln 2} = 1 + \frac{2m\pi i}{\ln 3}.$$

Da er

$$2\pi i \,(n \ln 3 - m \ln 2) = 0,$$

altså

$$3^n = 2^m.$$

På grund af den entydige primfaktorisering af $\mathbb{Z}^*$ er $n = m = 0$, og påstanden er bevist.

Heraf følger, at ζ-funktionen ved brug af den ene eller den anden udvidede bliver defineret og holomorf i halvplanen $\sigma > 0$ med den ene undtagelse $s = 1$.

I en udprikket omegn af punktet $s = 1$ gælder derfor

$$\zeta(s) = f_j(s)^{-1} \eta_j(s), \quad j = 2, 3,$$

hvor

$$f_j(s) = 1 - j^{-s+1}, \quad j = 2, 3.$$

Da

$$f_j'(s) = j^{-s+1} \ln j \neq 0 \quad \text{for alle } s \in \mathbb{C},$$

er Taylorudviklingen for $f_j(s)$ med udviklingspunkt $s = 1$:

$$f_j(s) = \ln j \cdot (s-1) + \cdots$$

Da

$$\eta_2(1) = 1 - \tfrac{1}{2} + \tfrac{1}{3} - \tfrac{1}{4} + \cdots = \ln 2$$

følger, at

$$\zeta(s) = f_2(s)^{-1} \eta_2(s)$$

har en pol af 1. orden med residuum 1 i punktet $s = 1$.

Anvendes formlen

$$\zeta(s) = f_3(s)^{-1} \eta_3(s)$$

kan vi derfor slutte, at

$$\eta_3(1) = 1 + \tfrac{1}{2} - \tfrac{2}{3} + \tfrac{1}{4} + \tfrac{1}{5} - \tfrac{2}{6} + \cdots = \ln 3.$$

Dette kan naturligvis også vises elementært (jvf. øvelserne side 171).

Sætning 109. Lad χ være en vilkårlig Dirichletkarakter modulo D. Da gælder for L-rækken

$$\sum_1^\infty \chi(n)\, n^{-s}$$

at

(i) $\sigma_c = \sigma_a = 1$, når $\chi = \chi_0$,

(ii) $\sigma_c = 0$, $\sigma_a = 1$, når $\chi \neq \chi_0$.

For den ved L-rækken fremstillede L-funktion

$$L(s,\chi) = \sum_1^\infty \chi(n)\, n^{-s}$$

er for $\chi = \chi_0$

(iii) $$L(s,\chi_0) = \zeta(s) \prod_{\substack{p \mid D \\ p \text{ primtal}}} (1 - p^{-s}) \quad \text{for } \sigma > 1.$$

Ved (iii) defineres $L(s,\chi_0)$ for $\sigma > 0$. $L(s,\chi_0)$ er holomorf for $\sigma > 0$ på nær i punktet $s = 0$, hvor $L(s,\chi_0)$ har en pol af første orden med residuum

(iv) $$\prod_{p \mid D} \left(1 - \frac{1}{p}\right) = \frac{\varphi(D)}{D},$$

hvor $\varphi(D)$ (Eulers φ-funktion) er antallet af primiske restklasser modulo D.

For $\chi \neq \chi_0$ er $L(s,\chi)$ holomorf for $\sigma > 0$.

Bevis: At L-rækken har $\sigma_a = 1$ for ethvert χ følger af, at

$$\sum_1^\infty \left| \chi(n)\, n^{-s} \right| = \sum_1^\infty \chi_0(n)\, n^{-\sigma} ,$$

hvor χ_0 er hovedkarakteren med samme modulus D som χ. Da $\chi_0(n) = 0, 1$ er den 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

$$\sum_1^\infty \frac{1}{nD+1} .$$

Heraf fremgår også, at $\sigma_c = 1$ for hovedkarakteren $\chi = \chi_0$. For $\chi \neq \chi_0$ er restriktionerne af χ og χ_0 til den primiske restklassegruppe G_D modulo D to forskellige gruppekarakterer på G_D. Af den første ortogonalitetsrelation for gruppekarakterer følger derfor, at

$$\sum_1^D \chi(n) = \sum_{\substack{1 \\ \gcd(n,D)=1}}^D \chi(n) = 0 .$$

På grund af χ's periodicitet med periode D er afsnitsfølgen for rækken

$$\sum_1^\infty \chi(n)$$

derfor begrænsit, medens rækken naturligvis er divergent. Af sætning 108, korollar, fås nu (med $s_0 = 0$) at $\sigma_c = 0$, når $\chi \neq \chi_0$. Heraf følger, at $L(s,\chi)$ er holomorf for $\sigma > 0$, når $\chi \neq \chi_0$.

For at vise (iii) udregner vi (for $\sigma > 1$)

$$\zeta(s) \prod_{p \mid D} (1 - p^{-s}) = \sum_{1}^{\infty} n^{-s} \sum_{\substack{p_1 \cdots p_r \mid D \\ r \geq 0}} (-1)^r (p_1 \cdots p_r)^{-s}$$

$$= \sum_{1}^{\infty} a_n n^{-s},$$

hvor

$$a_n = \begin{cases} 1, & \text{når } \gcd(D,n) = 1 \\ \sum_{r=0}^{q} (-1)^r \binom{q}{r} = 0, & \text{når } \gcd(D,n) \text{ har } q \text{ primdivisorer.} \end{cases}$$

Dette viser formel (iii). Ifølge eksempel 49 er $\zeta(s)$ holomorf for $\sigma > 0$ med undtagelse af $s = 0$, hvor der er en pol af første orden med residuum 1. Af formel (iii) følger derfor at $L(s,\chi_0)$ er holomorf for $\sigma > 0$ på nær i punktet $s = 0$, hvor $L(s,\chi_0)$ har en pol af første orden med det i (iv) anførte residuum. □

Bemærkning. En anden metode er at benytte, at

$$L(s,\chi) = D^{-s} \sum_{n=1}^{D} \chi(n) \zeta\left(s, \frac{n}{D}\right),$$

hvor

$$\zeta(s,a) = \sum_{n=1}^{\infty} (n+a)^{-s}, \quad 0 < a \leq 1,$$

er Hurwitz's ζ-funktion (A. Hurwitz: Eigenschaften Dirichlet'scher Funktionen ..., Z. für Math. u. Phys., Bd 27, 1882, S 86-101). Det kan nemlig vises, at $\zeta(s,a)$ for ethvert $a \in]0,1[$ kan udvides til halvplanen $\sigma > 0$ (umiddelbart er $\zeta(s,a)$ kun defineret for $\sigma > 1$), og bliver holomorf overalt på nær for $s = 1$, hvor der (uafhængigt af a) er en pol af første orden med residuum 1.

Sætning 110. Antag at funktionen $f : \mathbb{N} \to \mathbb{C}$ er fuldstændig multiplikativ ($f(n_1 n_2) = f(n_1) f(n_2)$, $n_1, n_2 \in \mathbb{N}$). Da gælder

$$\sum_{1}^{\infty} f(n) = \prod_{p \text{ primtal}} (1 - f(p))^{-1},$$

forudsat rækken er absolut konvergent.

Bevis: Da rækken er absolut konvergent og dermed konvergent vil nødvendig vis for ethvert $n > 1$:

$$f(n)^m = f(n^m) \to 0 \quad \text{for } m \to \infty.$$

Heraf følger, at $|f(n)| < 1$ for ethvert $n > 1$.
$f(1) = 1$ med mindre f er identisk 0.
Vi betragter et vilkårligt afsnit i produktet:

$$P(x) = \prod_{p \leq x} (1 - f(p))^{-1} = \prod_{p \leq x} \left(1 + f(p) + f(p)^2 + \cdots \right),$$

hvor konvergensen af de uendelige kvotientrækker er sikret af at $|f(p)| < 1$ for ethvert primtal p. Da de uendelige kvotientrækker er absolut konvergente er produktet af endelig mange af dem det også og vi finder derfor

$$P(x) = \sum_{n \in A(x)} f(n),$$

hvor

$$A(x) = \{ n \in \mathbb{N} \mid \text{alle primfaktorer i } n \text{ er} \leq x \}.$$

Følgelig er

$$\sum_1^\infty f(n) - \sum_{n \in A(x)} f(n) = \sum_{n \in A'(x)} f(n),$$

hvor $A'(x) = \mathbb{N} \setminus A(x)$. Altså er

$$\left| \sum_1^\infty f(n) - P(x) \right| \leq \sum_{n \in A'(x)} |f(n)| \leq \sum_{n > x} |f(n)|,$$

eftersom $A(x)$ med sikkerhed indeholder alle $n \leq x$.
Af den absolutte konvergens af $\sum_1^\infty f(n)$ følger derfor

$$P(x) \to \sum_1^\infty f(n) \quad \text{for} \quad x \to \infty. \qquad \square$$

<u>Korollar.</u> For enhver Dirichlet karakter χ er

$$L(s, \chi) = \sum_1^\infty \chi(n) n^{-s} = \prod_p \left(1 - \chi(p) p^{-s}\right)^{-1} \text{ for } \sigma > 1.$$

Denne produktfremstilling af $L(s,\chi)$ kaldes Euler-produktet.

Sætning 111. Lad k være et vilkårligt algebraisk tallegeme med $[k:\mathbb{Q}] = N$. Da gælder

$$\zeta_k(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1},$$

når $s = \sigma + it$ har $\sigma > \sigma_a$, hvor σ_a er den absolutte konvergensabscisse for rækken. Der gælder endvidere

$$\frac{1}{N} \leqq \sigma_c = \sigma_a \leqq 1.$$

Bevis: Sættes

$$a_n = \text{antal hele ideraler } \mathfrak{a} \in \mathfrak{o}_k \text{ med } N(\mathfrak{a}) = n$$

kan vi skrive

$$\zeta_k(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \sum_{1}^{\infty} a_n n^{-s}.$$

Da $a_n \geqq 0$ for alle $n \in \mathbb{N}$ og $n^{-\sigma} > 0$ for $\sigma \in \mathbb{R}$, er sidstnævnte række en Dirichletrække med $\sigma_a = \sigma_c$, idet σ_a og σ_c alene er bestemt ved konvergensforholdene på $\mathbb{R}$. $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ er derfor absolut konvergent for $\sigma > \sigma_a = \sigma_c$, men ikke absolut konvergent for $\sigma < \sigma_a = \sigma_c$, og altså divergent for $s = \sigma < \sigma_a = \sigma_c$.

Beviset for produktformlen er nu ganske som i sætning 110, dog med den forskel, at vi benytter, at O_k er en Dedekindring og at normen er fuldstændig multiplikativ. For $\sigma > \sigma_a$ er

$$\sum_{\mathfrak{a}} |N(\mathfrak{a})^{-s}| < \infty \Rightarrow \sum_{\mathfrak{p}} |N(\mathfrak{p})^{-s}| < \infty$$

Produktet er derfor ubetinget konvergent, og det er følgelig ikke nødvendigt at specificere nogen rækkefølge for primidealerne $\mathfrak{p}$ (hvad vi heller ikke har gjort).

For $s = \sigma > 0$ er produktet konvergent $\Leftrightarrow$

$$\ln \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-\sigma})^{-1} \in]0, \infty[\quad \Leftrightarrow$$

$$-\sum_{\mathfrak{p}} \ln (1 - N(\mathfrak{p})^{-\sigma}) < \infty \quad \Leftrightarrow$$

$$\sum_{\mathfrak{p}} N(\mathfrak{p})^{-\sigma} < \infty .$$

Imidlertid er

$$\sum_{\mathfrak{p}} N(\mathfrak{p})^{-\sigma} = \sum_{p} \sum_{\mathfrak{p} | (p)} p^{-f_{\mathfrak{p}} \sigma} ,$$

hvor

$$1 \leq f_{\mathfrak{p}} \leq N , \quad \text{antal } \mathfrak{p} | (p) \in [1, N].$$

og følgelig gælder ulighederne

$$(*) \qquad \sum_p p^{-N\sigma} < \sum_\gamma N(\gamma)^{-\sigma} < N \sum_p p^{-\sigma} .$$

Endelig gælder, at

$$\sum_p p^{-x}$$

er konvergent for $x > 1$ og divergent for $x = 1$ (og dermed for $x < 1$). Konvergensen følger ved sammenligning med $\sum_n n^{-x}$. Divergensen følger indirekte:

$$\sum_p p^{-1} < \infty \Rightarrow \prod_p (1 - p^{-1})^{-1} \text{ konvergent} \Rightarrow$$

$$\sum_n \frac{1}{n} < \infty \text{ , modstrid!}$$

Af (*) følger dertor, at $\sum_\gamma N(\gamma)^{-\sigma}$ er konvergent for $\sigma > 1$ og divergent for $\sigma = \frac{1}{N}$. Heraf følger ulighederne for $\sigma_a = \sigma_c$. □

<u>Sætning 112.</u> (Landau, 1905). Betragt en Dirichletrække

$$\sum_1^\infty a_n n^{-s} , \qquad a_n \geqq 0 \text{ for alle } n \in \mathbb{N}.$$

Antag, at $\sigma_a \, (= \sigma_c) \in \,]-\infty, \infty[$. Da har den ved rækken fremstillede funktion $f(s)$ et singulært punkt for $s = \sigma_a$ [dvs. f kan ikke

fortsættes analytisk (holomorft) til en omegn af punktet $s = \sigma_a$).

Bevis: Indirekte. Antag at

$$f(s) = \sum_1^\infty a_n n^{-s}$$

kan fortsættes analytisk i en cirkel $\{ s \mid |s - \sigma_a| < r \}$.

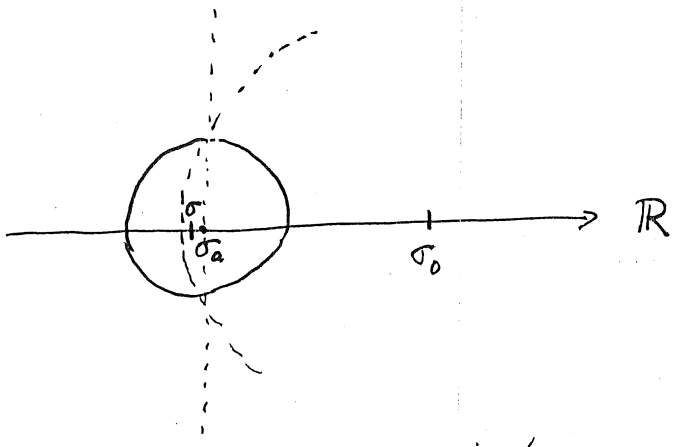
Vælg $\sigma_0 > \sigma_a$. Da gælder Taylorudviklingen

$$(*) \qquad f(s) = \sum_{\nu=0}^\infty \frac{f^{(\nu)}(\sigma_0)}{\nu!} (s - \sigma_0)^\nu ,$$

og hvor konvergensradius $\rho \geq \sqrt{(\sigma_0 - \sigma_a)^2 + r^2} > \sigma_0 - \sigma_a$.

Værdierne $f^{(\nu)}(\sigma_0)$ findes ved ledvis differentiation af Dirichletrækken for $f(s)$ (lovligt, da $\sigma_0 > \sigma_a$):

$$f^{(\nu)}(\sigma_0) = (-1)^\nu \sum_1^\infty a_n (\ln n)^\nu n^{-\sigma_0} .$$



Vælg nu $s = \sigma < \sigma_a$ men σ i konvergenscirklen for potensrækken (*). Da finder vi

$$f(\sigma) = \sum_{\nu=0}^\infty \left(\frac{(\sigma_0 - \sigma)^\nu}{\nu!} \sum_{n=1}^\infty a_n (\ln n)^\nu n^{-\sigma_0} \right).$$

Da denne dobbeltrække har lutter positive (≥ 0) led kan summationsrækkefølgen ombyttes:

$$f(\sigma) = \sum_{n=1}^{\infty} \left(a_n n^{-\sigma_0} \sum_{\nu=0}^{\infty} \frac{((\sigma_0 - \sigma) \ln n)^\nu}{\nu!} \right)$$

$$= \sum_{n=1}^{\infty} a_n n^{-\sigma_0} n^{\sigma_0 - \sigma}$$

$$= \sum_{n=1}^{\infty} a_n n^{-\sigma}.$$

Dirichletrækken er altså konvergent for $s = \sigma < \sigma_a = \sigma_c$, modstrid! □

Sætning 113. Lad $k = \mathbb{Q}(\sqrt{d})$ være et kvadratisk tallegeme med diskriminant d, og lad χ være den tilhørende primitive kvadratiske karakter (jvf. sætning 98). Da gælder

(i) $\zeta_k(s) = \zeta(s) L(s, \chi)$ for $\sigma > 1$.

(ii) $L(1, \chi) \neq 0$.

(iii) $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ har $\sigma_a = \sigma_c = 1$.

(iv) $\zeta_k(s)$ defineret ved (i) for $\sigma > 0$, er holomorf for $\sigma > 0$ pånær i punktet $s = 1$, hvor $\zeta_k(s)$ har en pol af første orden med residuum $L(1, \chi)$.

