Einführung in die algebraische und analytische Zahlentheorie

Dr. Klaus Haberland

Semester: WS 2006/07

Vorwort

Dieses Dokument wurde als Skript für die auf der Titelseite genannte Vorlesung erstellt und wird jetzt im Rahmen des Projekts „Vorlesungsskripte der Fakultät für Mathematik und Informatik“ weiter betreut. Das Dokument wurde nach bestem Wissen und Gewissen angefertigt. Denoch garantiert weder der auf der Titelseite genannte Dozent, die Personen, die an dem Dokument mitgewirkt haben, noch die Mitglieder des Projekts für dessen Fehlerfreiheit. Für etwaige Fehler und dessen Folgen wird von keiner der genannten Personen eine Haftung übernommen. Es steht jeder Person frei, dieses Dokument zu lesen, zu verändern oder auf anderen Medien verfügbar zu machen, solange ein Verweis auf die Internetadresse des Projekts `http://uni-skripte.lug-jena.de/` *enthalten ist.*

Diese Ausgabe trägt die Versionsnummer 2601 und ist vom 6. Dezember 2009. Eine (mögliche) aktuellere Ausgabe ist auf der Webseite des Projekts verfügbar.

Jeder ist dazu aufgerufen, Verbesserungen, Erweiterungen und Fehlerkorrekturen für das Skript einzureichen bzw. zu melden oder diese selbst einzupflegen – einfach eine E-Mail an die Mailingliste `<uni-skripte@lug-jena.de>` *senden. Weitere Informationen sind unter der oben genannten Internetadresse verfügbar.*

Hiermit möchten wir allen Personen, die an diesem Skript mitgewirkt haben, vielmals danken:

- *Jörg Sommer* `<joerg@alea.gnuu.de>` *(2006/07)*
- *Benjamin Sambale* `<tylerdurden104@web.de>` *(2006)*
- *Robert Müller (2006/07)*

Inhaltsverzeichnis

Auflistung der Theoreme

Sätze

Definitionen und Festlegungen

Literaturverzeichnis

[1] Боревич, Шафаревич (Borevich, Shafarevich): Теория чисел (Number theory), Изд. Наука (Hayka), Moskau 1985

[2] D. Zagier: Zetafunktion und quadratische Zahlenkörper, Springer 1981

[3] Edwards: Fermat's last theorem, Springer 1977

[4] H. Hasse: Vorlesungen über Zahlentheorie, Springer 1950

[5] E. Hecke: Vorlesungen über die Theorie der algebraischen Zahlen, Geest & Fortig, Leipzig 1954

[6] J. Neukirch: Algebraische Zahlentheorie, Springer 1992

1 Elementare Zahlentheorie

1.1 Die ganzen Zahlen

Die Standardbezeichnung der Menge der ganzen Zahlen ist $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ mit der Addition und Multiplikation, mit gutartigen Eigenschaften.

Definition 1.1
$a, b \in \mathbb{Z}$, $a \mid b$ (gespr. a teilt b) $:= \exists c \in \mathbb{Z}\colon b = ac$.

Bemerkung 1.1
± 1 teilen jede ganze Zahl und jede ganze Zahl teilt die Null.

Definition 1.2
Eine ganze Zahl $m \neq \pm 1$ heißt **Primzahl** $:\Leftrightarrow$ sie besitzt genau 4 Teiler.

Bemerkung 1.2
Die Menge der positiven Primzahlen sei $\mathbb{P}$. Euklid hat gezeigt $\mathbb{P}$ ist unendlich. Die aktuell, größe Primzahl von heute morgen ist $2^{32582657} - 1$. Quelle: GIMPS.

1.1.1 11 Beweise, dass $\mathbb{P}$ unendlich ist

Beweis: (Nach Euklid)
Angenommen: $\mathbb{P}$ ist endlich, dann hat das Produkt aller Primzahlen vermehrt um 1 keine Primteiler. ∎

Beweis: (Ch. Hermite (1870))
Sei p_n der kleinste Primteiler von $n! + 1$, dann ist $p_n > n$. ∎

Beweis: (T. Stieltjes (1890))
Sei $\mathbb{P} = \{p_1, \dots, p_n\}$ und $D = p_1 \cdot \dots \cdot p_n$. Zerlege $D = m \cdot n$, $m, n > 1$. Für jede Primzahl gilt: $p \mid m$ oder $p \mid n$, aber nicht beide. Also hat $m + n$ keine Primteiler. ∎

Beweis: (J. Braun (1890))
$\mathbb{P} = \{p_1, \dots, p_n\}, D = p_1 \cdot \dots \cdot p_n$

$$\sum \frac{1}{p_i} = \frac{a}{D} \quad \text{mit } a = \frac{D}{p_i}$$

Nun ist $a/D \geq 1/2 + 1/3 + 1/5 = 31/30 > 1$. Also muss a Primteiler haben, z. B. p_k. Es folgt: p_k teilt a und jedes $D/p_i, i \neq k$. Also auch D/p_k. Widerspruch. ∎