Bevis: (i) Ifølge sætningerne 60, 98, 110 (korollar), 111 finder vi for $\sigma > 1$:

$$\zeta_k(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$$

$$= \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

$$= \prod_{p} \prod_{\mathfrak{p} \mid (p)} (1 - N(\mathfrak{p})^{-1})^{-1}$$

$$= \prod_{p} \{ (1 - p^{-s})(1 - \chi(p) p^{-s}) \}^{-1}$$

$$= \prod_{p} (1 - p^{-s})^{-1} \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

$$= \zeta(s) L(s, \chi)$$

(ii) Indirekte. Antag $L(1, \chi) = 0$. Da $\zeta(s)$ er holomorf for $\sigma > 0$ påncer en pol af første orden for $s = 1$, og $L(s, \chi)$ ifølge sætning 109 er holomorf for $\sigma > 0$, medfører antagelsen, at $\zeta_k(s) = \zeta(s) L(s, \chi)$ bliver holomorf for $\sigma > 0$. Ifølge sætning 111 gælder for $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$:

(*) $$\tfrac{1}{2} \leqq \sigma_c = \sigma_a \leqq 1,$$

og da sætning 112 finder anvendelse ($a_n \geqq 0$) har $\zeta_k(s)$ følgelig et singulært punkt $\sigma_a \in [\tfrac{1}{2}, 1]$. Dette strider mod, at $\zeta_k(s)$ er holomorf for $\sigma > 0$.

(iii) HVI. Da $L(1,\chi) \neq 0$, har $\zeta_k(s)$ defineret ved (i) en pol af første orden i punktet $s = 1$ med residuum $L(s,\chi) \neq 0$. Heraf følger, at Dirichletrækken $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ har $\sigma_c \geq 1$, og (*) giver derfor det ønskede resultat. □

Sætning 114. Lad χ modulo D være en vilkårlig Dirichletkarakter, og lad ψ være den entydigt bestemte primitive Dirichletkarakter, som inducerer χ. Da gælder

$$L(s,\chi) = L(s,\psi) \prod_{p \mid D} (1 - \psi(p) p^{-s}).$$

For enhver Dirichletkarakter χ modulo D gælder

$$L(1,\chi) \neq 0, \text{ når } \chi \neq \chi_0.$$

Bevis: Da

$$\chi(p) = \begin{cases} \psi(p) & \text{når } p \nmid D \\ 0 & \text{når } p \mid D \end{cases},$$

fås for $\sigma > 1$

$$L(s,\psi) = \prod_{p} (1 - \psi(p) p^{-s})^{-1}$$

$$= \prod_{p \mid D} (1 - \psi(p) p^{-s})^{-1} \prod_{p \nmid D} (1 - \psi(p) p^{-s})^{-1}$$

$$= \prod_{p \mid D} (1 - \psi(p) p^{-s})^{-1} \prod_{p} (1 - \chi(p) p^{-s})^{-1}.$$

Lad χ være en vilkårlig karakter modulo D og χ_0 hovedkarakteren modulo D. Da gælder

$$(*) \qquad L(s,\chi_0)^3\,|L(s,\chi)|^4\,|L(s,\chi^2)|^2 \geq 1$$

for $s=\sigma>1$. Til beviset herfor bemærkes først, at

$$(**) \qquad 2\cos 2\theta + 4\cos\theta + 3 = (2\cos\theta+1)^2 \geqq 0$$

for $\theta \in \mathbb{R}$. Vi påstår endvidere, at

$$(***) \qquad (1-\alpha)^3\,|1-\alpha e^{i\theta}|^4\,|1-\alpha e^{2i\theta}|^2 < 1$$

for $0<\alpha\leq 1$ og $\theta\in\mathbb{R}$. Benyttes nemlig (**) og uligheden mellem geometrisk og aritmetisk middelværdi fås

$$\begin{aligned}
&(1-\alpha)^3\,|1-\alpha e^{i\theta}|^4\,|1-\alpha e^{2i\theta}|^2 \\
&\leqq (1-\alpha)^3\,(1-2\alpha\cos\theta+\alpha^2)^2(1-2\alpha\cos 2\theta+\alpha^2) \\
&\leqq (1-\alpha)^3\left(1-\tfrac{\alpha}{3}\,|4\cos\theta+2\cos 2\theta)+\alpha^2\right)^3 \\
&\leqq (1-\alpha)^3\,(1+\alpha+\alpha^2)^3 \\
&= (1-\alpha^3)^3 < 1,
\end{aligned}$$

hvormed (***) er vist.

I L^{ν} betragtes produktet af de faktorerer i Eulerproduktet, som hidrører fra et fast primtal p:

$$\left\{(1-\chi_0(p)\,p^{-s})^3\,|1-\chi(p)\,p^{-s}|^4\,|1-\chi^2(p)\,p^{-s}|^2\right\}^{-1}.$$

Såfremt $p\mid D$ er bidraget 1 og for $p\nmid D$ er bidraget

> 1 ifølge (***), anvendt med

$$\alpha = p^{-s} \quad , \quad e^{i\theta} = \chi(p).$$

Dette viser (*).

Antag først, at $\chi \neq \chi_0$ ikke er kvadratisk, dvs. $\chi^2 \neq \chi_0$.

Såfremt $L(1,\chi) = 0$ ville

$$L(s,\chi_0)^3 \, L(s,\chi)^4 \, L(s,\chi^2)^2,$$

da $4 > 3$, have et nulpunkt for $s = 1$, eftersom $L(s,\chi_0)$ har en pol af første orden og $L(s,\chi^2)$ er holomorf for $s = 1$. Dette strider mod (*), og følgelig har vi vist

$$L(1,\chi) \neq 0 \quad \text{for} \quad \chi^2 \neq \chi_0.$$

For $\chi \neq \chi_0$ men $\chi^2 = \chi_0$ er

$$L(s,\chi) = L(s,\psi) \prod_{p \mid D} (1 - \psi(p) p^{-s}),$$

hvor ψ er den tilhørende primitive kvadratiske karakter. Ifølge sætning 113 (ii) er $L(1,\psi) \neq 0$, hvoraf $L(1,\chi) \neq 0$. □

Sætning 115. (Dirichlet, 1837). Enhver primisk restklasse modulo D, $D \in \mathbb{N}$, indeholder uendelig mange primtal.

Bemærkning. Sætningen kan skærpes som følger: Lad $D \in \mathbb{N}$, og lad C være en vilkårlig primisk restklasse modulo D. Vi sætter

$$\pi(x; D, C) = \text{antal primtal } p \leq x \text{ for hvilke } p \in C.$$

Da gælder

$$(*) \qquad \frac{\pi(x; D, C)}{x / \ln x} \to \frac{1}{\varphi(D)} \qquad \text{for } x \to \infty$$

for enhver primisk restklasse C modulo D. Specielt gælder for $D = 1$

$$\frac{\pi(x)}{x / \ln x} \to 1 \qquad \text{for } x \to \infty,$$

hvor

$$\pi(x) = \text{antal primtal } p \leq x.$$

Sidstnævnte sætning er "primtalssætningen", som blev formodet af Gauss (på grundlag af tabeller over primtalsfunktionen $\pi(x)$), men først vist (1896) uafhængigt af hinanden af Hadamard (fransk matematiker) og de la Vallée-Poussin (belgisk matematiker) ved at benytte egenskaber for $\zeta(s)$ på linien $\sigma = 1$. Det i beviset for sætning 114 benyttede trick med at kigge på $\zeta(s, \chi_0)^3 |L(s, \chi)|^4 |L(s, \chi^2)|$ skyldes Hadamard og forekommer netop i hans bevis for primtalssætningen. A. Selberg og P. Erdös viste i 1949 primtalssætningen ved elementære metoder.

Bevis: Lad $D \in \mathbb{N}$ være givet, og lad χ være en vilkårlig af de $\varphi(D)$ Dirichletkarakterer modulo D. Da er

$$L(s,\chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$$

konvergent i halvplanen $\sigma > 1$, og $L(s,\chi) \neq 0$ her, da ingen af faktorerne bliver 0. For hver faktor er

$$-\log\left(1-\chi(p)p^{-s}\right) = \sum_{n=1}^{\infty} \frac{1}{n}\chi(p)^n p^{-ns}$$

en kontinuert logaritmefunktion, da $|\chi(p)p^{-s}| < 1$.

Vi definerer nu

$$(*) \qquad \log L(s,\chi) = \sum_p \sum_{n=1}^{\infty} \frac{1}{n}\chi(p)^n p^{-ns}, \qquad \sigma > 1.$$

Det bemærkes, at

$$\sum_p \sum_{n=1}^{\infty} \frac{1}{n}\chi(p)^n p^{-ns} = \sum_{m=1}^{\infty} a_m m^{-s}$$

er en Dirichletrække med

$$a_m = \begin{cases} \frac{1}{n}\chi(p)^n, & \text{hvis } m = p^n \\ 0 & \text{ellers} \end{cases}.$$

Det er derfor klart, at $\sigma_a \leq 1$. Den ved denne række fremstillede funktion er derfor en kontinuert (og dermed holomorf) logaritmefunktion. Vi omskriver nu (*) på følgende måde

$$(**) \qquad \log L(s,\chi) = \sum_p \chi(p)p^{-s} + R(s,\chi),$$

hvor

$$R(s,\chi) = \sum_p \left(\tfrac{1}{2}\chi(p)^2 p^{-2s} + \tfrac{1}{3}\chi(p)^3 p^{-3s} + \cdots \right).$$

I det følgende vil vi antage, at $s = \sigma > 1$. Der gælder da

$$|R(s,\chi)| \leqq \sum_p (p^{-2s} + p^{-3s} + \cdots) = \sum_p \frac{1}{p^{2s} - p^s}$$

$$< \sum_p \frac{1}{p(p-1)} < \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1,$$

og denne vurdering af restleddet gælder uniformt for s i intervallet $]1, \infty[$.

Formlen (**) omskrives yderligere til

$$(***) \qquad \text{Log } L(s,\chi) = \sum_C \chi(C) f(s,C) + R(s,\chi),$$

hvor der summeres over de $\varphi(D)$ primiske restklasser C modulo D og

$$f(s,C) = \sum_{p \in C} p^{-s}.$$

Ialt er der $\varphi(D)$ karakterer χ modulo D, og derfor $\varphi(D)$ ligninger (***). Opfattes de $\varphi(D)$ funktioner $f(s,C)$ som ubekendte kan ligningssystemet løses m.h.t. disse, idet

$$\frac{1}{\sqrt{\varphi(D)}} \det \left(\chi(C)\right)_{\chi,C}$$

er en unitær matrix, og derfor har determinant 1.

For at løse m.h.t. $f(s,A)$, hvor A er en given primisk

restklasse modulo D multipliceres hver af ligningerne (***) med $\chi(A^{-1})$, hvorefter disse adderes. Da

$$\sum_{\chi}\sum_{C}\chi(CA^{-1})f(s,C) = \sum_{C} f(s,C)\sum_{\chi}\chi(CA^{-1})$$

$$= f(s,A)\cdot\varphi(D),$$

ifølge sætning 96 (**), fås herved

$$\log L(s,\chi_0) + \sum_{\chi\neq\chi_0}\left(\log L(s,\chi)\,\chi(A^{-1})\right) = f(s,A)\cdot\varphi(D) + R_A(s,\chi),$$

hvor $R_A(s,\chi)$ er uniformt begrænset for s i $]1,\infty[$.

Da $L(1,\chi)\neq 0$ for $\chi\neq\chi_0$ er

$$\sum_{\chi\neq\chi_0}\left(\log L(s,\chi)\,\chi(A^{-1})\right)$$

ligeledes begrænset i et interval $]1,s_0[$, $s_0>1$.

Da $L(s,\chi_0)$ har en pol af første orden for $s=1$ er $\log L(s,\chi_0)$ derimod <u>ikke</u> begrænset for $s\to 1^+$, og følgelig er funktionen

$$f(s,A) = \sum_{p\in A} p^{-s}, \quad A \text{ primisk restkl. mod. } D$$

det heller ikke.

Heraf følger umiddelbart, at A må indeholde uendeligt mange primtal p.

Summation af L-rækker.

Formålet med det følgende er at beregne $L(1,\chi)$, når χ er en fra hovedkarakteren forskellig karakter modulo D, $D \in \mathbb{N}$. På grund af formlen i sætning 114 kan det uden indskrænkning antages, at χ er en primitiv karakter modulo D, og at $D > 1$. På grund af periodiciteten af χ kan vi skrive

$$L(s,\chi) = \sum_{x \bmod D} \chi(x) \sum_{n \equiv x\,(D)} n^{-s}.$$

Den inderste række er derfor en Dirichletrække

$$\sum_{n=1}^{\infty} a_n n^{-s}$$

hvor

$$a_n = \begin{cases} 1 & \text{for } n \equiv x \ (D) \\ 0 & \text{for } n \not\equiv x \ (D). \end{cases}$$

Funktionen $n \mapsto a_n$ er periodisk med periode D, og da vektorrummet af sådanne periodiske funktioner har en basis bestående af (jvf. pag. 187)

$$\{ f_c : n \mapsto \zeta^{cn} \mid \zeta = e^{2\pi i/D}, \ c \text{ modulo } D \},$$

kan vi på entydig måde skrive

$$a_n = \sum_{c \bmod D} b_c \zeta^{cn}, \quad b_c \in \mathbb{C}.$$

Det verificeres umiddelbart, at fremstillingen er

$$a_n = \frac{1}{D} \sum_{c=0}^{D-1} \zeta^{c(x-n)} .$$

Vi har derfor

$$L(s,\chi) = \sum_{x \bmod D} \chi(x) \sum_{n=1}^{\infty} \frac{1}{D} \sum_{c=0}^{D-1} \zeta^{c(x-n)} n^{-s}$$

$$= \frac{1}{D} \sum_{c=0}^{D-1} \Big(\sum_{x \bmod D} \chi(x) \zeta^{cx} \Big) \sum_{n=1}^{\infty} \zeta^{-cn} n^{-s}$$

$$= \frac{1}{D} \sum_{c=0}^{D-1} \tau_c(\chi) \sum_{n=1}^{\infty} \zeta^{-cn} n^{-s} .$$

Her gælder for det første

$$\tau_c(\chi) = \overline{\chi(c)}\, \tau(\chi) ,$$

hvor $\tau(\chi) = \tau_1(\chi)$ er den normerede gaussiske sum.

For $\gcd(c,D) = 1$ er nemlig (idet $\chi(c) \neq 0$)

$$\tau_c(\chi) = \overline{\chi(c)} \sum_{x \bmod D} \chi(cx) \zeta^{cx} = \overline{\chi(c)}\, \tau(\chi).$$

For $\gcd(c,D) = r > 1$, og vi skal derfor vise, at $\tau_c(\chi) = 0$.

Sæt $D = r D'$ og vælg $z \equiv 1 \ (D')$ og $\gcd(z,D) = 1$ (jvf. ① pag. 180). Da gælder (idet $\gcd(z,D) = 1$ og $(\zeta^c)^{D'} = 1$)

$$\tau_c(\chi) = \sum_{x \bmod D} \chi(x) \zeta^{cx} = \sum_{x \bmod D} \chi(xz) \zeta^{cxz}$$

$$= \chi(z) \sum_{x \bmod D} \chi(x) \zeta^{cx} = \chi(z)\, \tau_c(\chi).$$

Her kan yderligere antages, at $\chi(z) \neq 1$, idet $\chi(z) = 1$ for alle

$z \equiv 1 \ (D')$, $\gcd(z, D) = 1$ medfører (øvelse), at χ er induceret af en karakter χ' mod D'.
Formlen for $L(s, \chi)$ kan herefter skrives

$$L(s,\chi) = \frac{\tau(\chi)}{D} \sum_{c=1}^{D-1} \overline{\chi(c)} \sum_{n=1}^{\infty} \zeta^{-cn} n^{-s}.$$

For det andet har Dirichletrækken

$$\sum_{n=1}^{\infty} \zeta^{-cn} n^{-s}$$

for $c \not\equiv 0 \ (D)$ begrænsede afsnit for $s = 0$, medens rækken naturligvis er divergent. Følgelig er $\sigma_c = 0$, og Dirichletrækken er specielt konvergent for $s = 1$, dvs.

$$L(1,\chi) = \frac{\tau(\chi)}{D} \sum_{c=1}^{D-1} \overline{\chi(c)} \sum_{n=1}^{\infty} \frac{1}{n} \zeta^{-cn}.$$

Da

$$\sum_{n=1}^{\infty} \frac{1}{n} \zeta^{-cn} = -\log(1 - \zeta^{-c})$$

ifølge Abels sætning anvendt på potensrækken

$$-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$$

og konvergenspunktet $z = \zeta^{-c}$, fås endelig

$$\boxed{L(1,\chi) = -\frac{\tau(\chi)}{D} \sum_{c=1}^{D-1} \overline{\chi(c)} \log(1 - \zeta^{-c})},$$

hvilket er det søgte endelige udtryk for $L(1, \chi)$.

Da $0 < c/D < 1$ og

$$1 - e^{-\frac{2\pi i}{D}c} = 2i\, e^{-\frac{\pi i}{D}c}\, \frac{e^{\frac{\pi i}{D}c} - e^{-\frac{\pi i}{D}c}}{2i} = 2i\, e^{-\frac{\pi i}{D}c} \sin\frac{\pi c}{D}$$

$$= 2\sin\frac{\pi c}{D}\, e^{i\left(\frac{\pi}{2} - \frac{\pi c}{D}\right)},$$

er hovedværdien af logaritmefunktionen givet ved

$$\log\left(1 - \zeta^{-c}\right) = \ln\left(2\sin\frac{\pi c}{D}\right) + i\pi\left(\frac{1}{2} - \frac{c}{D}\right).$$

Ved konjugering fås derfor

$$\log\left(1 - \zeta^{c}\right) = \ln\left(2\sin\frac{\pi c}{D}\right) - i\pi\left(\frac{1}{2} - \frac{c}{D}\right).$$

Det bemærkes, at hovedværdien af logaritmefunktionen er den analytiske fortsættelse af $\ln x$, $0 < x < \infty$, til $\mathbb{C} \setminus]-\infty, 0]$, og at denne hovedværdi (her kaldet $\log$) har Taylorudviklingen

$$-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n} \qquad \text{for} \qquad |z| \leq 1\,,\ z \neq 1.$$

Specielt er

$$\log w = \overline{\log \bar{w}} \qquad \text{for} \qquad w \in \mathbb{C} \setminus]-\infty, 0].$$

Vi vil nu omforme

$$S(\chi) = \sum_{c=1}^{D-1} \bar{\chi}(c) \log\left(1 - \zeta^{-c}\right),$$

alt afhængigt af om χ er lige ($\chi(-1) = 1$) eller χ er ulige ($\chi(-1) = -1$).

Da

$$S(\chi) = \frac{1}{2}\left\{ \sum_{c=1}^{D-1} \bar{\chi}(c) \log (1-\zeta^{-c}) + \sum_{c=1}^{D-1} \bar{\chi}(-c) \log (1-\zeta^{c}) \right\}$$

$$= \frac{1}{2} \sum_{c=1}^{D-1} \bar{\chi}(c) \left\{ \log (1-\zeta^{-c}) + \chi(-1) \log (1-\zeta^{c}) \right\}$$

finder vi ved indsættelse af udtrykkene for $\log (1-\zeta^{\pm c})$:

$$L(1,\chi) = -\frac{\tau(\chi)}{D} \sum_{c=1}^{D-1} \bar{\chi}(c) \ln \sin \frac{\pi c}{D} \qquad \text{for } \chi \text{ lige},$$

$$L(1,\chi) = \frac{\pi i\, \tau(\chi)}{D^2} \sum_{c=1}^{D-1} \bar{\chi}(c)\, c \qquad \text{for } \chi \text{ ulige}.$$

Bemærk, at vi begge steder har benyttet, at

$$\sum_{c=1}^{D-1} \overline{\chi(c)} = 0.$$

<u>Sætning 116</u> (Dirichlet). Lad $k = \mathbb{Q}(\sqrt{d})$ være et kvadratisk tallegeme af diskriminant d, og sæt $|d| = D$. Da er klassetallet h for k givet ved

$$h = -\frac{1}{2 \ln \varepsilon} \sum_{0<c<\frac{D}{2}} \chi(c) \ln \sin \frac{\pi c}{D} \qquad \text{for } d > 1,$$

$$h = -\frac{w}{2} \frac{1}{D} \sum_{c=1}^{D-1} \chi(c)\, c \qquad \text{for } d < 0,$$

hvor χ er den primitive kvadratiske karakter hørende til legemet k.

Bevis: Ifølge sætning 113 er

$$\zeta_k(s) = \zeta(s)\, L(s,\chi),$$

hvor χ er den primitive kvadratiske karakter for k.

Der gælder derfor

$$\lim_{s\to 1}(s-1)\,\zeta_k(s) = \lim_{s\to 1}(s-1)\,\zeta(s)\,L(s,\chi) = L(1,\chi),$$

og ifølge hovedsætningen (pag. 166) er derfor

$$h = \frac{w\sqrt{D}}{2^{r_1+r_2}\pi^{r_2}R}\,L(1,\chi).$$

For $d>1$ er

$$w=2,\quad r_1=2,\quad r_2=0,\quad R=\ln\varepsilon,$$

hvor $\varepsilon>1$ er fundamentalenhed i O_k^*.

For $d<0$ er

$$w=2 \text{ for } d<-4 \quad (w=6 \text{ for } d=-3,\ w=4 \text{ for } d=-4),$$

$$r_1=0,\quad r_2=1,\quad R=1.$$

Endelig er ifølge sætning 99:

$$\tau(\chi)=\sqrt{D} \text{ for } \chi \text{ lige, dvs. } d>1, \qquad d>1$$

$$\tau(\chi)=i\sqrt{D} \text{ for } \chi \text{ ulige, dvs. } d<0.$$

Heraf følger formlerne for h, idet der i det reelle tilfælde yderligere er benyttet en symmetri i summen. □

Sætning 117 Lad $k = \mathbb{Q}(\sqrt{d})$ være et reelt kvadratisk talleseme af diskriminant d (>1). Da er

$$\eta = \prod_{\substack{0<a,b<\frac{d}{2} \\ \chi(a)=1,\ \chi(b)=-1}} \frac{\sin \frac{\pi b}{d}}{\sin \frac{\pi a}{d}} \in O_k^*,$$

og

$$\eta = \varepsilon^h,$$

hvor $\varepsilon > 1$ er fundamentalenhed i O_k^*, og h er klassetallet for k.

Bevis: Resultatet følger umiddelbart af sætning 116. □

Eksempel 50. For $k = \mathbb{Q}(\sqrt{5})$ af diskriminant 5 er $\chi(1) = 1$, $\chi(2) = -1$, dvs.

$$\eta = \sin 2\pi/5 \,/\, \sin \pi/5 = 2\cos \pi/5$$
$$= 2 \cdot \frac{1+\sqrt{5}}{4} = \frac{1+\sqrt{5}}{2}.$$

Da

$$\varepsilon = \frac{1+\sqrt{5}}{2} > 1$$

tillige er fundamentalenhed i O_k^*, er $h = 1$. (Jvf. sætn 79).

Bemærk. Der kendes intet elementært bevis for at enheden $\eta \in O_k^*$ opfylder uligheden $\eta > 1$.

Sætning 118. Lad $k = \mathbb{Q}(\sqrt{d})$ være et imaginært kvadratisk tallegeme af diskriminant $d < -4$, og sæt $-d = D$. Da er

$$h = \frac{1}{2 - \chi(2)} \sum_{0<c<\frac{D}{2}} \chi(c),$$

hvor χ er den primitive kvadratiske karakter hørende til k.

Bevis: Da $w = 2$ fås af sætning 116

$$hD = -\sum_{0<c<D} \chi(c)\, c.$$

For D lige, dvs. $D/2$ lige og derfor $\chi(D/2) = 0$, fås

$$(*) \quad hD = -\sum_{0<c<\frac{D}{2}} \chi(c)\, c - \sum_{0<c<\frac{D}{2}} \chi\left(c+\tfrac{D}{2}\right)\left(c+\tfrac{D}{2}\right).$$

Lad

$$d = d_0 d_1 \cdots d_g,$$

hvor

$$d_0 = 4, \pm 8 \; ; \quad d_j = (-1)^{\frac{p_j-1}{2}} p_j \; , \; p_j \text{ ulige primtal.}$$

Da er

$$\chi(x) = \chi_0(x) \left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_g}\right),$$

hvor χ_0 er en primitiv kvadratisk karakter modulo $4, 8$.

Da

$$\chi_0\left(x+\tfrac{D}{2}\right) = -\chi_0(x) \; , \quad \left(\frac{x+D/2}{p_j}\right) = \left(\frac{x}{p_j}\right) \text{ for alle } j$$

er

$$\chi\left(x+\tfrac{D}{2}\right) = -\chi(x) \quad \text{for alle } x \in \mathbb{Z}.$$

(*) kan derfor omskrives til

$$h_D = \sum_{0<c<\frac{D}{2}} \chi(c)\left(c+\frac{D}{2}-c\right) = \frac{D}{2}\sum_{0<c<\frac{D}{2}} \chi(c),$$

hvilket er den angivne formel for h i dette tilfælde, da $\chi(2) = 0$.

For D ulige benyttes blot, at $\chi(-1) = -1$, hvorfor (*) nu kan omskrives til

$$h_D = -\sum_{0<c<\frac{D}{2}} \chi(c)\,c - \sum_{0<c<\frac{D}{2}} \chi(D-c)(D-c)$$

$$= \sum_{0<c<\frac{D}{2}} \chi(c)(D-2c),$$

altså

$$(**) \qquad h_D = D\sum_{0<c<\frac{D}{2}} \chi(c) - 2\sum_{0<c<\frac{D}{2}} \chi(c)\,c.$$

På den anden side er (da D er ulige)

$$h_D = -\sum_{\substack{0<c<D \\ c \text{ lige}}} \chi(c)\,c - \sum_{\substack{0<c<D \\ c \text{ lige}}} \chi(D-c)(D-c)$$

$$= \sum_{\substack{0<c<D \\ c \text{ lige}}} \chi(c)(D-2c)$$

$$= \chi(2)\sum_{0<c<\frac{D}{2}} \chi(c)(D-4c),$$

altså, da $\chi(2) = \pm 1 = \chi(2)^{-1}$,

(***) $$hD\,\chi(2) = D \sum_{0<c<\frac{D}{2}} \chi(c) - 4 \sum_{0<c<\frac{D}{2}} \chi(c)\,c .$$

Af (**) og (***) fås nu

$$hD\,(2 - \chi(2)) = D \sum_{0<c<\frac{D}{2}} \chi(c),$$

hvilket er den angivne formel for D ulige. □

Eksempel 51. $k = \mathbb{Q}(\sqrt{-5})$, $d = -20$. Da $d = -20 = -4 \cdot 5$ er

$$\chi(x) = \begin{cases} (-1)^{\frac{x-1}{2}} \left(\frac{x}{5}\right) & , \ x \text{ ulige} \\ 0 & , \ x \text{ lige} \end{cases}$$

eller i tabelform:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\chi(x)$	0	1	0	1	0	0	0	1	0	1	0	-1	0	-1	0	0	0	-1	0	-1

Altså er

$$h = \frac{1}{2} \sum_{0<c<10} \chi(c) = \frac{1}{2} \cdot 4 = 2.$$

Bemærk, at det også er muligt at bruge formlen

$$h = \frac{\sqrt{20}}{\pi}\, L(1, \chi)$$

til beregning af h. Det følger nemlig ved en simpel vurdering, at

$$1.3 < 1 + \tfrac{1}{3} + \tfrac{1}{7} + \tfrac{1}{9} - \tfrac{1}{11} - \tfrac{1}{13} - \tfrac{1}{17} - \tfrac{1}{19} < L(1, \chi) < 1 + \tfrac{1}{3} + \tfrac{1}{5} + \tfrac{1}{7} < 1.6,$$

hvorfor

$$1.8 < \frac{\sqrt{20}}{\pi} \cdot 1.3 < h < \frac{\sqrt{20}}{\pi} \cdot 1.6 < 2.3 ,$$

og følgelig $h = 2$. (Jvf. eksemplerne 29 og 44).

Eksempel 52. $k = \mathbb{Q}(\sqrt{-23})$, $d = -23$. Her er

$\chi(x) = \left(\frac{x}{23}\right)$ eller i tabelform:

x	0	1	2	3	4	5	6	7	8	9	10	11	----
$\chi(x)$	0	1	1	1	1	-1	1	-1	1	1	-1	-1	----

Altså er

$$h = \sum_{0<c<\frac{23}{2}} \chi(c) = 3.$$

Eksempel 53. $k = \mathbb{Q}(\sqrt{-14})$, $d = -56 = 8 \cdot (-7)$. Her er

$\chi(x) = \left(\frac{x}{7}\right) \cdot \chi_8(x)$, hvor

$$\chi_8(x) = \begin{cases} (-1)^{\frac{x^2-1}{8}} & x \text{ ulige} \\ 0 & x \text{ lige} \end{cases}.$$

Vi har derfor (idet vi udelader x lige):

x	1	3	5	7	9	11	13	15	17	19	21	23	25	27
$\chi(x)$	1	1	1	0	1	-1	1	1	-1	1	0	1	1	1

Altså er

$$h = \frac{1}{2} \sum_{0<c<28} \chi(c)$$

Øvelse. Vis, at klassegruppen for $\mathbb{Q}(\sqrt{-14})$ er C_4. Vink: Vis, at idealklassen indeholdende $(3, 1+\sqrt{-14})$ er af 4. orden.

Relative udvidelser. Lad $k \subset K$ være algebraiske tallegemer af relativ grad $[K:k] = \dim_k K = n$. Vi vil kort omtale (men kun undtagelsesvis bevise) en række vigtige forhold, som tildels er os bekendte ved såkaldte absolutte udvidelser, dvs. $k = \mathbb{Q}$. Det "lille" legeme k kaldes grundlegemet ved den betragtede udvidelse. De tilsvarende Dedekindringe af hele algebraiske tal i k og K betegnes som sædvanligt O_k og O_K. Idealer i k betegnes med små gotiske bogstaver, idealer i K med store gotiske bogstaver. Ethvert helt ideal $\mathfrak{A}$ i O_K har en naturlig udvidelse til K. Ethvert helt ideal $\mathfrak{A}$ har en naturlig kontraktion $\mathfrak{A} \cap O_k$ til k. Det vises let, at $\mathfrak{A} O_K \cap O_k = \mathfrak{A}$ for alle hele idealer $\mathfrak{A}$ i k. (Jvf. beviset for 2. hovedsætning om Dedekindringe).

Lad $K = k(\vartheta)$, $K^{(\nu)} = k(\vartheta^{(\nu)})$, hvor $\vartheta^{(1)}, \dots, \vartheta^{(n)}$ er ϑ's konjugerede. Idet vi regner indtil for spaltningslegemet $\hat{K} = k(\vartheta^{(1)}, \dots, \vartheta^{(n)}) =$ K's normale hylster m.h.t. k, definieres den relative norm af et ideal $\mathfrak{A}$ i K ved:

$$N_{K/k}\,\mathfrak{A} = \mathfrak{A}^{(1)} \cdot \dots \cdot \mathfrak{A}^{(n)}.$$

Det vises, at $N_{K/k}\,\mathfrak{A}$ er et ideal i k. Så hvert $\mathfrak{A}$ er et helt ideal bliver $N_{K/k}\,\mathfrak{A}$ et helt ideal i k.

Lad $\mathfrak{p} \neq (0)$ være et vilkårligt primideal i O_k. Da gælder

(*) $\quad \mathfrak{p}\,\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$,

hvor $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ er primidealer i $\mathcal{O}_K$. I denne entydige primidealdekomposition er

$$N_{K|k}(\mathfrak{P}_j) = \mathfrak{p}^{f_j} \quad ,$$

hvor $1 \leq f_j$ kaldes graden af $\mathfrak{P}_j$. Eksponenterne $e_j \geq 1$, kaldes forgreningsindices. $\mathfrak{p}$ kaldes uforgrenet såfremt $e_1 = \cdots = e_g = 1$, og ellers forgrenet.

Ved i (*) at tage den relative norm $N_{K|k}$ på begge sider fås:

(**) $$n = \sum_{j=1}^{g} e_j f_j .$$

For at skaffe klarhed over hvilke primidealer $\mathfrak{p}$, der er forgrenede, indføres relativ different og relativ diskriminant:

$$\delta_{K|k}^{-1} = \{ x \in K \mid S_{K|k}(x\,\mathcal{O}_K) \subset \mathcal{O}_k \},$$

$$d_{K|k} = N_{K|k}(\delta_{K|k}).$$

Differenten $\delta_{K|k}$ er et helt ideal i $\mathcal{O}_K$, og diskriminanten $d_{K|k}$ er et helt ideal i $\mathcal{O}_k$.

Bemærkning: Det er ikke muligt i almindelighed at indføre diskriminanten $d_{K|k}$ i lighed med den absolutte diskriminant. Dette skyldes, at $\mathcal{O}_k$

normalt ikke er PID og (jvf. sætning 21) dette medfører, at $\mathcal{O}_K$ normalt ikke er en fri $\mathcal{O}_k$-modul.
Fx. kan dette vises, når

$$k = \mathbb{Q}(\sqrt{-14}), \qquad K = k(\sqrt{2}).$$

Sætning 119 (Dedekind). Et primideal $\mathfrak{p}$ i k er forgrenet, hvis og kun hvis $\mathfrak{p} \mid d_{K/k}$.
Et primideal $\mathfrak{p}$ i k med dekomposition (*) er forgrenet i $\mathfrak{P}_j$ (dvs. $e_j > 1$), hvis og kun hvis $\mathfrak{P}_j \mid \delta_{K/k}$.