Beweis: (Euler (1759) (falscher Beweis))
Wir wollen

$$\prod_{p\in\mathbb{P}} 1-\frac{1}{p}=0$$

Setze dazu

$$\begin{aligned}
x &= 1+\frac{1}{2}+\frac{1}{3}+\cdots\\
\frac{1}{2}x &= \frac{1}{2}+\frac{1}{2}+\frac{1}{6}+\cdots\\
\frac{1}{2}x &= 1+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots\\
\frac{1}{6}x &= \frac{1}{3}+\frac{1}{9}+\frac{1}{15}+\cdots
\end{aligned}$$

$$\Rightarrow \frac{1\cdot 2}{2\cdot 3}x = 1+\frac{1}{5}+\frac{1}{7}+\cdots = \sum_{n \text{ prim zu } 6}\frac{1}{n}$$

$$\Rightarrow \frac{(p_1-1)(p_2-1)\cdots(p_k-1)}{p_1p_2\cdots p_k}x = \sum_{n \text{ prim zu } p_1\cdots p_k}$$

$$\Rightarrow \prod_{p\in\mathbb{P}}(1-\frac{1}{p})x = 1$$

Da $x=\infty$ ist, folgt $\prod_{p\in\mathbb{P}}(1-\frac{1}{p})=0$ ∎

Beweis: (Sylvester (1888))
Korrektur des Beweises von Euler.

$$\prod_{p\le x}\big(1-\frac{1}{p}\big)^{-1} = \prod_{p\le x}\big(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\big) \ge \sum_{n\le x}\frac{1}{n} \ge \int_2^x \frac{dt}{t} = \ln x - \ln 2 \to \infty$$ ∎

Beweis: (Perrot (1881))
Für $n>2$ ist die Anzahl der natürlichen Zahlen $\le N$, welche quadratische Teiler >1 besitzen, beschränkt durch

$$\sum_{2\le n\le N}\frac{N}{n^2} < N\Big(\frac{1}{4}+\sum_{n=3}^{\infty}\frac{1}{n^2}\Big) \le N\Big(\frac{1}{4}+\int_2^{\infty}\frac{dt}{t^2}\Big) = \frac{3}{4}N$$

Also existieren im Intervall $[1,N]$ mindestens $\frac{N}{4}$ quadratfreie Primzahlen.

Sei $P=\{p_1,\ldots,p_n\}$. Dann existieren genau 2^n quadratfreie Zahlen: $p_{i_1},\ldots,p_{i_r}$ für $1\le i_1<i_r\le n$. ∎

X Menge, O Familie von Teilmengen, so dass

1. $\emptyset, X \in O$
2. $U, V \in O \Rightarrow U \cap V \in O$
3. $\forall U_i \in O, i \in I \Rightarrow \bigcup U_i \in O$

(X, O) heißt **topologischer Raum** oder **Topologie**, $U \in O$ offene Menge.

Eine **arithmetische Progression** in $\mathbb{Z}$: $a + m\mathbb{Z}, m > 0$. Diese bilden Familie von Teilmengen in $\mathbb{Z}$, welche durchschnittsabgeschlossen ist. Sie erzeugt also durch Vereinigung die Topologie auf $\mathbb{Z}$.

Beweis: (Fürstenberg (1955))
Jede arithmetische Progression ist offen und abgeschlossen. Sei $A_p = p \cdot \mathbb{Z}$, $A = \bigcup_{p \in \mathbb{P}} A_p$.

$\mathbb{Z} \setminus A = \{-1, 1\}$ ist nicht offen, also ist A nicht abgeschlossen. Die A_p sind abgeschlossen, also auch jede endliche Vereinigung. ∎

Beweis: (Tchebyshev (18??))
Für eine reelle Zahl x gilt: $x - 1 < [x] \leq x$. Es folgt

$$[x + y] - [x] - [y] \in \{0,1\}$$

Wie oft geht eine Primzahl p in $n!$ auf?

$$[\ln(n!) = n \ln n - n + \frac{1}{2} \ln 2\pi n + \frac{\Theta(n)}{12n} \quad \text{wobei } |\Theta(n)| < 1]$$
$$\operatorname{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Also $\operatorname{ord}_p(\binom{n}{k}) = \sum_{r=1}^{\infty}([\frac{n}{p^r}] - [\frac{n}{p^r}] - [\frac{n-k}{p^r}]) \leq \frac{\ln n}{\ln p}$.

Es folgt:

$$p^{\alpha p} \mid \binom{n}{k} \Rightarrow p^{\alpha p} \leq n$$

Also

$$\binom{n}{k} = \prod_{p \leq n} p^{\alpha p} \leq n^{\pi(n)} \quad \pi(n) = \operatorname{card}\{p \leq n\}$$
$$2^n = \sum_{k=0}^{n} \binom{n}{k} \leq (n+1) n^{\pi(n)}$$
$$n \ln 2 \leq \ln(n+1) + \pi(n) \ln n$$
$$\Rightarrow \pi(n) \geq \ln 2 \frac{n}{\ln n} - \frac{\ln n + 1}{\ln n} \geq \frac{2}{3} \frac{n}{\ln n} \qquad (n \geq 200)$$

Analog: $\pi(n) \leq 1{,}7 \frac{n}{\ln n}$. todo: Irgendwie formulieren: $\frac{n}{\ln n}$ ist fast n, Quadratzahlen gibt es nur $\sqrt{n}$, also mehr Primzahlen als Quadratzahlen ∎