Det fremgår, at der kun er endeligt mange forgrenede primidealer (i k og K). Problemet er blot, at det normalt er vanskeligt at beregne diskriminanten og meget vanskeligt at beregne differenten.

I det følgende vil vi nøjes med at betragte udvidelser $k < K$, som er galoiske (dvs K/k er normal). Galoisgruppen $\mathrm{Gal}(K/k)$ betegnes med G. Specielt kaldes udvidelsen abelsk (cyklisk), såfremt G er abelsk (cyklisk).

Sætning 120. Lad K/k være galoisk, og lad $\mathfrak{p}$ ($\neq(0)$) være et vilkårligt primideal i $\mathcal{O}_k$. I dekompositionen

$$\mathfrak{p}\,\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

gælder da

$e_1 = \cdots = e_g = e$, $f_1 = \cdots = f_g = f$,

og primidealerne $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ er konjugerede (m.ht. til virkningen af G).

Bevis: Den første påstand følger af den sidste, thi antag, at $\mathfrak{P}_j = \sigma_j(\mathfrak{P}_1)$, $\sigma_j \in G$, for alle $j = 1, \cdots, g$. Da er

$$N_{K|k}\,\mathfrak{P}_j = \prod_{\sigma \in G} \sigma(\mathfrak{P}_j) = \prod_{\sigma \in G} \sigma\sigma_j(\mathfrak{P}_1) = \prod_{\sigma \in G} \sigma(\mathfrak{P}_1)$$

$$= N_{K|k}\,\mathfrak{P}_1 ,$$

hvor for $f_j = f_1$ for $1 \leq j \leq g$. Endvidere er

$\mathfrak{p}\,\mathfrak{O}_K = \sigma_j(\mathfrak{p}\,\mathfrak{O}_K)$ for $1 \leq j \leq g$, hvoraf

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} = \sigma_j(\mathfrak{P}_1)^{e_1} \cdots \sigma_j(\mathfrak{P}_g)^{e_g} = \mathfrak{P}_j^{e_1} \cdots .$$

Følgelig er $e_j = e_1$ for $1 \leq j \leq g$.

For at vise den sidste påstand får vi brug for følgende: Hvis et ideal $\mathfrak{A}$ i en kommutativ ring R er indeholdt i foreningen af primidealerne $\mathfrak{P}_1, \cdots, \mathfrak{P}_s$, da er $\mathfrak{A}$ indeholdt i et af primidealerne $\mathfrak{P}_1, \cdots, \mathfrak{P}_s$. I kontraponeret form lyder denne sætning således: Hvis $\mathfrak{A} \nsubseteq \mathfrak{P}_j$, $1 \leq j \leq s$, da findes et $a \in \mathfrak{A}$, så $a \notin \mathfrak{P}_j$, $1 \leq j \leq s$. Vi viser dette ved induktion efter s. For $s = 1$ er påstanden trivielt opfyldt. Ved anvendelse af induktions-

antagelsen for $s-1$ primidealer findes for hvert $j = 1, \dots, s$, et $a_j \in \mathcal{O}_k$, så $a_j \notin \mathfrak{P}_1, \dots, \mathfrak{P}_{j-1}, \mathfrak{P}_{j+1}, \dots, \mathfrak{P}_s$.

Sæt $a = \sum_{j=1}^{s} a_1 \cdots a_{j-1}\, a_{j+1} \cdots a_s$. Da er klart $a \in \mathcal{O}_k$, men $a \notin \mathfrak{P}_j$, $1 \le j \le s$, da det j'te led i summen ikke tilhører $\mathfrak{P}_j$, medens alle andre led gør.

Vi viser nu den sidste påstand indirekte, idet vi antager, at to af primidealerne $\mathfrak{P}_1, \dots, \mathfrak{P}_g$, fx $\mathfrak{P}_1$ og $\mathfrak{P}_g$ ikke er konjugerede. Da $\mathfrak{P}_g \neq \sigma(\mathfrak{P}_1)$ for $\sigma \in G$, og $\mathfrak{P}_g$ er et maksimalt ideal i $\mathcal{O}_k$ er $\mathfrak{P}_g \not\subseteq \sigma(\mathfrak{P}_1)$ for noget $\sigma \in G$. I følge det netop viste gælder derfor

$$\mathfrak{P}_g \not\subseteq \bigcup_{\sigma \in G} \sigma(\mathfrak{P}_1).$$

Vælg $x \in \mathfrak{P}_g$, $x \notin \sigma(\mathfrak{P}_1)$ for $\sigma \in G$, og betragt

$$N(x) = N_{k/k}(x) = \prod_{\sigma \in G} \sigma(x).$$

Da $\mathrm{id} \in G$, er det klart, at $N(x) \in \mathfrak{P}_g$, og da $N(x) \in \mathcal{O}_k$, er derfor

$$(*) \qquad N(x) = \mathfrak{P}_g \cap \mathcal{O}_k = \mathfrak{p}.$$

På den anden side er $x \notin \sigma(\mathfrak{P}_1)$, $\sigma \in G$, hvorfor $\sigma^{-1}(x) \notin \mathfrak{P}_1$ for $\sigma \in G$. Følgelig er

$$(**) \qquad N(x) = \prod_{\sigma \in G} \sigma(x) = \prod_{\sigma \in G} \sigma^{-1}(x) \notin \mathfrak{P}_1.$$

(*) og (**) giver en modstrid, da $\mathfrak{p} = \mathfrak{P}_1 \cap \mathcal{O}_k \subset \mathfrak{P}_1$. $\square$

Lad K/k være galoisk med $G = \mathrm{Gal}(K/k)$. Lad $\mathfrak{p}$ være et vilkårligt primideal i O_k. Ifølge den foregående sætning er da

$$\mathfrak{p}\, O_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e, \quad N_{K/k}(\mathfrak{P}_j) = \mathfrak{p}^f \ (f \text{ uafh. af } j)$$

og følgelig er

$$[K:k] = n = efg.$$

Vi definerer med Hilbert:

$$G_Z^{(j)} = \{\sigma \in G \mid \sigma(\mathfrak{P}_j) = \mathfrak{P}_j\},$$

$$G_T^{(j)} = \{\sigma \in G \mid \sigma(a) \equiv a \ (\mathfrak{P}_j) \text{ for alle } a \in O_K\}.$$

Det er umiddelbart, at se at $G_Z^{(j)}$ og $G_T^{(j)}$ er undergrupper af G, kaldet <u>opløsningsgruppe</u> ("Zerlegungsgruppe") og <u>trægtedsgruppe</u> ("Trägheitsgruppe"). Det fremgår ligeledes umiddelbart, at

$$G_Z^{(j)} = \sigma_j\, G_Z^{(1)}\, \sigma_j^{-1}, \quad G_T^{(j)} = \sigma_j\, G_T^{(1)}\, \sigma_j^{-1},$$

hvor $\sigma_j(\mathfrak{P}_1) = \mathfrak{P}_j$. (Et sådant σ_j findes for alle j ifølge sætning 120). Specielt skriver vi G_Z, G_T uden index j, når G er abelsk. Vi anfører uden bevis:

Sætning 121. (Hilbert, Artin) R

$$|G_Z^{(j)}| = ef \quad , \quad |G_T^{(j)}| = e,$$

$$G_T^{(j)} \triangleleft G_Z^{(j)} \quad , \quad G_Z^{(j)}/G_T^{(j)} \cong C_f.$$

For $e = 1$ er en kanonisk frembringer for $G_Z^{(j)} \cong C_f$ givet ved

$$\sigma^{(j)} = \left(\frac{K/k}{\mathfrak{Y}_j}\right),$$

hvor $\sigma^{(j)} \in G_Z^{(j)}$ er entydigt bestemt ved, at

$$\sigma^{(j)}(x) \equiv x^q \pmod{\mathfrak{Y}_j} \text{ for alle } x \in O_K,$$

hvor $q = N_{k/\mathbb{Q}}(\mathfrak{y})$ er absolutnormen af $\mathfrak{y}$.

Anderledes udtrykt: $\sigma^{(j)}$ inducerer en automorfi $\bar{\sigma}^{(j)}$ af $(O_K/\mathfrak{Y}_j)/(O_k/\mathfrak{y})$, hvor $O_k/\mathfrak{y} \cong GF(q)$, $O_K/\mathfrak{Y}_1 \cong GF(q^f)$, nemlig Frobeniusautomorfien defineret ved

$$\bar{\sigma}^{(j)}(\bar{x}) = \bar{x}^q \text{ for alle } \bar{x} \in O_K/\mathfrak{Y}_j.$$

Automorfien $\sigma^{(j)}$ kaldes ligeledes Frobeniusautomorfien.

Når K/k er abelsk er $\sigma^{(j)}$ uafhængig af j, idet $\sigma^{(j)} = \sigma$ er bestemt ved

$$\sigma(x) \equiv x^q \pmod{\mathfrak{y}} \text{ for alle } x \in O_K.$$

Frobeniusautomorfien skrives da $\sigma = \left(\frac{K/k}{\mathfrak{y}}\right)$. Når k er underforstået (fx når $k = \mathbb{Q}$) skrives undertiden $\sigma = \left(\frac{K}{\mathfrak{y}}\right)$. Symbolet $\left(\frac{K/k}{\mathfrak{y}}\right)$ kaldes også Artinsymbolet.

Korollar. Lad $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/m}$, $m \geq 3$. For et primtal $p \nmid m$ gælder

$$p\mathcal{O}_K = \mathfrak{Y}_1 \cdots \mathfrak{Y}_g \quad , \quad fg = \varphi(m) \, ,$$

og hvor f = graden af $\mathfrak{Y}_j$ er bestemt ved:

$$f = \min \{ r \in \mathbb{N} \mid p^r \equiv 1 \pmod m \}.$$

Bevis: Det kan vises, at $\{1, \zeta, \cdots, \zeta^{\varphi(m)-1}\}$ er en $\mathbb{Z}$-basis for $\mathcal{O}_K$. (Vi har tidligere vist dette når $m = \ell$ er et ulige primtal). Derved vises relativt let, at den absolutte diskriminant for K kun indeholder primfaktorer fra m, altså specielt, at $p \nmid d$. Ifølge sætning 119 (der også gælder for $k = \mathbb{Q}$ og absolut diskriminant) er p derfor utforgrenet. Der gælder derfor som anført

$$p\mathcal{O}_K = \mathfrak{Y}_1 \cdots \mathfrak{Y}_g \quad , \quad fg = \varphi(m).$$

Ifølge sætning 121 med $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta)$, er $G \cong G_m$ (gruppen af primiske restklasser modulo m). For $\mathfrak{y} = (p)$ er $e = 1$ og derfor $G_T = 1$. Altså er $G_Z \cong G_f$ frembragt af Frobenius automorfien $\sigma = \left(\frac{K}{p}\right) \in G$, som her er bestemt ved

$$\sigma(x) \equiv x^p \pmod p \, . \tag{*}$$

Da σ permuterer nulpunkterne i $\Phi_m(x)$ er

$$\sigma(\zeta) = \zeta^a \quad , \quad \gcd(a,m) = 1.$$

Sammenholdt med (*) giver dette $\zeta^a \equiv \zeta^p \pmod p$ eller $\zeta^p(1-\zeta^{a-p}) \equiv 0 \pmod p$, altså

$$(**) \qquad 1-\zeta^{a-p} \equiv 0 \pmod p.$$

Vi påstår nu, at (**) medfører, at $a \equiv p \pmod m$, eller

$$(***) \qquad \sigma(\zeta) = \zeta^p.$$

Hvis nemlig $a \not\equiv p \pmod m$ følger af (**), at

$$(****) \qquad \prod_{\substack{r \bmod m \\ r \not\equiv 0 (m)}} (1-\zeta^r) \equiv 0 \pmod p.$$

Imidlertid er

$$\prod_{\substack{r \bmod m \\ r \not\equiv 0 (m)}} (x-\zeta^r) = \frac{x^m-1}{x-1} = x^{m-1}+x^{m-2}+\cdots+x+1,$$

hvorfor (***) medfører $m \equiv 0 \pmod p$, modstrid!

Da σ har orden f følger nu af (***), at

$$f = \min\{r \in \mathbb{N} \mid p^r \equiv 1 \pmod m\}. \qquad \square$$

<u>Sætning 122.</u> Lad $K = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/m}$. Da gælder

$$\zeta_K(s) = \prod_{\chi} L(s,\chi), \qquad \operatorname{Re} s > 1,$$

hvor produktet tages over de $\varphi(m)$ primitive karakterer, som induceres af de $\varphi(m)$ karakterer modulo m.

Lad $K_0 = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(2\cos 2\pi/m)$ være det maksimale reelle dellegeme af $K = \mathbb{Q}(\zeta)$. Da gælder

$$\zeta_{K_0}(s) = \prod_{\chi \text{ lige}} L(s, \chi), \qquad \operatorname{Re} s > 1,$$

hvor produktet tages over de $\frac{1}{2}\varphi(m)$ primitive karakterer, som induceres af de $\frac{1}{2}\varphi(m)$ lige karakterer modulo m.

Bevis: For simpelhedens skyld viser vi kun sætningen for $m = l =$ ulige primtal. I dette tilfælde er alle Dirichletkarakterer modulo l påvirker hovedkarakteren primitive, og vi skal derfor vise:

(1) $$\zeta_K(s)/\zeta(s) = \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0}} L(s, \chi),$$

(2) $$\zeta_{K_0}(s)/\zeta(s) = \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0,\ \chi \text{ lige}}} L(s, \chi).$$

(1): I sætning 89 har vi vist, at diskriminanten d for K (over $\mathbb{Q}$) er

$$d = (-1)^{\frac{l-1}{2}} l^{l-2}.$$

Eneste forgrenede primtal er derfor l selv, og vi har endvidere i sætning 88, korollar, fundet at

$$l\mathcal{O}_K = (\lambda)^{l-1},$$

hvor $\lambda = 1 - \zeta$ har $N((\lambda)) = l$. For primtallet l er altså

$$e_l = l - 1 \quad , \quad f_l = g_l = 1 .$$

For primtal $p \neq l$ gælder ifølge sætning 121, korollar:

$$e_p = 1 \quad , \quad f_p \cdot g_p = l - 1 \quad ,$$

hvor

$$f_p = \min \{ r \in \mathbb{N} \mid p^r \equiv 1 \pmod{l} \} .$$

Vi finder derfor

$$(*) \qquad \zeta_K(s) = \prod_{p} \prod_{\mathfrak{y} \mid p} \left(1 - N(\mathfrak{y})^{-s}\right)^{-1}$$

$$= \prod_{p} \left(1 - p^{-f_p s}\right)^{-g_p}$$

$$= \left(1 - l^{-s}\right)^{-1} \prod_{p \neq l} \left(1 - p^{-f_p s}\right)^{-\frac{l-1}{f_p}} .$$

På den anden side er

$$(**) \qquad \zeta(s) \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0}} L(s, \chi) = \prod_{p} \left\{ \left(1 - p^{-s}\right)^{l-1} \cdot \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0}} \left(1 - \chi(p) p^{-s}\right)^{-1} \right\} .$$

Skrives

$$1 - p^{-f_p s} = \prod_{j=0}^{f_p - 1} \left(1 - \varepsilon_p^{\,j} p^{-s}\right) ,$$

hvor ε_p er en primitiv f_p'te enhedsrod, fremgår det

umiddelbart, at produkterne (*) og (**) for hvert primtal p indeholder præcis de samme Euler-faktorer. Hermed er formel (1) bevist.

(2): Da $\mathcal{O}_{K_0} = \mathcal{O}_K \cap K_0$, består K_0 af de elementer i

$$\mathcal{O}_K = \mathbb{Z}\,\zeta + \mathbb{Z}\,\zeta^2 + \cdots + \mathbb{Z}\,\zeta^{\ell-1},$$

som er invariante under kompleks konjugering, dvs. invariante ved automorfien $\zeta \mapsto \zeta^{-1} \in \mathrm{Gal}(K/\mathbb{Q})$.

Følgelig er

$$\mathcal{O}_{K_0} = \mathbb{Z}\,(\zeta+\zeta^{-1}) + \mathbb{Z}\,(\zeta^2+\zeta^{-2}) + \cdots + \mathbb{Z}\,(\zeta^{\frac{\ell-1}{2}}+\zeta^{-\frac{\ell-1}{2}}),$$

og da $[K_0 : \mathbb{Q}] = \frac{\ell-1}{2}$ er derfor

$$\{\,\omega_j = \zeta^j + \zeta^{-j} \mid 1 \le j \le \tfrac{\ell-1}{2}\,\}$$

en $\mathbb{Z}$-basis for $\mathcal{O}_{K_0}$.

Det bemærkes nu at

$$\mathrm{Gal}(K_0/\mathbb{Q}) = \{\sigma_j : \zeta+\zeta^{-1} \mapsto \zeta^j+\zeta^{-j},\ 1 \le j \le \tfrac{\ell-1}{2}\},$$

således at $\omega_1, \ldots, \omega_{\frac{\ell-1}{2}}$ er indbyrdes konjugerede.

Specielt er derfor

$$(*) \qquad S(\omega_1) = \cdots = S(\omega_{\frac{\ell-1}{2}}),$$

hvor $S = S_{K_0/\mathbb{Q}}$. Da minimalpolynomiet for ζ er

$$\Phi_\ell(x) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1,$$

er indvidere

$$(**) \qquad \omega_1 + \cdots + \omega_{\frac{l-1}{2}} + 1 = 0 .$$

Af (*) og (**) følger derfor

$$S(\omega_j) = -\frac{2}{l-1}\, S(1) = -1 \quad \text{for } 1 \le j \le \tfrac{l-1}{2}.$$

Da

$$\begin{aligned} \omega_r \omega_s &= (\zeta^r + \zeta^{-r})(\zeta^s + \zeta^{-s}) \\ &= \zeta^{r+s} + \zeta^{-(r+s)} + \zeta^{r-s} + \zeta^{-(r-s)}, \end{aligned}$$

er derfor for $1 \le r, s \le \frac{l-1}{2}$:

$$S(\omega_r \omega_s) = \begin{cases} -2 & \text{for } r \neq s \\ l-2 & \text{for } r = s \end{cases}.$$

Af det foregående fremgår nu, at diskriminanten d_0 for K_0 (over $\mathbb{Q}$) er givet ved

$$d_0 = D(\omega_1, \cdots, \omega_{\frac{l-1}{2}}) = \det \left(S(\omega_r \omega_s) \right)_{r,s=1,\cdots,\frac{l-1}{2}}$$

$$= \det \begin{pmatrix} l-2 & -2 & \cdots & -2 \\ -2 & l-2 & \cdots & -2 \\ \vdots & \vdots & & \vdots \\ -2 & -2 & \cdots & l-2 \end{pmatrix} = l^{\frac{l-3}{2}},$$

idet vi benytter den bekendte formel (hvor matricen er $n \times n$):

$$\det \begin{pmatrix} a & b & \cdots & b \\ b & a & \cdots & b \\ \vdots & \vdots & & \vdots \\ b & b & \cdots & a \end{pmatrix} = (a + (n-1)b)(a-b)^{n-1}.$$

Bemærk, at vi for $l = 7$ finder $d_0 = 7^2 = 49$ i overensstemmelse med et resultat i eksempel 34.

Enste forgrenede primtal er derfor l selv. Da

$$l = \Phi_l(1) = \prod_{j=1}^{l-1} (1-\zeta^j) = \prod_{j=1}^{\frac{l-1}{2}} (1-\zeta^j)(1-\zeta^{-j})$$

$$= \prod_{j=1}^{\frac{l-1}{2}} (2 - 2\cos 2\pi j/l),$$

og

$$2 - 2\cos 2\pi j/l = \sigma_j (2 - 2\cos 2\pi/l), \ \sigma_j \in Gal(K_0/\mathbb{Q}),$$

kan l i O_{K_0} skrives som produkt af elementer $2 - 2\cos 2\pi j/l$, $1 \leq j \leq \frac{l-1}{2}$, som alle har norm $= l$.

Da

$$\frac{1-\zeta^j}{1-\zeta} \in O_K^*, \text{ for alle } j = 1, \dots, l-1,$$

og $O_{K_0}^* = O_K^* \cap K_0$ følger det, at

$$\frac{2 - 2\cos 2\pi j/l}{2 - 2\cos 2\pi/l} = \frac{1-\zeta^j}{1-\zeta} \cdot \text{konj}\left(\frac{1-\zeta^j}{1-\zeta}\right) \in O_{K_0}^*$$

for $j = 1, \dots, \frac{l-1}{2}$. Følgelig er

$$l O_{K_0} = (\mu)^{\frac{l-1}{2}}, \qquad \mu = 2 - 2\cos 2\pi/l,$$

og for primtallet l er altså

$$e_l^0 = \frac{l-1}{2}, \quad f_l^0 = g_l^0 = 1.$$

Lad nu p være et primtal $\neq l$. Da er

$$e_p^\circ = 1, \quad f_p^\circ \cdot g_p^\circ = \frac{l-1}{2},$$

og vi påstår, at

$$f_p^\circ = \min \{ r \in \mathbb{N} \mid p^r \equiv \pm 1 \pmod{l} \}.$$

Da Frobeniusautomorfien $\sigma = \left(\frac{K}{p}\right)$, givet ved $\zeta \mapsto \zeta^p$, opfylder

$$\sigma(x) \equiv x^p \pmod{p} \text{ for alle } x \in \mathcal{O}_K,$$

vil σ's restriktion σ_0 til K_0 være givet ved $\zeta + \zeta^{-1} \mapsto \zeta^p + \zeta^{-p}$. Der gælder derfor specielt

$$\sigma_0(x) \equiv x^p \pmod{p} \text{ for alle } x \in \mathcal{O}_{K_0},$$

dvs.

$$\left(\frac{K_0}{p}\right) = \sigma_0.$$

Da $\sigma_0 \in G_Z^\circ$ har orden f_p° gælder:

$$\begin{aligned} f_p^\circ &= \min \{ r \in \mathbb{N} \mid \sigma_0^r = id \} \\ &= \min \{ r \in \mathbb{N} \mid \zeta^{p^r} \in \{ \zeta, \zeta^{-1} \} \} \\ &= \min \{ r \in \mathbb{N} \mid p^r \equiv \pm 1 \pmod{l} \}, \end{aligned}$$

hvilket viser formlen for f_p°. Bemærk, at

$$f_p^\circ = f_p, \quad g_p^\circ = \tfrac{1}{2} g_p, \text{ hvis } f_p \text{ ulige},$$

$$f_p^\circ = \tfrac{1}{2} f_p, \quad g_p^\circ = g_p, \text{ hvis } f_p \text{ lige}.$$

Vi finder nu

$$(*) \qquad \zeta_{K_0}(s) = \prod_{p} \prod_{\mathfrak{Y} \mid p} (1 - N(\mathfrak{Y})^{-s})^{-1}$$

$$= \prod_{p} (1 - p^{f_p^0 s})^{-g_p^0}$$

$$= (1 - l^{-s})^{-1} \prod_{p \neq l} (1 - p^{-f_p^0 s})^{-\frac{l-1}{2 f_p^0}}.$$

På den anden side er

$$(**) \qquad \zeta(s) \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0,\ \chi \text{ lige}}} L(s, \chi) = \prod_{p} \left\{ (1 - p^{-s})^{-1} \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0,\ \chi \text{ lige}}} (1 - \chi(p) p^{-s})^{-1} \right\}.$$

Skrives

$$1 - p^{-f_p^0 s} = \prod_{j=0}^{f_p^0 - 1} (1 - \varepsilon_p^j p^{-s}),$$

hvor ε_p er en primitiv f_p^0'te enhedsrod fremgår det, at produkterne (*) og (**) for hvert primtal p indeholder præcis de samme Euler-faktorer. For $p = l$ er dette klart. For $p \neq l$ skal man indse, at

$$\{1\} \cup \{ \chi(p) \mid \chi \neq \chi_0,\ \chi \text{ lige} \}$$

præcis er samtlige f_p^0'te enhedsrødder, hver med multiplicitet $(l-1)/2 f_p^0$. Da $p^{f_p^0} \equiv \pm 1 \pmod{l}$ er for χ lige, $\chi(p^{f_p^0}) = 1$, dvs. $\chi(p)$ er nødvendigvis en f_p^0'te enhedsrod. På den anden side

definieres ved

$$\chi_j(p) = \varepsilon_p^j \quad , \quad 0 \leq j < f_p^\circ - 1 \, ,$$

en karakter på den cyklische undergruppe $\langle p \rangle \triangleleft G_\ell$, og hver af disse karakterer kan på $\ell-1/f_p$ måder udvides til en gruppekarakter på G_ℓ og dermed til en Dirichletkarakter modulo ℓ.

Hvis f_p er ulige er $f_p^\circ = f_p$, og præcis halvdelen af hver af disse udvidelser, dvs.

$$\frac{1}{2} \cdot \frac{\ell-1}{f_p} = \frac{\ell-1}{2f_p^\circ}$$

Dirichletkarakterer χ mod ℓ, med $\chi(p) = \varepsilon_p^j$ er lige.

Hvis f_p er lige er $2f_p^\circ = f_p$, og samtlige af hver af disse udvidelser, dvs.

$$\frac{\ell-1}{f_p} = \frac{\ell-1}{2f_p^\circ}$$

Dirichletkarakterer χ mod ℓ, med $\chi(p) = \varepsilon_p^j$ er lige.

Hermed er også formel (2) bevist. □

<u>Sætning 123.</u> For klassetallene h og h_0 for $K = \mathbb{Q}(\zeta)$, $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$, $\zeta = e^{2\pi i/\ell}$, ℓ ulige primtal, gælder:

$$h = \frac{\ell^{\frac{\ell}{2}}}{2^{m-1}\pi^m R} \prod_{\substack{\chi \bmod \ell \\ \chi \neq \chi_0}} L(1,\chi) \, ,$$

$$h_0 = \frac{\ell^{\frac{\ell-3}{4}}}{R} \prod_{\substack{\chi \bmod \ell \\ \chi \neq \chi_0, \, \chi \text{ lige}}} L(1,\chi) \, ,$$

hvor $m = \frac{\ell-1}{2}$ og R er regulatoren for K.

Bevis: Ifølge sætning 122 er

$$\lim_{s \to 1} (s-1)\, \zeta_K(s) = \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0}} L(1, \chi).$$

Da $r_1 = 0$, $r_2 = \frac{l-1}{2} = m$, $w = 2l$ (jvf. sætning 91) og $|d| = l^{l-2}$. Formlen for h følger nu af hovedsætningen.

Ifølge sætning 122 er

$$\lim_{s \to 1} (s-1)\, \zeta_{K_0}(s) = \prod_{\substack{\chi \bmod l \\ \chi \neq \chi_0,\ \chi \text{ lige}}} L(1, \chi).$$

I dette tilfælde er $r_1^0 = \frac{l-1}{2} = m$, $r_2^0 = 0$, $w_0 = 2$ og $d_0 = l^{\frac{l-3}{2}}$. Ifølge Kummers sætning (sætning 92) er enhver enhed i O_K^* en enhedsrod gange en reel enhed (i $O_{K_0}^*$). Heraf følger, at der i O_K^* findes et system af reelle fundamentalenheder $(\varepsilon_1, \dots, \varepsilon_{m-1})$. Dette system er da samtidig et sæt af fundamentalenheder for $O_{K_0}^*$. På grund af definitionen af regulatoren - hvor der er faktoren 2 ved de komplekse isomorfier - er følgelig $R = 2^{m-1} R_0$. Formlen for h_0 følger nu af hovedsætningen. □

Sætning 123 er af fundamental betydning for det fuldstændige bevis for Kummers sætning (sætning 94). Vi nøjes her med at skitsere hovedpunkterne i beviset. (Jvf. Borevich-Shafarevich: Number Theory).

1. Skrives $h = h_0 h^*$, bliver

$$h^* = \frac{l^{\frac{l+3}{4}}}{2^{m-1}\pi^m} \cdot \prod_{\substack{\chi \bmod l \\ \chi \text{ ulige}}} L(1,\chi).$$

Det kan vises, at $h^* \in \mathbb{N}$, idet den egentlige grund hertil er at h^* kan opfattes som et relativt klassetal for udvidelsen K/K_0. Da

$$L(1,\chi) = \frac{\pi i\, \tau(\chi)}{l^2} \sum_{c=1}^{l-1} \bar{\chi}(c)\, c \quad \text{for } \chi \text{ ulige},$$

af

$$|\tau(\chi)| = \sqrt{l},$$

omskrives formlen for h^* til

$$h^* = \frac{1}{(2l)^{m-1}} \prod_{\substack{\chi \bmod l \\ \chi \text{ ulige}}} \bar{\chi}(c)\, c \cdot \prod \left| \sum_{c=1}^{l-1} \ldots \right|$$

Formlen for h^* er derfor meget mere elementær end formlen for h_0.

2. Ud fra formlen for h^* ses, at

$$l \mid h^* \iff l \mid B_2 \cdot B_4 \cdot \ldots \cdot B_{l-3},$$

dvs. l går op i en af tællerne af de anførte Bernoullital.

3. Klassetallet h_0 er lig gruppeindexet $[E : E_0]$, hvor E er undergruppen af positive enheder i $O_{K_0}^*$, medens E_0 er undergruppen af $O_{K_0}^*$ frembragt af de såkaldte <u>cirkeldelingsenheder</u> (eng: "cyclotomic units"; tysk: "Kreiseinheiten"):

$$\theta_j = \frac{\sin j\pi/l}{\sin \pi/l} \quad , \quad 2 \leq j \leq \frac{l-1}{2} \text{ o.m.}$$

4. Ved p-adisk analyse vises, at

$$l \nmid h^* \implies l \nmid h_0 \quad \text{(og dermed } l \nmid h\text{)}.$$

Med andre ord:

l er et regulært primtal $\iff l \mid B_2 \cdot B_4 \cdot \cdots \cdot B_{l-3}$. +

5. "Kummers lemma": Lad l være et regulært primtal. Antag at $\varepsilon \in O_K^*$ $(K = \mathbb{Q}(e^{2\pi i/l}))$ i O_K er kongruent med et $c \in \mathbb{Z}$ modulo l. Da er ε l'te potensen af en enhed i O_K.

6. Ved brug af Kummers lemma vises (forholdsvis let) unløsbarheden af Fermats ligning

$$x^l + y^l = z^l$$

i andet tilfælde: $\gcd(x,y,z) = 1$, $l \mid xyz$, forudsat l er et regulært primtal.

Abelske udvidelser.

Hovedemnet i den såkaldte klasselegemeteori er at give en beskrivelse af samtlige abelske udvidelser K/k for et givet grundlegeme k. For absolut abelske udvidelser, dvs. $k = \mathbb{Q}$ gælder

Sætning 124. (Kronecker, Weber)
K er et absolut abelsk tallegeme, hvis og kun hvis K er dellegeme af et cirkeldelingslegeme $\mathbb{Q}(e^{2\pi i/m})$, $m \in \mathbb{N}$.

I mindre et tilfælde, nemlig for $k = \mathbb{Q}(\sqrt{d})$, $d < 0$ er det muligt helt eksplicit at angive samtlige abelske udvidelser K. Dette sker i teorien for "kompleks multiplikation". Et resultat af denne art blev - uden held - efterstræbt af Kronecker (Kroneckers "Liebster Jugendtraum"), men først vist meget senere af Weber, Fueter og Takagi.

Den generelle klasselegemeteori er udviklet i tidsrummet 1900 - 1940 af bl.a. Hilbert, Weber, Takagi, Artin, Furtwängler, Hasse og Chevalley. (Jvf. Cassels, Fröhlich: Algebraic Number Theory, 1967; specielt oversigtsartiklen af Hasse).

For ethvert absolut abelsk tallegeme K kan der på entydig måde knyttes en endelig gruppe $\mathfrak{X}$ af primitive Dirichletkarakterer med den egenskab, at

$$\zeta_K(s) = \prod_{\chi \in \mathfrak{X}} L(s, \chi).$$

Udover cirkeldelingslegemerne $\mathbb{Q}(\zeta)$, $\mathbb{Q}(\zeta + \zeta^{-1})$, hvor vi har vist en sådan produktfremstilling og angivet karaktergruppen $\mathfrak{X}$, ser vi at også $K = \mathbb{Q}(\sqrt{d})$ giver eksempler herpå med $\mathfrak{X} = \{\chi_0, \chi\}$, hvor χ_0 er hovedkarakteren modulo 1 og χ "Kroneckerkarakteren" hørende til $\mathbb{Q}(\sqrt{d})$.

Det er muligt meget vidtgående at beskrive talteoretiske egenskaber for absolut abelske tallegemer ud fra karaktergruppen $\mathfrak{X}$. Fx. gælder:

(i) $$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{X}.$$

(ii) Diskriminanten d for K er givet ved

$$d = \prod_{\chi \in \mathfrak{X}} \chi(-1) f(\chi),$$

hvor $f(\chi)$ er den minimale modulus for χ.

(iii) K's <u>modulus</u> ("Führer", "conductor") defineres ved

$$f = \operatorname*{lcm}_{\chi} f(\chi).$$

Der gælder, at f er det mindste naturlige tal for hvilket $K \subset \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/f}$.