1.1.2 Primzahlverteilung

$x \in \mathbb{R}_+$

$$\pi(x) \cong \frac{x}{\ln x} \quad \text{für } x \to \infty$$

$$\pi(x) = \mathrm{li}(x) + R(x)$$

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\ln t} + c = \frac{x}{\ln x} + \frac{x}{2!(\ln x)^2} + \frac{x}{3!(\ln x)^3} + \cdots$$

Lemma 1.1 (Goldbach-Vermutung)

1. Jede ungerade natürliche Zahl ist Summe dreier positiver ungerader Primzahlen. Bewiesen von Vinogradov (1937).
2. Jede gerade natürliche Zahl ist Summer zweier positiver ungerader Primzahlen.

- Als einen **Primzahlzwilling** bezeichnet man eine Zahl $p \in \mathbb{P}$, wobei gilt $p+2 \in \mathbb{P}$.
- Unbewiesen ist, dass es unendlich viele Primzahlen der Form n^2+1 gibt. Vermutung: Ja
- Arithmetische Progressionen enthalten so viele Primzahlen:

$$a + m\mathbb{Z} \cap \mathbb{P} \text{ ist unendlich, falls } (a, m) = 1.$$

Nette Aufgabe zum Schluss: Sei

$$f(n) = (n-1)\left[\left[\frac{n!+1}{n+1}\right] - \frac{n!-n}{n+1}\right] + 2$$

$f\colon \mathbb{N}^* \to \mathbb{N}^*$. Dann hat f nur Primzahlwerte und jede Primzahl tritt als Wert auf.

1.1.3 Euklids Algorithmus

Für zwei natürliche Zahlen a, b existieren zwei eindeutig bestimmte Zahlen $q, r \in \mathbb{N}$ so, dass

$$a = qb + r, \quad 0 \le r < b$$

(Division mit Rest). Denn es existiert genau ein $q \in \mathbb{N}$ so, dass

$$qb \le a < (q+1)b$$

$$\begin{aligned} a &= q_1 b + r_1 & 0 \le r_1 < b \\ b &= q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 \le r_3 < r_2 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n & 0 \le r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Fakt 1.1
r_n ist der größte gemeinsame Teiler von a und b.

Beweis:
Von unten nach oben: $r_n \mid r_{n-1}, r_{n-2}, \dots, b, a$.

Sei d Teiler von a und b. Von oben nach unten: d teilt r_n. ∎

Definition 1.3
Der ggT von a, b wird mit (a, b) oder $\mathrm{ggT}(a, b)$ bezeichnet. Ist $(a, b) = 1$, so heißen a und b **teilerfremd**.

Folgerung 1.1
Der ggT von a, b ist $\mathbb{Z}$-Linearkombination von a und b:

$$\exists x, y \in \mathbb{Z}\colon (a, b) = xa + yb$$

Beweis:
Substituieren von unten nach oben ∎

Folgerung 1.2
Sei $p \in \mathbb{P}, a, b \in \mathbb{Z}$. Dann gilt: $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.

Beweis:
Annahme: $p \nmid b \Rightarrow (p, b) = 1 \Rightarrow xp + yb = 1 \Rightarrow xap + yab = a \Rightarrow p \mid a$. ∎

Satz 1.1 (Hauptsatz der elementaren Arithmetik)
Jede ganze Zahl $\neq 0, \pm 1$ ist Produkt von Primzahlpotenzen. Diese D'g ist bis auf VZ und Reihenfolge eindeutig bestimmt.

Beweis:
o. B. d. A. nur natürliche Zahlen.

Exisitenz: Induktion: richtig für alle $m < n$, ist $n \in \mathbb{P}$, so fertig. sonst: $n = kl, k > 1, l > 1 \Rightarrow k < n, l < n \Rightarrow$ IV.

Eindeutigkeit $p_1^{a_1} \cdots p_r^{a_r} = q_1^{b_1} \cdots q_s^{b_s}$. p_1 teil RHS $\Rightarrow p \mid q_j^{b_j} \Rightarrow p_1 = q_j$. Teile durch p_1 und IV. ∎

1.1.4 Die Restrechnung (d'aprés GAUSS)

Definition 1.4
Für $m \in \mathbb{N}^*$ bezeichnet man eine Menge der Form $a + m\mathbb{Z} = \{a + mb \colon b \in \mathbb{Z}\}$ mit $a \in \mathbb{Z}$ als **Restklasse modulo m**. Die Menge dieser m Restklassen heißt **Restklassenring modulo m** und wird mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet.

$$(a + b) + m\mathbb{Z} := (a + m\mathbb{Z}) + (b + m\mathbb{Z})$$
$$a \cdot b + m\mathbb{Z} := (a + m\mathbb{Z}) \cdot (b + m\mathbb{Z})$$

Diese Definitionen sind repräsentantenunabhängig. (Übungsaufgabe)

Bemerkung 1.3
Wir erhalten surjektive Abbildungen $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \colon a \mapsto a + m\mathbb{Z}$. Sie repräsentiert $+$ und $\cdot$, sind also **Homomorphismen** von Ringen. Addition, Multiplikation in $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ, kommutativ, die Null ist $m\mathbb{Z}$, die 1 ist $1 + m\mathbb{Z}$. Das Distributivgesetz gilt auch.