(iv) For $p \nmid f$ (dvs. $p \nmid d$) er Frobenius automorfien $\left(\frac{K}{p}\right)$ induceret af Frobenius automorfien $\left(\frac{\mathbb{Q}(\zeta)}{p}\right) : \zeta \mapsto \zeta^p$ ved restriktion. Artinsymbolet $\left(\frac{K}{s}\right)$ defineres nu for $s \in \mathbb{N}$, $\gcd(s, f) = 1$, ved

$$\left(\frac{K}{s}\right) = \prod_{j=1}^{r} \left(\frac{K}{p_j}\right)^{\alpha_j}, \qquad s = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

$\left(\frac{K}{s}\right)$ afhænger kun af $s \pmod f$. Afbildningen $s \mapsto \left(\frac{K}{s}\right)$ er en homomorfi (isomorfi) af G_f på $\mathrm{Gal}(K/\mathbb{Q}) = G$.

Ved fortsættelsen

$$\chi\left(\left(\frac{K}{s}\right)\right) = \chi(s)$$

bliver karaktererne $\chi \in \mathfrak{X}$ lissledes defineret på G.

(v) For $p \nmid f$ gælder

$$p\mathcal{O}_K = \mathfrak{Y}_1 \cdots \mathfrak{Y}_{g_p}, \qquad N(\mathfrak{Y}_j) = f_p,$$

hvor $f_p g_p = [K : \mathbb{Q}] = |G|$.

f_p er ordenen af $\left(\frac{K}{p}\right) \in G$, og der gælder

$$f_p = \min\{ r \in \mathbb{N} \mid \chi(p^r) = 1 \text{ for alle } \chi \in \mathfrak{X} \}.$$

(vi) $$\zeta_K(s) = \prod_{\chi \in \mathfrak{X}} L(s, \chi), \qquad \mathrm{Re}\, s > 1.$$

—

I nyere tid er absolut abelske tallegemer med stort held studeret af især Hasse og Leopoldt. Et led i dette studium er anvendelsen af p-adiske L-funktioner (indført af Kubota-Leopoldt, 1964), der gør det muligt at opstille en p-adisk klassetalsformel i fuldstændig analogi med Dedekind's klassiske klassetalsformel (= hovedsætningen). Se i øvrigt: K. Iwasawa, Lectures on p-adic L-Functions, Princeton 1972.

Ved studiet af relative abelske hhv. galoiske udvidelser er det ikke tilstrækkeligt at betragte Dirichlet L-funktioner, men man må for at opnå lignende produkt fremstillinger for $\zeta_K(s) / \zeta_k(s)$ betragte Hecke L-funktioner hhv. Artin L-funktioner. Se: Cassels, Fröhlich, Algebraic Number Theory, 1967; specielt artiklen af Heilbronn, Zeta Functions and L-Functions, samt Tate (thesis), Fourier Analysis in Number Fields and Hecke's Zeta Functions.

Eksempel 54. Lad $[K : \mathbb{Q}] = 3$, dvs K er et kubisk tallegeme, og lad $\overline{K}$ være K's normale afslutning i $\mathbb{C}$. Da er enten $[\overline{K} : \mathbb{Q}] = 6$ og $\mathrm{Gal}(\overline{K}/\mathbb{Q}) \cong S_3$ eller $\overline{K} = K$ og $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3$.

Øvelse. Vis, at der findes præcis et cyklisk kubisk legeme i hvert af tilfældene $f = 7, 9, 13$. Angiv i hvert tilfælde diskriminanten og en definerende ligning for legemet.

Øvelse. Vis, at der findes præcis to cykliske kubiske legemer med $f = 63$. Angiv diskriminanterne

Øvelse. Vis, at der ikke findes noget cyklisk kubisk legeme med $f = 21$.

Bevis for hovedsætningen: Vi skal med de gængse betegnelser vise

$$(1) \qquad \lim_{s \to 1} (s-1)\, \zeta_K(s) = h\kappa,$$

hvor

$$(2) \qquad \kappa = \frac{2^{r_1+r_2}\, \pi^{r_2}\, R}{w \sqrt{|d|}}.$$

I virkeligheden vil vi dog vise lidt mindre, nemlig

$$(1^+) \qquad \lim_{s \to 1^+} (s-1)\, \zeta_K(s) = h\kappa.$$

Derimod vil vi ikke vise, at $\zeta_K(s)$ bortset fra en pol af første orden for $s = 1$ er holomorf i $\mathbb{C}$. I tilfælde af at K er absolut abelsk, følger det dog af produktfremstillingen

$$\zeta_K(s) = \prod_{\chi \in \mathfrak{X}} L(s, \chi),$$

at $\zeta_K(s)$ bortset fra en pol for $s = 1$ i det mindste er holomorf for $\operatorname{Re} s > 0$.

I det følgende vil den variable $s \in]1, \infty[$. Vi skriver nu

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$$

$$= \sum_{C} f(s, C),$$

hvor vi for hver idealklasse C i klassegruppen H skriver

$$f(s, C) = \sum_{\mathfrak{a} \in C} N(\mathfrak{a})^{-s}, \tag{3}$$

idet det overalt er underforstået, at $\mathfrak{a} \neq (0)$ er et helt ideal i $\mathcal{O}_K$. Det bemærkes, at rækken i (3) for $s > 1$ er delrække af en konvergent række med positive led og derfor selv konvergent. Vi vil vise, at

$$\lim_{s \to 1+} (s-1) f(s, C) = \kappa \tag{4}$$

uafhængigt af $C \in H$. Da $|H| = h$ følger (1^+) derfor af (4).

Vi vælger nu et fast helt ideal $\mathfrak{a}' \in C^{-1}$. Da $\mathfrak{a}\mathfrak{a}' \sim (1)$ er

$$\mathfrak{a} \in C \iff \mathfrak{a} = \frac{(\alpha)}{\mathfrak{a}'}, \qquad \alpha \in \mathfrak{a}',$$

idet

$$\mathfrak{a}' \mid (\alpha) \iff (\alpha) \subset \mathfrak{a}' \iff \alpha \in \mathfrak{a}'.$$

Vi har følgelig

$$f(s, C) = N(\mathfrak{a}')^s \sum_{(\alpha) \subset \mathfrak{a}'} N((\alpha))^{-s}$$

eller

$$(5) \qquad f(s, C) = N(\mathfrak{a}')^s \sum_{\alpha \in \mathfrak{a}'}{}' |N(\alpha)|^{-s},$$

hvor $\sum'$ angiver, at der i hver klasse af associerede elementer i $\mathfrak{a}'$ (bortset fra nulklassen) skal vælges præcis et α.

Til dette formål benyttes de tidligere - i forbindelse med beviset for Dirichlets enhedssætning - indførte afbildninger φ og l:

$$\varphi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

defineret ved

$$\varphi(\alpha) = (\sigma_1(\alpha), \cdots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \cdots, \sigma_{r_1+r_2}(\alpha)),$$

og

$$l : (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^* \to \mathbb{R}^{r_1+r_2}$$

defineret ved

$$x = (x_1, \cdots, x_{r_1+r_2}) \mapsto l(x) = \left(\ln|x_1|, \cdots, \ln|x_{r_1}|, 2\ln|x_{r_1+1}|, \cdots, 2\ln|x_{r_1+r_2}|\right).$$

Vi minder om, at O_K^* virker på $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ ved at

$$(\varepsilon, x) \mapsto \varphi(\varepsilon) \cdot x ,$$

hvor

$$\varphi(\varepsilon) \cdot x = (\sigma_1(\varepsilon) x_1, \cdots, \sigma_{r_1+r_2}(\varepsilon) x_{r_1+r_2}).$$

Vælg nu et system $\{\varepsilon_1, \cdots, \varepsilon_r, \ r = r_1 + r_2 - 1\}$ af fundamentalenheder i O_K^*, og definér $\{e, e_1, \cdots, e_r\}$ ved

$$e = (\underbrace{1, \cdots, 1}_{r_1}, \underbrace{2, \cdots, 2}_{r_2}), \quad e_j = l \circ \varphi(\varepsilon_j), \ 1 \leq j \leq r.$$

Vi har tidligere vist, at

$$\operatorname{span}_{\mathbb{R}}(e_1, \cdots, e_r) = \Pi = \{(\lambda_1, \cdots, \lambda_{r_1+r_2}) \mid \sum_1^{r_1+r_2} \lambda_j = 0\},$$

og da $e \notin \Pi$ er derfor $(e, e_1, \cdots, e_r)$ en $\mathbb{R}$-basis for $\mathbb{R}^{r_1+r_2}$. Vi sætter

$$\mathcal{P} = \{\xi e + \xi_1 e_1 + \cdots + \xi_r e_r \mid \xi \in \mathbb{R}, \ \xi_j \in [0, 1[\text{ for } 1 \leq j \leq r\}$$

og vi definerer nu $X \subset (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^*$ ved

$$x \in X \overset{\text{def}}{\iff} \begin{cases} l(x) \in \mathcal{P} \\ \arg x_1 \in [0, \frac{2\pi}{w}[\end{cases}.$$

Endelig defineres

$$X_0 = X \cap \{x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^* \mid |N(x)| \leq i\}.$$

Vi påstår at følgende gælder:

(i) X er en kegle i $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^*$ med toppunkt 0;

(ii) X er et fundamentalområde for virkningen af O_K^* på $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^*$;

(iii) $\mathrm{vol}(X_0) = \dfrac{2^{r_1} \pi^{r_2} R}{w}$.

For vi viser dette, vil illustrere situationen for $[K : \mathbb{Q}] = 2$.

<u>$r_1 = 0, r_2 = 1$:</u> (K imaginær kvadratisk)

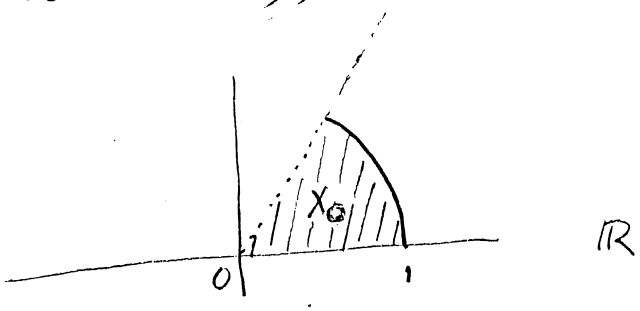
Da er

$$(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^* = \mathbb{C}^*,$$

og

$$X = \{ x_1 \in \mathbb{C}^* \mid 0 \leq \arg x_1 < \tfrac{2\pi}{w} \}.$$

Fx er for $K = \mathbb{Q}(\sqrt{-3})$, $w = 6$;



dvs. X er et vinkelrum af størrelse $\frac{2\pi}{6}$. Det er klart, at X er et fundamentalområde for virkningen af $O_K^* = \{ e^{\frac{2\pi i}{6}\nu} \mid 1 \leq \nu \leq 6 \}$.

Endvidere er $\mathrm{vol}(X_0) = \frac{\pi}{6}$; overensstemmelse med (iii), da $r_1 = 0$, $r_2 = 1$, $R = 1$, $w = 6$.

$r_1 = 2$, $r_2 = 0$: (K reel kvadratisk)

Da er

$$\left(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}\right)^* = \left(\mathbb{R}^2\right)^* = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 x_2 = N(x) \neq 0\}.$$

Endvidere er $r = 1$ og

$$e = (1, 1), \quad e_1 = (\ln \varepsilon_1, -\ln \varepsilon_1),$$

hvor $\varepsilon_1 > 1$ er fundamentalenhed for O_K^*.

Da

$$(\alpha_1, \alpha_2) = \frac{\alpha_1 + \alpha_2}{2} e + \frac{\alpha_1 - \alpha_2}{2 \ln \varepsilon_1} e_1,$$

er

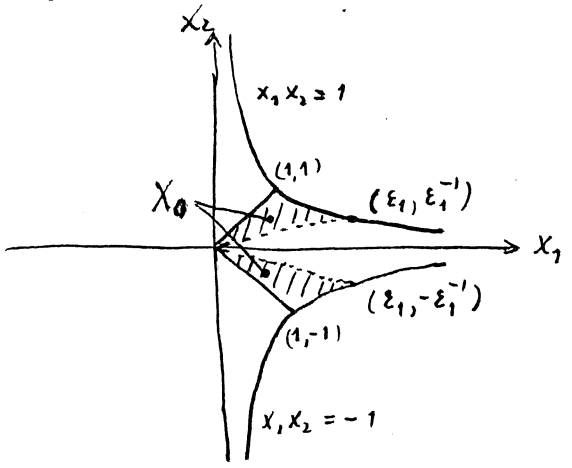
$$l(x) = (\ln |x_1|, \ln |x_2|) \in \mathcal{P}$$

$$\Leftrightarrow \quad \frac{\ln \left|\frac{x_1}{x_2}\right|}{\ln \varepsilon_1^2} \in [0, 1[$$

$$\Leftrightarrow \quad 1 \leq \left|\frac{x_1}{x_2}\right| < \varepsilon_1^2.$$

Da $w = 2$ er derfor

$$X = \left\{ x = (x_1, x_2) \in \mathbb{R}^2 \mid x_1 > 0, \ 1 \leq \frac{x_1}{|x_2|} < \varepsilon_1^2 \right\}.$$



Det er klart, at X er et fundamentalområde for virkningen af

$$O_K^* = \{ \pm \varepsilon_1^{n_1} \mid n_1 \in \mathbb{Z} \}.$$

Endvidere er

$$\begin{aligned} \mathrm{vol}(X_0) &= 2\left(\int_0^1 t\,dt + \int_1^{\varepsilon_1} \frac{dt}{t} - \int_0^{\varepsilon_1} \frac{t}{\varepsilon_1^2}\,dt \right) \\ &= 2\left(\tfrac{1}{2} + \ln \varepsilon_1 - \tfrac{1}{2} \right) \\ &= 2 \ln \varepsilon_1, \end{aligned}$$

hvilket er i overensstemmelse med (iii), da $r_1 = 2$, $r_2 = 0$, $R = \ln \varepsilon_1$, $w = 2$.

Vi vender nu tilbage til beviset for egenskaberne (i), (ii), (iii):

(i) Vi skal vise, at

$$x \in X,\ t > 0 \Rightarrow tx \in X.$$

Da

$$\arg(tx)_1 = \arg tx_1 = \arg x_1,$$

og

$$\begin{aligned} l(tx) &= (\ln t + \ln|x_1|, \cdots, 2\ln t + 2\ln|x_{r_1+1}|, \cdots) \\ &= (\ln t)\, e + l(x), \end{aligned}$$

er dette imidlertid klart.

(ii) Vi skal vise, at der til et givet $y \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^*$ findes præcis et par $(\varepsilon, x) \in O_K^* \times X$ så

$$(*) \qquad \varphi(\varepsilon) \cdot x = y.$$

Antag, at (*) gælder. Ved at anvende afbildningen l fås:

$$(**) \qquad l(\varphi(\varepsilon)) + l(x) = l(y).$$

Da

$$l(\varphi(\varepsilon)) \in \Pi_0 = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n, \quad l(x) \in \mathcal{P},$$

og $\mathcal{P}$ er et fundamentalområde for virkningen af $(\Pi_0, +)$ på $\mathbb{R}^{r_1+r_2}$, fastlægger (**) entydigt værdien af $l(\varphi(\varepsilon))$, dvs. ε er bestemt på nær en faktor ζ, som er en w'te enhedsrod. Da $[0, \frac{2\pi}{w}[$ er et fundamentalområde for virkningen af gruppen af enhedsrødder i O_K^* på mængden af argumenter $= \mathbb{R} \pmod{2\pi}$, er faktoren ζ entydigt bestemt ved at $\arg x_1 \in [0, \frac{2\pi}{w}[$. Denne analyse viser at der højst findes et par (ε, x) som tilfredsstiller (*). Omvendt bestemmes imidlertid ved den anvendte fremgangsmåde et sådant par.

(iii) Det fremgår af (ii), at mængderne

$$X_j = \varphi(e^{\frac{2\pi i j}{w}}) \cdot X_0, \quad 0 \le j < w,$$

er disjunkte, og at

$$T = \bigcup_{j=0}^{w-1} X_j = \{x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^* \mid l(x) \in \mathcal{P}, |N(x)| \le 1\}.$$

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 $x \mapsto \varphi(e^{\frac{2\pi i j}{w}}) \cdot x$ en volumenbevarende (under Lebesguemål = vol) afbildning af $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^*$.

Følgelig er

$$vol(X_0) = \frac{1}{w}\, vol(T).$$

Da T er symmetrisk mht. koordinatene $x_1, \dots, x_{r_1}$ er

$$vol(X_0) = \frac{2^{r_1}}{w}\, vol(T_+),$$

hvor

$$T_+ = \left\{ x \in (\mathbb{R}_+^{r_1} \times \mathbb{C}^{r_2})^* \mid l(x) \in \mathcal{P},\ N(x) \leqq 1 \right\}.$$

For at vise (iii) skal vi derfor blot godtgøre, at

$$(***) \qquad vol(T_+) = \pi^{r_2} R.$$

Herfil skiftes fra retvinklede koordinater

$$x_1, \dots, x_{r_1}, x_{r_1+1} = x'_{r_1+1} + i\, x''_{r_1+1}, \dots, x_{r_1+r_2} = x'_{r_1+r_2} + i\, x''_{r_1+r_2}$$

til polære koordinater

$$\varrho_1, \dots, \varrho_{r_1}, \varrho_{r_1+1}, \varphi_1, \dots, \varrho_{r_1+r_2}, \varphi_{r_2},$$

hvor koordinatskiftet er givet ved

$$\begin{cases} x_j = \varrho_j & \text{for } 1 \leqq j \leqq r_1 \\ x'_{r_1+j} = \varrho_{r_1+j} \cos\varphi_j & \text{for } 1 \leqq j \leqq r_2 \\ x''_{r_1+j} = \varrho_{r_1+j} \sin\varphi_j & \text{for } 1 \leqq j \leqq r_2 \end{cases}.$$

Volumenfaktoren (= absolutværdien af Jacobideterminanten) ved beregning af volumen i polære koordinater er derfor

$$\varrho_{r_1+1} \cdots \varrho_{r_1+r_2}.$$

For et vilkårligt $x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^*$ er $l(x)$ mht. den naturlige basis for $\mathbb{R}^{r_1+r_2}$

$$l(x) = (l_1(x), \cdots, l_{r_1+r_2}(x)),$$

og hvor ifølge definition af $l(x)$ og $N(x)$:

$$\sum_{j=1}^{r_1+r_2} l_j(x) = \ln |N(x)|.$$

På den anden side er

$$l(x) = \xi e + \xi_1 e_1 + \cdots + \xi_r e_r,$$

hvor $e, e_1, \cdots, e_r$ udtrykt ved den naturlige basis er

$$e = (1, \cdots, 1, 2, \cdots, 2)$$

$$e_1 = (\ln|\sigma_1(\varepsilon_1)|, \cdots, \ln|\sigma_{r_1}(\varepsilon_1)|, 2\ln|\sigma_{r_1+1}(\varepsilon_1)|, \cdots, 2\ln|\sigma_{r_1+r_2}(\varepsilon_1)|)$$

$$\vdots$$

$$e_r = (\ln|\sigma_1(\varepsilon_r)|, \cdots, \ln|\sigma_{r_1}(\varepsilon_r)|, 2\ln|\sigma_{r_1+1}(\varepsilon_r)|, \cdots, 2\ln|\sigma_{r_1+r_2}(\varepsilon_r)|)$$

Altså er

$$\sum_{j=1}^{r_1+r_2} l_j(x) = (r_1+2r_2)\xi + \sum_{j=1}^{r} \xi_j \ln|N(\varepsilon_j)| = n\xi.$$

Ved at sammenholde de to udtryk for $\sum l_j(x)$ fås altså

$$\xi = \frac{1}{n} \ln|N(x)|.$$

Vi finder derfor

$$\mathrm{vol}(T_+) = \rho_{r_1+1} \cdots \rho_{r_1+r_2} (2\pi)^{r_2} \int_{\Omega} d\rho_1 \cdots d\rho_{r_1+r_2},$$

hvor

$$(\rho_1, \cdots, \rho_{r_1+r_2}) \in \Omega \subset \mathbb{R}_+^{r_1+r_2} \iff \begin{cases} \rho_1 \cdots \rho_{r_1} (\rho_{r_1+1} \cdots \rho_{r_1+r_2})^2 \leqq 1 \\ (\ln\rho_1, \cdots, \ln\rho_{r_1}, 2\ln\rho_{r_1+1}, \cdots, 2\ln\rho_{r_1+r_2}) \\ = \xi e + \xi_1 e_1 + \cdots + \xi_r e_r, \text{ hvor} \\ \xi = \frac{1}{n} \ln \rho_1 \cdots \rho_{r_1} \rho_{r_1+1}^2 \cdots \rho_{r_1+r_2}^2, \ \xi_j \in [0,1[\end{cases}$$

Vi kan yderligere simplificere udtrykket for $\mathrm{vol}(T_+)$ ved at sætte

$$\tau_j = \begin{cases} \rho_j & \text{for } 1 \leqq j \leqq r_1 \\ \rho_j^2 & \text{for } r_1 < j \leqq r_1 + r_2 . \end{cases}$$

Vi finder nemlig herved

$$\mathrm{vol}(T_+) = \pi^{r_2} \int_{\Omega'} d\tau_1 \cdots d\tau_{r_1+r_2} ,$$

hvor området Ω' er bestemt ved

$$(\tau_1, \dots, \tau_{r_1+r_2}) \in \Omega' \subset \mathbb{R}_+^{r_1+r_2} \Leftrightarrow \begin{cases} (\ln \tau_1, \dots, \ln \tau_{r_1+r_2}) = \\ \xi e + \xi_1 e_1 + \cdots + \xi_r e_r , \\ \xi \leqq 0 , \quad \xi_j \in [0,1[\text{ for } 1 \leqq j \leqq r \end{cases}$$

Benyttes parameteren

$$\xi_0 = e^{n\xi} = \tau_1 \cdots \tau_{r_1+r_2} , \qquad \xi_0 \in]0,1]$$

i stedet for ξ, $\xi \leqq 0$, fås endelig

$$\mathrm{vol}(T_+) = \pi^{r_2} \int_{]0,1[^{r_1+r_2}} \left\| \frac{\partial \tau}{\partial \xi} \right\| d\xi_0 \cdots d\xi_r ,$$

hvor $\left\| \frac{\partial \tau}{\partial \xi} \right\|$ er absolutværdien af funktionaldeterminanten for afbildningen $(\xi_0, \dots, \xi_r) \mapsto (\tau_1, \dots, \tau_{r_1+r_2})$ givet ved

$$\ln \tau_k = \left(\frac{1}{n} \ln \xi_0 + \sum_{j=1}^{r} \xi_j \ln \sigma_k(\varepsilon_j) \right) f_k ,$$

hvor $f_k = 1$ for $1 \leqq k \leqq r_1$, $f_k = 2$ for $r_1 < k \leqq r_1 + r_2$.

Følgelig er

$$\frac{1}{\tau_1 \cdots \tau_{r_1+r_2}} \left\| \frac{\partial \tau}{\partial \xi} \right\| = \left\| \begin{matrix} \frac{1}{n\xi_0} & \cdots & \frac{1}{n\xi_0} & \frac{2}{n\xi_0} & \cdots & \frac{2}{n\xi_0} \\ \ln|\sigma_1(\varepsilon_1)| & \cdots & \ln|\sigma_{r_1}(\varepsilon_1)| & 2\ln|\sigma_{r_1+1}(\varepsilon_1)| & \cdots & 2\ln|\sigma_{r_1+r_2}(\varepsilon_1)| \\ \vdots & & & & & \\ \ln|\sigma_1(\varepsilon_r)| & \cdots & \ln|\sigma_{r_1}(\varepsilon_r)| & 2\ln|\sigma_{r_1+1}(\varepsilon_r)| & \cdots & 2\ln|\sigma_{r_1+r_2}(\varepsilon_r)| \end{matrix} \right\| .$$

I determinanten sættes $\frac{1}{n s_0}$ uden for, hvorefter alle øvrige søjler adderes til 1. den første søjle, og determinanten udvikles efter første søjle, som bortset fra $n = r_1 + 2r_2$ øverst består af lutter nuller. Hermed fås

$$\left\| \frac{\partial T}{\partial s} \right\| = T_1 \cdots T_{r_1+r_2} \cdot \frac{1}{n s_0} \cdot n \cdot R = R .$$

Følgelig er

$$\mathrm{vol}(T_+) = \pi^{r_2} R \int_{J_0 \times \Sigma^{r_1+r_2}} ds_0 \cdots ds_n = \pi^{r_2} R .$$

Vi har hermed gradtgjort (***), og dermed (2.i).

Vi kan nu omskrive formel (5) til

$$(6) \qquad f(s, C) = N(\mathfrak{O}')^s \sum_{x \in M \cap X} |N(x)|^{-s} ,$$

hvor $M = \varphi(\mathfrak{O}')$ er indlejringen af $\mathfrak{O}'$ 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

$$d(\Lambda) = 2^{-r_2} \sqrt{|d|} .$$

Nøjagtig samme ræsonnement viser, at $M = \varphi(\mathfrak{O}')$ er et fuldt gitter i $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ med

$$d(M) = 2^{-r_2} |D(\omega_1, \cdots, \omega_n)|^{1/2} ,$$

hvor $(\omega_1, \cdots, \omega_n)$ er en $\mathbb{Z}$-basis for $\mathfrak{O}'$. Da (jfr. sætning 52)

$$|D(\omega_1, \cdots, \omega_n)| = N(\mathfrak{O}')^2 |d| ,$$

er derfor

$$d(M) = 2^{-r_2} N(\mathfrak{o}') \sqrt{|d|}.$$

Vi vil skulle vise, at

$$(7) \qquad \lim_{s \to 1+} (s-1) \sum_{x \in M \cap X} |N(x)|^{-s} = \frac{\mathrm{vol}(X_0)}{d(M)} = \frac{\kappa}{N(\mathfrak{o}')}.$$

idet det bemærkes, at (6) og (7) tilsammen viser (4) og dermed hovedsætningen.

Lad for $t > 1$:

$$N(t) = |M \cap t X_0| = |\tfrac{1}{t} M \cap X_0|,$$

dvs. $N(t)$ er antallet af gitterpunkter i $M \cap X$ med $|N(x)| \leqq t^n$ eller $|N(x)|^{1/n} \leqq t$.

Da

$$\mathrm{vol}(X_0) = \lim_{t \to \infty} N(t) \cdot d(\tfrac{1}{t} M)$$

$$= d(M) \cdot \lim_{t \to \infty} \frac{N(t)}{t^n}$$

er

$$\lim_{t \to \infty} \frac{N(t)}{t^n} = \frac{\mathrm{vol}(X_0)}{d(M)}.$$

Lad nu $x_1, x_2, \ldots$ være samtlige punkter i $M \cap X$ ordnet efter voksende værdier af $|N(x)|$.

Sæt $t_k = |N(x_k)|^{1/n}$. Det følger da af definitionen på $N(t)$, at der for ethvert $\varepsilon > 0$ gælder:

$$N(t_k - \varepsilon) < k \leqq N(t_k),$$

hvoraf

$$\frac{N(t_k - \varepsilon)}{t_k^n} < \frac{k}{t_k^n} \leqq \frac{N(t_k)}{t_k^n}.$$

Da

$$\lim_{k \to \infty} \frac{N(t_k)}{t_k^n} = \frac{\mathrm{vol}(X_0)}{d(M)}$$

findes der for ethvert $\varepsilon > 0$ et $k_0 = k_0(\varepsilon)$ så

$$(1-\varepsilon)\frac{\mathrm{vol}(X_0)}{d(M)} < \frac{k}{t_k^n} < (1+\varepsilon)\frac{\mathrm{vol}(X_0)}{d(M)} \quad \text{for alle } k > k_0.$$

Da $t_k = |N(x_k)|^{1/n}$ følger heraf for $k > k_0$; $s > 1$:

$$(1-\varepsilon)^s \left(\frac{\mathrm{vol}(X_0)}{d(M)}\right)^s \frac{1}{k^s} < \frac{1}{|N(x_k)|^s} < (1+\varepsilon)^s \left(\frac{\mathrm{vol}(X_0)}{d(M)}\right)^s \frac{1}{k^s}.$$

Da

$$\lim_{s \to 1^+} (s-1) \sum_{k > k_0} \frac{1}{k^s} = 1,$$

følger umiddelbart

$$(1-\varepsilon)\,\frac{\mathrm{vrl}(X_0)}{d(M)} \leq \liminf_{s\to 1+} (s-1)\sum_k \frac{1}{|N(x_k)|^s}$$

$$\leq \limsup_{s\to 1+} (s-1)\sum_k \frac{1}{|N(x_k)|^s} \leq (1+\varepsilon)\,\frac{\mathrm{vrl}(X_0)}{d(M)}.$$

Da $\varepsilon > 0$ er vilkårlig gælder

$$\lim_{s\to 1+} (s-1)\sum_k \frac{1}{|N(x_k)|^s} = \frac{\mathrm{vrl}(X_0)}{d(M)}. \qquad \square$$

Funktionalligninger for $\zeta_K(s)$ og $L(s,\chi)$.

Vi skal afslutte omtale funktionalligningerne for $\zeta_K(s)$ og $L(s,\chi)$, som i øvrigt har nøje sammenhæng med udvidelsen af de omhandlede funktioner til hele funktioner i $\mathbb{C}$ på nær højst en pol af 1. orden for $s = 1$.

For enkelhedens skyld nøjes vi med tilfældet K absolut abelsk. Den gælder da, at

$$\begin{cases} d^{\frac{s}{2}} \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^n \zeta_K(s) & \text{for } K \text{ reel},\ [K:\mathbb{Q}] = n \\ d^{\frac{s}{2}} \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^{n_0} \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s+1}{2}\right)\right)^{n_0} \zeta_K(s) & \text{for } K \text{ imag},\ [K:\mathbb{Q}] = 2n_0 \end{cases}$$

er invariant ved afbildningen $s \mapsto 1-s$.

For en primitiv karakter χ gælder tilsvarende, at

$$\begin{cases} f(\chi)^{\frac{s}{2}} \left(\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)\right) L(s,\chi) & \text{for } \chi \text{ lige} \\ f(\chi)^{\frac{s}{2}} \left(\pi^{-\frac{s}{2}} \Gamma\left(\frac{s+1}{2}\right)\right) L(s,\chi) & \text{for } \chi \text{ ulige} \end{cases}$$

får faktoren

$$\frac{\sqrt{\chi(-1)\cdot f(\chi)}}{\tau(\chi)}$$

ved afbildningen $s \mapsto 1-s$, $\chi \mapsto \overline{\chi}$.

Funktionalligningen for $\zeta_K(s)$ for et vilkårligt algebraisk tallegeme K er først opstillet af E. Hecke (1917). (Se fx Landau [23]).

Kapitel 5. Den gaussiske teori for binære kvadratiske former.

Vi betragter binære kvadratiske former

$$f = (a,b,c), \qquad a,b,c \in \mathbb{Z},$$

givet ved

$$(x,y) \mapsto f(x,y) = ax^2 + bxy + cy^2.$$

Formen f siges at <u>repræsentere</u> et helt tal m, hvis der findes $(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ med $f(x,y) = m$, specielt siges f at repræsentere m <u>egentligt</u>, dersom x, y kan vælges indbyrdes primiske. Formen f kaldes <u>primitiv</u>, dersom $\gcd(a,b,c) = 1$. Til formen $f = (a,b,c)$ knyttes matricen

$$\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} = A = A(f)$$

bestemt ved at

$$f(x,y) = (x\ y)\, A \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{og} \quad A^T = A.$$

Der gælder øjensynlig for formens diskriminant $d = d(f)$

$$d(f) = b^2 - 4ac = -4 \det A(f).$$

To former f, g siges at være egentlig ækvivalente, $f \approx g$, hvis der findes en matrix $M \in SL_2(\mathbb{Z})$, altså en heltalsmatrix med determinant $= +1$ så

$$A(g) = M^T A(f)\, M.$$

Dette er ensbetydende med at sige at

$$g(x,y) = f(\alpha x + \beta y,\ \gamma x + \delta y),$$

når

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Det fremgår, at

$$f \approx g \implies d(f) = d(g).$$

Da

$$(x,y) \in \mathbb{Z}^2 \iff (\alpha x + \beta y,\ \gamma x + \delta y) \in \mathbb{Z}^2,$$

og $\quad \gcd(x,y) = 1 \iff \gcd(\alpha x + \beta y,\ \gamma x + \delta y) = 1,$

repræsenterer egentlig ækvivalente former de samme tal $m \in \mathbb{Z}$, og de samme tal egentligt.

Det er derfor naturligt for et givet $d \in \mathbb{Z}$, at betragte alle egentlige ækvivalensklasser af former f med $d(f) = d$. For at overskue disse ækvivalensklasser indføres begrebet <u>reduceret form</u>, som for <u>definite former</u> ($d < 0$) indførtes af Lagrange og for <u>indefinite former</u> ($d > 0$) af Gauss. Former med diskriminant $d = m^2$, $m \in \mathbb{Z}$, viser sig at være uinteressante for vort formål, og vi vil i det følgende se bort fra denne mulighed. Endvidere er det tilstrækkeligt for $d < 0$, at betragte <u>positivt definite former</u> ($d < 0$; $a > 0$).

Formen $f = (a,b,c)$ har rødderne

$$\xi, \eta = \frac{-b \pm \sqrt{d}}{2a},$$

hvor vi for $d < 0$ vælger $\xi = \frac{-b+\sqrt{d}}{2a}$ med $\operatorname{Im} \xi > 0$,

og for $d > 0$ vælger $\xi = \dfrac{-b+\sqrt{d}}{2a}$.