Beispiel 1.1
$m = 8$, Multiplikationstabelle für $\mathbb{Z}/8\mathbb{Z}$

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

$\mathbb{Z}/8\mathbb{Z}$ ist kein Körper, da die Multiplikation nicht injektiv ist.

$m = 7$ Multiplikationstabelle für $\mathbb{Z}/7\mathbb{Z}$

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$\mathbb{Z}/7\mathbb{Z}$ ist ein Körper.

Fakt 1.2
Für $m = p \in \mathbb{P}$ ist $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein **Körper**. Für $m \notin \mathbb{P}$ ist $\mathbb{Z}/p\mathbb{Z}$ kein Körper.

BEWEIS:
$m = a \cdot b, a > 1, b > 1$. Dann gilt $\mathbb{Z}/m\mathbb{Z}$: $ab = 0$, aber $a \neq 0, b \neq 0$. Sei $m = p \in \mathbb{P}, x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0$.

Betrachte $x, 2x, \ldots, (p-1)x$, das sind Restklassen $\neq 0$ und es gilt, dass sie alle verschieden sind, denn nehmen wir an $rx = sx$ mit $1 \leq r < s \leq p-1$, es folgt $(s-r)x = 0$, $-p < s - r < p \Rightarrow$ Widerspruch.

Also kommt in der List oben die 1 vor. ∎

Beispiel 1.2
$\mathbb{F}_2 = \{0,1\} = \mathbb{Z}/2\mathbb{Z}$

Definition 1.5
$a + m\mathbb{Z}$ heißt **prime Restklasse modulo m** $:\Leftrightarrow (a, m) = 1$

Beispiel 1.3
In $\mathbb{Z}/8\mathbb{Z}$ haben wir 4 prime Restklassen: 1,3,5,7. In $\mathbb{F}_p$ sind alle Restklassen $\neq 0$ prim.

Fakt 1.3 (Chinesischer Restsatz)
Sei der größte gemeinsame Teiler $(a, b) = 1$, der kanonische Homomorphismus $\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ist eindeutig.

BEWEIS:
Sei das Bild von $x + ab\mathbb{Z}$ gleich $(0,0) \Rightarrow a \mid x, b \mid x$, wegen $(a, b) = 1$ folgt $ab \mid x$. Also $x + ab\mathbb{Z} = 0$. ∎

Folgerung 1.3
Sei $m = p_1^{a_1} \cdots p_n^{a_n} \Rightarrow \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{a_n}\mathbb{Z}$.

Definition 1.6
Sei $\varphi(m)$ die Anzahl der primen Restklassen modulo m. ($\varphi(1) = 1$) φ heißt **Euler-Funktion**.

Fakt 1.4

$$\varphi(m) = m \prod_{p \mid m} (1 - \frac{1}{p})$$

BEWEIS:
$x \in \mathbb{Z}$ induziert prime Restklasse modulo $m \Leftrightarrow x$ ist prim zu $p_1, \ldots, p_n \Leftrightarrow x$ ist prim zu $p_1^{a_1}, \ldots, p_n^{a_n}$. Also $\varphi(m) = \varphi(p_1^{a_1}) \cdots \varphi(p_n^{a_n})$.

$\varphi(p^a) = p^a - p^{a-1} = p(1 - \frac{1}{p})$ ∎

Fakt 1.5
Die primen Restklassen modulo m bilden bezüglich Multiplikation eine Gruppe.

Beweis:
Mit x, y ist auch xy prim zu m. Neutrales Element ist $1 + m\mathbb{Z}$ das Inverse zu $x + m\mathbb{Z}$ findet man wie oben. Betrachte $xy + m\mathbb{Z}$ für alle $\varphi(m)$ prime Restklasse y.

In der Liste kommt 1 vor. ∎

Fakt 1.6 (Kleiner Fermat'scher Satz)
Ist a prime Restklasse modulo m, so gilt $a^{\varphi(m)} \equiv 1 \pmod{m}$ oder anders dargestellt in $\mathbb{Z}/m\mathbb{Z}$ ist $a^{\varphi(m)} = 1$.

Beweis:
Mit r durchläuft auch ar die prime Restklasse modulo m. Also

$$a^{\varphi(m)} \prod_r r = \prod_r (ar) = \prod_r r$$

Dividiert man jetzt beide Seiten durch $\prod_r r$, erhält man $a^{\pi(m)} = 1$. ∎

Folgerung 1.4
(kuriose Folgerung): Jede Primzahl $\neq 2{,}5$ teil eine der Zahlen $9, 99, 999, \ldots$

Beweis:

$$10^{p-1} \equiv 1 \pmod{p}$$ ∎

Fakt 1.7

$$\sum_{d|m} \varphi(d) = m \tag{1.1}$$

Beweis:
Unter den Brüchen $\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m-1}{m}, \frac{m}{m}$ gilt es genau $\varphi(m)$ viele, die sich nicht kürzen lassen. Die anderen kürzen wir soweit es geht. Danach treten alle $d \mid m$ als Nenner auf und zwar $\varphi(d)$ mal. ∎

Bemerkung 1.4
Die Einheiten in $\mathbb{Z}/m\mathbb{Z}$, d. h. die multiplikativ invertierbaren Restklassen sind genau die primen Restklassen.