Definition. $f = (a,b,c)$ siges at være reduceret, hvis

(i) $-a < b \leqq a \leqq c$ og $b \geqq 0$ hvis $a = c$

i tilfælde af at $d < 0$ (og $a > 0$), ækvivalent hermed er at

$$\zeta \in \Omega = \left\{ z = x+iy \;\middle|\; -\tfrac{1}{2} < x \leqq \tfrac{1}{2},\ |z| \geqq 1,\ \text{dog } x \geqq 0 \text{ for } |z| = 1 \right\},$$

hvor Ω er et fundamentalområde for $SL_2(\mathbb{Z})$'s virkning på den øvre halvplan.

(ii) $|\zeta| > 1$, $0 < |\eta| < 1$,

i tilfældet $d > 0$, hvor automatisk $\zeta\eta < 0$.

Der gælder nu:

Sætning 25. Enhver kvadratisk form f er egentlig ækvivalent med en reduceret form. Der findes kun endelig mange reducerede former med given diskriminant d.

Korollar. Klassetallet $h_+(d)$ af egentlige ækvivalensklasser af primitive former af diskriminant d er endeligt.

Bevis (for 2. del af sætningen):

(i) $d < 0$. Da er

$$d = b^2 - 4ac \leqq a^2 - 4a^2 = -3a^2,$$

altså

$$\boxed{0 \leqq |b| \leqq a \leqq \sqrt{\tfrac{-d}{3}}}.$$

Der er derfor kun endelig mange muligheder for (a,b) og dermed

for $f = (a, b, c)$, da $b^2 - 4ac = d$.

(ii) $d > 0$. Antag fx, at

$$\zeta = \frac{-b+\sqrt{d}}{2a} > 1 \quad , \quad \eta = \frac{-b-\sqrt{d}}{2a} \in]-1, 0[\, ;$$

da er

$$\zeta - \eta = \frac{\sqrt{d}}{a} > 1 \, , \text{ altså} \quad \boxed{0 < a < \sqrt{d}} \, .$$

Følgelig er

$$-b+\sqrt{d} > b+\sqrt{d} > 0 \, , \quad \text{altså} \quad \boxed{0 < -b < \sqrt{d}} \, .$$

Som ovenfor viser dette, at der kun er endelig mange muligheder for $f = (a, b, c)$. Generelt gælder: $\boxed{0 < |a| < \sqrt{d} \, , \; 0 < -b < \sqrt{d}}$.

<u>Eksempel 55.</u> For $d = -19$ er for en reduceret form

$$-a < b \leq a \leq c \quad \text{og} \quad a \leq \sqrt{\tfrac{19}{3}} < 3 \, .$$

Altså er $a = 1, 2$. Da $b^2 \equiv d \equiv 1 \; (2)$ er b ulige. Eneste muligheder for (a, b) er derfor $(1, 1)$, $(2, 1)$, $(2, -1)$. Imidlertid findes kun i første af disse tre tilfælde et $c \in \mathbb{Z}$ så $-19 = b^2 - 4ac$. Eneste reducerede form er derfor $f = (1, 1, 5)$. Følgelig er $h_+(-19) = 1$. (Jvf. eksempel 28).

<u>Eksempel 56.</u> For $d = -23$ er tilsvarende $a \leq \sqrt{\tfrac{23}{3}} < 3$. Som ovenfor er $(a, b) = (1, 1)$, $(2, 1)$, $(2, -1)$, som giver de tre reducerede former

$$f_1 = (1, 1, 6) \, , \quad f_2 = (2, 1, 3) \, , \quad f_2^- = (2, -1, 3) \, .$$

Disse tre former kan vises <u>ikke</u> at være egentlig ækvivalente, og følgelig er $h_+(-23) = 3$. (Jvf. eksempel 52).

Eksempel 57. For $d=-20$ er $a \leq \sqrt{\frac{20}{3}} < 3$, og $b^2 \equiv d \equiv 0 \ (2)$, dvs. b er lige. Eneste muligheder for (a,b) er derfor $(1,0)$, $(2,2)$ og $(2,0)$. Dette giver imidlertid kun de to muligheder

$$f_1 = (1,0,5), \quad f_2 = (2,2,3).$$

Da disse to former er egentlig inækvivalente er $h_+(20) = 2$. (Jvf. bemærkningen efter eksempel 47.)

Eksempel 58. For $d=12$ er $0 < -b < \sqrt{12} < 4$ og $b^2 \equiv d \equiv 0 \ (2)$, dvs. b er lige. Eneste mulighed for b er derfor $b=-2$. Derfor er

$$4ac = b^2 - d = -8, \text{ dvs. } ac = -2.$$

Dette giver mulighederne

$$f_1 = (1,-2,-2), \ f_2 = (-2,-2,1),$$

$$g_1 = (-1,-2,2), \ g_2 = (2,-2,-1),$$

som alle er reducerede. Det er let at se, at $f_1 \approx f_2$ og $g_1 \approx g_2$. Derimod er

$$f_1(x,y) = (x-y)^2 - 3xy \equiv 0,1 \pmod 3 \text{ for alle } x,y \in \mathbb{Z},$$

$$g_1(x,y) = -f_1(x,y) \equiv 0,-1 \pmod 3 \text{ for alle } x,y \in \mathbb{Z}.$$

Heraf følger, at $f_1 \not\approx g_1$, altså at $h_+(12) = 2$.

—

$p \equiv 1 \ (4) \Rightarrow \left(\frac{-1}{p}\right) = 1 \qquad z^2+1 = rp \Rightarrow (2z)^2 + 4 = 4rp \Rightarrow -4 = d(p,2z,r)$

$f \approx (1,0,1)$ som derfor repr. p.

Definition. To kvadratiske former f og g med diskriminant d siges at være genus ækvivalente, $f \approx\!\!\approx g$, dersom f og g repræsenterer primtal i præcis de samme primiske restklasser modulo $|d|$. (Det forlanges derimod ikke, at f og g repræsenterer de samme primtal). Ekvivalent hermed er (ifl. Hasse), at f og g har matricer $A(f)$ og $A(g)$, hvor

$$A(g) = M^T A(f) M, \qquad M \in SL_2(\mathbb{Z}).$$

Bemærkning. I eksempel 56 er $f_1 \approx f_2 \approx f_2^-$, men f_1 og f_2 repræsenterer ikke de samme primtal, idet f_1 ikke repræsenterer 2 og 3, hvad f_2 tydeligvis gør.

Sætning 126. For $d = d_0 d_1 \cdots d_g$, hvor betegnelserne er som i sætning 102, er der præcis 2^g genusækvivalensklasser af primitive kvadratiske former af diskriminant d.

Bevis: Gauss' bevisidé består i at indføre de ambige former $f = (a, b, c)$, dvs. former, hvor $f \approx f^- = (a, -b, c)$. $\square$

I klasserne af primitive kvadratiske former med given diskriminant d mht. en af ækvivalensrelationerne $\approx$ eller $\sim$ indfører Gauss en såkaldt komposition på følgende måde:

(i) Givet f, g primitive kvadratiske former af diskriminant d. Ved at erstatte f, g med ækvivalente (mht. $\approx$) kan

opnås, at

$$f = (a_1, b, a_2 c) \quad , \quad g = (a_2, b, a_1 c).$$

(ii) Man definerer

$$f * g = (a_1 a_2, b, c).$$

Det kan nu vises, at dette er en lovlig komposition af de to typer ækvivalensklasser, samt at der herved er defineret gruppekompositioner i de to tilfælde.

<u>Øvelse</u>. Lad (a, b, c) være en primitiv kvadratisk form af diskriminant $d = b^2 - 4ac$, som ikke er et kvadrattal. Vis, at $f_1 = (1, b, ac)$ repræsenterer et element i klassegruppen $H_+(d)$, og at $f = (a, b, c)$ og $f^- = (a, -b, c)$ repræsenterer inverse elementer.

—

Det kan vises, at der er en bijektiv korrespondance mellem klasser af egentligt ækvivalente hele idealer i $\mathbb{Q}(\sqrt{d})$ og klasser af egentligt ækvivalente primitive former af diskriminant d. (Jvf. fx. Cohn [7] eller Hecke [17].) Ved denne korrespondance svarer genusklasserne til hinanden. Specielt svarer til idoniske legemer $\mathbb{Q}(\sqrt{d})$, negative diskriminanter d for hvilke hver genusklasse af primitive kvadratiske former med diskriminant d kun indeholder en egentlig ækvivalensklasse. Sådanne "idoniske tal" d blev af Euler benyttet til at konstruere store primtal (ca 10^6), jvf. Dickson: Introd. to Theory of NOs.

Litteratur

1. T. M. Apostol: Introduction to Analytic Number Theory, 1976.
2. E. Artin, J. Tate: Class Field Theory, 1951-52.
3. A. Baker: Transcendental Number Theory, 1975.
4. Z.I. Borevich, I. R. Safarevich: Number Theory, 1966.
5. J.W.S. Cassels, A. Fröhlich (ed.): Algebraic Number Theory, 1967.
6. C. Chevalley: Class Field Theory, 1953-54.
7. H. Cohn: A Second Course in Number Theory, 1962.
8. H. Cohn: A Classical Invitation to Algebraic Numbers and Class Fields, 1978.
9. M. Deuring: Klassenkörpertheorie, 1965-66.
10. G.L. Dirichlet: Vorlesungen über Zahlentheorie (m. suppl. af R. Dedekind), 1871.
11. G.L. Dirichlet: Werke I, II, 1889, 1897.
12. M. Eichler: Introduction to the Theory of Algebraic Numbers and Functions, 1963.
13. C.F. Gauss: Disquisitiones Arithmeticae, 1801.
14. H. Hasse: "Klassenkörperbericht", I (1926), Ia (1927), II (1930).
15. H. Hasse: Vorlesungen über Zahlentheorie, 1950.
16. H. Hasse: Über die Klassenzahl abelscher Zahlkörper, 1952.
17. E. Hecke: Vorlesungen über die Theorie der algebraischen Zahlen, 1923.
18. D. Hilbert: Die Theorie der algebraischen Zahlkörper, 1897. (Werke I).
19. L. Holzer: Zahlentheorie I (1958), II (1959).
20. A.E. Ingham: Distribution of Prime Numbers, 1932.

21. K. Iwasawa : Lectures on p-adic L-Functions, 1972.

22. E. E. Kummer : Collected papers I, 1975.

23. E. Landau : Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, 1918.

24. E. Landau : Vorlesungen über Zahlentheorie, I-III, 1927.

25. D. A. Marcus : Number Fields, 1977.

26. H. Minkowski : Geometrie der Zahlen, 1896.

27. H. Minkowski : Diophantische Approximationen, 1907.

28. J. Neukirch : Klassenkörpertheorie, 1967

29. H. Weber : Lehrbuch der Algebra I-III, 1896.

30. A. Weil : Basic Number Theory, 1967.

31. E. Weiss : Algebraic Number Theory, 1963

Rettelser

pag. 15, nederst : $v = 0$.

pag. 23, 7.n : $[K : k]$ i st. f. $[K\ k]$.

pag. 27, 4.0 : $\neq (0)$ mgl.

pag. 37, nederst : $0 \leq \lambda < l$, $0 \leq \mu < m$.

pag. 41, 4.0 : $b d_1 d_2$ i st. f. $b d_1$.

pag. 49, 10.n : $x = \sum_{j=1}^{s} (p_1^{(j)} + a\, r_1^{(j)})(p_2^{(j)} + a\, r_2^{(j)})$; sumtegnet skal tilføjes i linierne nedenfor.

pag. 82, 4.0 : $a \neq 0$ mgl.

pag. 88, nederst : Formler for y_1, y_2 og y er givet i øvelsen efter sætning 60.

pag. 93, 3.n : } mgl.

pag. 96, nederst : for $r_2 = 0$ for alle i pånær ét.

pag. 102, 2.n : (p) er treg i st. f. $\left(\frac{d}{p}\right) = -1$.

pag. 104, 4.n :) mgl.

pag. 106, nederst : Ifølge sætning 69, korollar, er derfor $h = 1$.

pag. 107, 10.n : 7 i st. f. -7.

pag. 114, 10.n :) mgl.

pag. 116, 5.n : $[\cdots] + 1$ i st. f. $[\cdots]$.

pag. 121, 9.n : 282 (1976), 133-156, 283-84 (1976), 77-85 mgl.

pag. 126, nederst : $e_{r_1+2r_2} = (0, 0, \cdots, 0, 0, 0, \cdots, i)$.

pag. 131, 5.0 : $\mathbb{C}^{r_1}$ i st. f. $\mathbb{C}$.

pag 131, 9.n : $\alpha_1, \cdots, \alpha_M \in O_k$, $0 < |N(\alpha_j)| < Q$ for $0 \leq j \leq M$ (index N erstattes i det følgende med M).

pag. 132, 3.n : $|N(\alpha)|$ i st. f. $N(\alpha)$.

pag. 134, 12.0 : $e^{\frac{1}{2}c}$ i st. f. e^{2c}.

pag. 142, 11.0 : σ_1 i st. f. σ.

pag. 169, 6.0 : fuldstændig mgl.

pag. 174, 1-2.n : $a = e$ og $\chi = \chi_0$ (hovedk.) ombyttes.

pag. 177, 4.n : vil i st.f. vi.

pag. 180, afsnit ② : $\tilde{D}$, D', D'' erstattes af $\tilde{\chi}$, χ', χ'' en del steder.

pag. 181, nederst : Der tilføjes : Karakteren χ for $\mathbb{Q}(\sqrt{d})$ kaldes <u>Kronecker karakteren</u>.

pag. 183, 8.0 og 10.0 : $\frac{x^2-1}{8}$ i st.f. $\frac{x^2-1}{2}$.

pag. 185, 7.n : mod D i st.f. mod p.

pag. 187, 3.0 : ζ^x i st.f. ζ^{-x}.

pag. 192, 2.0 og 5.0 }
pag. 193, 7.0 og 8.0 } : sgn i st.f. arg. [$\operatorname{sgn} z = \frac{z}{|z|}$ for $z \in \mathbb{C} \setminus \{0\}$].

pag. 192, 6.n : $\eta = e^{\pi i/p}$ i st.f. $\eta = e^{2\pi i/p}$.

pag. 209, 9.n : Da k har fundamentalenheden $\varepsilon_1 = 3+\sqrt{10}$ og $N(\varepsilon_1) = -1$ er k af type <u>II</u> er ....

pag. 212, 8.0 : $\psi_3'^3$ i st.f. $\psi_3'^2$.

pag. 215, 7.0 : $\chi_j(N(\mathfrak{A}))$ i st.f. $\chi_j(\mathfrak{A})$.

pag. 217, 6.0 : vise (**) i st.f. vise.

pag. 218, 1.n : φ i st.f. p.

pag. 223-24 : $\sum_{n=M+1}^{N}$ i st.f. $\sum_{n=M}^{N}$ fem steder.

pag. 236, 2.n : og divergent for $\sigma < \sigma_a = \sigma_c$ i st.f. men....

pag. 243, 9.n : $=$ i st.f. $\leqq$

pag. 243, 4.n : I (*) i st.f. I.

pag. 248, 6.0 og 7.0 : $R_A(s)$ i st.f. $R_A(s, X)$.

pag. 250, 6.n : For $\gcd(c, D) = r > 1$ er $\bar{\chi}(c) = 0$, ...

pag. 254, 4.n : 1 mgl.

pag. 264, 3.0 : Der indskydes : Hvis $a_j \notin \mathfrak{O}_j$ for et $j \in \{1, \dots, s\}$ kan vi bruge $a = a_j$, ellers sættes ....

pag. 266, 1.o : (Hilbert, Artin) i st.f. (Hilbert).

pag. 278, 6.n : $\left| \sum_{c=1}^{l-1} \bar{\chi}(c)\, c \right|$ i st.f. $\bar{\chi}(c)\, c$.

pag. 279, 10.n : $l\,t \cdots$ i st.f. $l\,1 \cdots$.

pag. 282, 9.n : homomorfi i st.f. isomorfi.

pag. 293, 3.n : $\mathrm{vol}(T_+) = (2\pi)^{r_2} \int_{\mathfrak{R}} \rho_{r_1+1} \cdots \rho_{r_1+r_2}\, d\rho_1 \cdots d\rho_{r_1+r_2}$,

pag. 297, 2.o : flg. udgår : der for ethvert $\varepsilon > 0$ gælder:.

pag. 297, 3.o, 4.o : ε erstattes af 1.

pag. 297, 7.o. : $\lim_{k\to\infty} \frac{N(t_k - 1)}{t_k^{\,n}} = \lim_{k\to\infty} \frac{N(t_k)}{t_k^{\,n}} = \frac{\mathrm{vol}(X_0)}{d(M)}$.

—

Ekstra litteratur

1. H. M. Edwards : Fermat's Last Theorem, 1977
2. S. Lang : Cyclotomic Fields, 1978.
3. L. E. Dickson : Introduction to the Theory of Numbers, 1929.