Beweis:
Übungsaufgabe ∎

1.1.5 Quadratische Gleichungen über $\mathbb{F}_p$

Wir betrachten Polynome mit Koeffizienten aus $\mathbb{F}_p$. Also

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d$$

mit $a_d \neq 0$ heißt **Polynom** d-ten Grades.

Bemerkung 1.5
Jedes solche f verursacht eine Abbildung $\mathbb{F}_p \to \mathbb{F}_p$. Verschiedene Polynome können diese Abbildung verursachen. $x^p - x$ verursacht die Nullabbildung.

Fakt 1.8
Ist $\alpha \in \mathbb{F}_p$ Nullstelle von f, so existiert Polynom g über $\mathbb{F}_p$ so dass $f(x) = (x - \alpha)g(x)$.

Beweis:
Das ist klar für $\alpha = 0$, sonst lineare Substitution. ∎

Folgerung 1.5
Die Anzahl der Nullstellen eines Polynoms ist $\leq$ Grad.

Bemerkung 1.6
Das Polynom $f(x) = x^2 - 1$ hat 4 Nullstellen in $\mathbb{Z}/8\mathbb{Z}$. (Hinweis: dies ist so, weil $\mathbb{Z}/8\mathbb{Z}$ ein Ring und kein Körper ist.)

Satz 1.2 (Gauss)
Die multiplikative Gruppe $\mathbb{F}_p^*$ ist zyklisch.

Beweis:
$\mathbb{F}_p^*$ hat $p-1$ Elemente $\Rightarrow$ die $(p-1)$-te Potenz jedes Elements ist 1.

Die **Ordnung** von $x \in \mathbb{F}_p^*$ ist die kleinste positive natürliche Zahl f, so dass $x^f = 1$.

Wir zeigen: f teilt $p-1$. $d := (f, p-1) \Rightarrow d = af + b(p-1)$, $x^d = x^{af} x^{b(p-1)} = 1 \Rightarrow d = f$.

Sei nun f ein Teiler von $p-1$. Die Elemente aus $\mathbb{F}_p^*$, deren Ordnung f teilt, sind Nullstellen des Polynoms $x^f - 1$.

Also gibt es höchstens f viele.

- Ist x ein Element der Ordnung f, so haben alle $x^a, 0 \leq a < f$ eine Ordnung, welche f teilt. Sie sind alle verschieden. Das sind also alle.
- Ist $0 \leq a < f$ und a und f sind teilerfremd, so hat x^a die Ordnung f. Begründung: $x^{af} = 1$ ist klar. Sei $x^{ag} = 1$ und $g \leq f$. $1 = au + fv$ $(u, v \in \mathbb{Z}) \Rightarrow x = x^{au} \cdot \underbrace{x^{fv}}_{=1} \Rightarrow$ $1 = x^{aug} = x^g \Rightarrow f = g$.
- Ist $(a, f) > 1$, so ist die Ordnung von x^a echt kleiner als f. $(d = (a, f) \Rightarrow (x^a)^{\frac{f}{d}} = 1)$

Es gibt für jedes $f \mid (p-1)$ entweder gar keine oder $\varphi(f)$ viele Elemente der Ordnung f.

Zerlege $\mathbb{F}_p^* = \bigcup_{f|p-1} \Phi_f$. Φ_f sind alle Elemente der Ordnung f. $\Rightarrow p-1 = \sum_{f|p-1} \varepsilon_f \varphi(f)$, $\varepsilon_f = 0$ oder $\varepsilon_f = 1$.

Aus Gleichung 1.1 folgt: Alle $\varepsilon_f = 1$. Insbesondere existieren Elemente der Ordnung $p-1$. ∎

Bemerkung 1.7
Die Elemente der Ordnung $p-1$ heißen **Primitivwurzeln modulo p**. Es gibt $\varphi(p-1)$ viele.

Beispiel 1.4
$p = 13$, $\varphi(12) = \varphi(4)\varphi(3) = 4$

x	ord(x)	
1	1	
2	12	1,2,4,8,3,6,12,11,9,5,10,7,1
3	3	1,3,9,1
4	6	1,5,-1, -5, 1
6	12	1, 6, -3, -5, -4, 2, -1
...		

Satz 1.3
Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist **zyklisch**.

Beweis:
Übungsaufgabe ∎

Fakt 1.9
$(\mathbb{F}_p^*)^2$ ist die Untergruppe der Quadrate in $\mathbb{F}_p^*$. Für $p > 2$ hat $(\mathbb{F}_p^*)^2$ die Ordnung $\frac{p-1}{2}$. Es gibt also im $\mathbb{F}_p^*$ genau $\frac{p-1}{2}$ Quadrate und Nichtquadrate.

Beweis:
Sei g Primitivwurzel, dann ist g^a $(0 \leq a < p-1)$ eine Quadrat $\Leftrightarrow$ a ist gerade. ∎

Definition 1.7
Das **Legendre-Symbol** ist die Abbildung

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to \{\pm 1\}$$

definiert durch

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & : x \in (\mathbb{F}_p^*)^2 \\ -1 & : x \in \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2 \end{cases}$$

Dabei ist $p > 2$.

Bemerkung 1.8
Es wird nicht präzisiert, wo ± 1 liegen. Es kann $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_l^*$ sein.

Fakt 1.10 (Elementare Eigenschaften)

1. $(\frac{x}{p}) = x^{\frac{p-1}{2}}$ (in $\mathbb{F}_p$)
2. $(\frac{xy}{p}) = (\frac{x}{p})(\frac{y}{p})$
3. $(\frac{1}{p}) = 1$
4. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

Beweis:

1. $x = g^a, g \in \mathbb{F}_p^*$ Primitivwurzel. $0 \leq a < p-1$, $x^p = 1 \Rightarrow x^{\frac{p-1}{2}} = \pm 1$. Weiter $g^{\frac{p-1}{2}} = -1$. Ist x Quadrat, so ist a gerade, also $x^{\frac{p-1}{2}} = g^{a\frac{p-1}{2}} = (-1)^a = 1$.

   Ist $x^{\frac{p-1}{2}} = 1$,so folgt $g^{a\frac{p-1}{2}} = 1$, also $(-1)^a = 1 \Rightarrow a$ ist gerade.
2. folgt sofort aus (i)
3. ist trivial
4. $(-1)^{\frac{p-1}{2}} = (\frac{-1}{p})$ nach (i). ∎

Bemerkung 1.9
(iv) heißt 1. Ergänzungssatz zum quadratischen Reziprozitätsgesetz.

Bemerkung 1.10
-1 ist Quadrat in $\mathbb{F}_p^* \Leftrightarrow p \equiv 1 \pmod 4$

Definition 1.8
Sei $p > 2$ prim, $S \subset \mathbb{F}_p^*$ heißt **Halbsystem** $:\Leftrightarrow S \cup (-S) = \mathbb{F}_p^*$ und $S \cap (-S) = \emptyset$.

Beispiel 1.5
Sei $S = \{1,2,\ldots,\frac{p-1}{2}\}$. Wenn $s \in S, a \in \mathbb{F}_p^*$, dann ist $a \cdot s = e_s(a) \cdot s'$ für ein $s' \in S, e_s(a) = \pm 1$.

Lemma 1.2 (Gauss)

$$\left(\frac{x}{p}\right) = \prod_{s \in S} e_s(x)$$

Beweis:
Seien $s_1, s_2 \in S, s_1 \neq s_2, a \in \mathbb{F}_p^*, as_1 = e_{s_1}(a)s_1', as_2 = e_{s_2}(a)s_2'$.

Dann gilt $s_1' \neq s_2'$. Denn $s_1' = s_2' \Rightarrow s_1 = \pm s_2$. ↯ ∎

Also ist die Abbildung $s \mapsto s' \colon S \to S$ eine Bijektion. Wir multiplizierne die Gleichungen $as = e_s(a)s'$ über $s \in S$ auf:

$$a^{\frac{p-1}{2}} \prod_{s\in S} s = \prod_{s\in S} e_s(a) \prod_{s\in S} s'$$
$$\Rightarrow a^{\frac{p-1}{2}} = \prod_{s\in S} e_s(a)$$

Fakt 1.11 (2. Ergänzungssatz zum QRG)

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

Oder

$$(\frac{2}{p}) = \begin{cases} +1 & : p \equiv 1{,}7 \pmod 8 \\ -1 & : p \equiv 3{,}5 \pmod 8 \end{cases}$$

Beweis:
$S = \{1{,}2, \ldots, \frac{p-1}{2}\}$. Dann ist $e_s(2) = 1$ für $2s \leq \frac{p-1}{2}$, $e_s(2) = -1$ für $2s > \frac{p-1}{2}$.

Also $(\frac{2}{p}) = (-1)^{\alpha(p)}, \alpha(p) = \text{card}\{s \in \mathbb{Z} \colon \frac{p-1}{4} < s \leq \frac{p-1}{2}\}$.

Fall 1: $p = 4k+1$, dann ist $\alpha(p) = \text{card}\{k < s \leq 2k\} = k$: also $(\frac{2}{p}) = (-1)^k = \begin{cases} 1 & p \equiv 1 \pmod 8 \\ -1 & p \equiv 5 \pmod 8 \end{cases}$.

Fall 2: $p = 4k+3$. $k + \frac{1}{2} < s \leq 2k+1 \Rightarrow \alpha(p) = k+1 \Rightarrow (\frac{2}{k}) = \begin{cases} 1 & p \equiv 7 \pmod 8 \\ -1 & p \equiv 3 \pmod 8 \end{cases}$. ∎

Satz 1.4 (Quadratische Reziprozitätsgesetz)
Seien p, l ungerade Primzahlen, $p \neq l$, dann gilt

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

Beweis: (nach V. G. KAC)
Sei $\zeta = e^{\frac{2\pi\sqrt{-1}}{p}}$. Dann gilt

$$\prod_{j=1}^{p-1}(X - \zeta^j Y) = \frac{X^p - Y^p}{X - Y}$$
$$\Rightarrow \prod_{j=1}^{p-1}(\zeta^j X - \zeta^{-j} Y) = \zeta^{2\frac{(p-1)p}{2}} \prod (X - \zeta^j Y) = \prod (X - \zeta^j Y)$$
$$\prod_{j=1}^{p-1}(\zeta^j X - \zeta^{-j} Y) = \prod_{j=1}^{\frac{p-1}{2}} (\zeta^j X - \zeta^{-j} Y)(\zeta^{-j} X - \zeta^j Y)$$

$T = \{1,2,\ldots,\frac{p-1}{2}\}$.

Sei $\Theta = e^{\frac{2\pi\sqrt{-1}}{p}}, X = \Theta^i, Y = \Theta^{-i}$.

Es folgt

$$\frac{\Theta^{ip} - \Theta^{-ip}}{\Theta^i - \Theta^{-i}} = \prod_{i\in T}(\zeta^j\Theta^i - \zeta^{-j}\Theta^{-i})(\zeta^{-j}\Theta^i - \zeta^j\Theta^{-i})$$

Produkt über $i \in S = \{1,2,\ldots,\frac{l-1}{2}\}$

$$\prod_{i\in S}\frac{\Theta^{ip} - \Theta^{-ip}}{\Theta^i - \Theta^{-i}} = \prod_{i\in S}\prod_{i\in T}(\zeta^j\Theta^i - \zeta^{-j}\Theta^{-i})(\zeta^{-j}\Theta^i - \zeta^j\Theta^{-i})$$

$$LHS = \prod_{i\in S}\frac{\sin(\frac{2\pi ip}{l})}{\sin(\frac{2\pi i}{l})} = \prod_{i\in S} e_p(i) = (\frac{p}{l})$$

Es folgt (Vertauschung von l und p):

$$(\frac{l}{p}) = \prod_{i\in S}\prod_{j\in T}(\zeta^j\Theta^i - \zeta^{-j}\Theta^{-i})(\zeta^j\Theta^{-i} - \zeta^{-j}\Theta^i)$$

Beide Ausdrücke underscheiden sich nur in den 2. Faktoren um jeweils -1. $\Rightarrow$

$$(\frac{p}{l})(\frac{l}{p}) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}}$$ ∎

Beweis: (Gauss)
Sei $m = \frac{p-1}{2}, n = \frac{l-1}{2}$ und wir betrachten die $m \cdot n$ Zahlen $py - lx$, $1 \le x \le m, 1 \le y \le n$. Diese sind alle $\neq 0$ und verschieden:

$$py_1 - lx_1 = py_2 - lx_2 \Rightarrow p(y_1 - y_2) = l(x_1 - x_2)$$

$\Rightarrow p \mid x_1 - x_2$ $-m < x_1 - x_2 < m \Rightarrow x_1 = x_2$, analog $y_1 = y_2$.

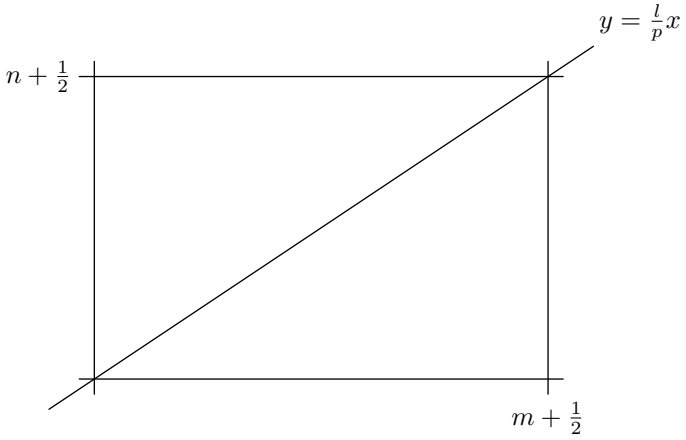
Sei P Anzahl der positiven $py - lx$, N die Anzahl der negativen. Also $P + N = m \cdot n$. Wir fixieren x und fragen: Wie viele y liefern negative Werte: $py - lx < 0$? Anzahl ist $[\frac{lx}{p}]$.

Somit gilt

$$N = \sum_{x=1}^{m}\left[\frac{lx}{p}\right]$$

und

$$P = \sum_{y=1}^{n}\left[\frac{py}{l}\right]$$



In oberen Dreieck liegen die Gitterpunkte, welche in P gezählt werden, im unteren Dreieck die zu N.

Sei $S = \{1,2,\ldots,m\}, T = \{1,2,\ldots,n\}$. Sei $x \in S$, dann ist

$$lx = \left[\frac{lx}{p}\right] \cdot p + r(x), \quad 1 \leq r(x) \leq 2m$$

Die lx bilden modulo p wieder ein Halbsystem, also auch die $r(x)$.

GAUSS' Lemma (Lemma 1.2)

$$(\frac{l}{p}) = (-1)^{\alpha}$$

$\alpha =$ Anzahl der $r(x)$, welche in $-S$ liegen.

$$\sum_{x=1}^{m} lx = \sum_{x=1}^{m} ([\frac{lx}{p}] \cdot p + r(x))$$
$$\Rightarrow l \cdot \frac{m(m+1)}{2} = p \sum_{x=1}^{m} [\frac{lx}{p}] + \sum_{x=1}^{m} r(x)$$
$$\sum_{x=1}^{m} r(x) = \sum_{r(x) \in S} r(x) + \sum_{r(x) \in -S} r(x)$$

Ist $r(x) \in -S$, so $r(x) = p - s(x)$ für ein $s(x) \in S$. (wegen $1 \leq r(x) \leq 2m = p - 1$)

Also $r(x) \equiv p + s(x) \pmod 2$. Es folgt

$$\sum_{x=1}^{m} r(x) = \sum_{x=1}^{m} x + \alpha p \pmod 2$$
$$\Rightarrow l\frac{m(m+1)}{2} \equiv p\sum_{x\in S}[\frac{lx}{p}] + \frac{m(m+1)}{2} + \alpha p \pmod 2$$
$$\Rightarrow \sum_{x\in S}[\frac{lx}{p}] \equiv \alpha \pmod 2$$

Analog

$$\sum_{y\in T}[\frac{py}{l}] \equiv \beta \pmod 2 \quad \text{mit}(\frac{p}{l}) = (-1)^\beta$$

Es gilt $\alpha + \beta \equiv P + N \pmod 2 \equiv m \cdot n \pmod 2$.

Also $(\frac{p}{l})(\frac{l}{p}) = (-1)^{\alpha+\beta} \equiv (-1)^{m\cdot n}$ ∎

1.1.6 Quadratsummen

Fakt 1.12
Jede Primzahl $p \equiv 1 \pmod 4$ besitzt die Darstellung $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$. Dabei sind x, y bis auf das Vorzeichen und die Reihenfolge eindeutig bestimmt.

Beweis:
-1 ist ein Quadrat $\pmod p$, also existiert ein $z \in \mathbb{F}_p^*$ mit $z^2 = -1$ in $\mathbb{F}_p$. Sei n die kleinste natürliche Zahl mit $n^2 > p$. Wir betrachten alle $zx - y$ mit $0 \le x < n, 0 \le y < n$ in $\mathbb{F}_p$. Die Anzahl der Klassen ist $n^2 > p$. Nach dem Dirichlet-Schubfachprinzip existiert also mindestens ein $(x_1, y_1) \neq (x_2, y_2)$ mit $zx_1 - y_1 = zx_2 - y_2$. Es folgt $z = \frac{x}{y}$ mit $|x|, |y| < n$. Also $-1 \equiv \frac{x^2}{y^2} \pmod p$ mit $|x| < n, |y| < n$. $\Rightarrow x^2 + y^2 = p \cdot r, x^2 < p, y^2 < p$. $\Rightarrow x^2 + y^2 = p$.

Fehlt noch die Eindeutigkeit: Annahme: $p = x^2 + y^2 = u^2 + v^2$ mit $x, y, u, v > 0$. Es folgt: $(x, y) = (u, v) = 1$ sowie $\frac{u}{v} \equiv -\frac{v}{u} \pmod p \Rightarrow -1 \equiv \frac{x^2}{y^2} \equiv \frac{u^2}{v^2} \pmod p \Rightarrow \frac{x}{y} \equiv \pm\frac{u}{v} \pmod p$.

Durch Vertauschung von u und v erriecht man $\frac{x}{y} \equiv \frac{u}{v} \pmod p \Rightarrow xv - yu \equiv 0 \pmod p$.

$p^2 = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2 \Rightarrow (xv - yu)^2 < p^2$ und teilbar durch $p^2 \Rightarrow xv = yu \Rightarrow x = u, y = v$. ∎

Fakt 1.13 (Lagrande (1770))
Jede natürliche Zahl ist Summe von vier Quadratzahlen. (Hier ist Null auch eine Quadratzahl).

Beweis:
Wegen

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)\\ &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &\quad +(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2,\end{aligned}$$

genügt es zu zeigen, dass der Satz für die Primzahlen gilt: Der Fall $p=2$ ist klar – $2=0^2+0^2+1^2+1^2$.

Sei $p>2, p\in\mathbb{P}$, Für $0\le x^2<\frac{1}{2}p$ sind die x^2 alle verschieden in $\mathbb{F}_p$, wie auch die $-1-y^2, 0\le y<\frac{1}{2}p$. Das sind je $\frac{p+1}{2}$ viele Elemente, also existierien x,y mit $x^2+y^2+1=0$ in $\mathbb{F}_p$.

Wähle $a,b\in\mathbb{Z}$. Repräs. von $x,y\in\mathbb{F}_p$ mit $|a|,|b|\le\frac{p-1}{2}$. Es folgt $a^2+b^2+1=pr$, $a^2+b^2+1<\frac{p^2}{4}+\frac{p^2}{4}+1<p^2\Rightarrow r<p$.

Abstieg: Sei $pr=x_1^2+x_2^2+x_3^2+x_4^2$ mit $1<r<p$. Wir konstruieren für ein s (mit $1\le s<r$) eine D'g von ps durch vier Quadrate.

Seien dazu $y_i\in\mathbb{Z}$ so, dass

$$y_i\equiv x_i \pmod r, \quad -\frac{r}{2}<y_i\le\frac{r}{2}$$

Dann gilt $\sum y_i^2\equiv 0 \pmod r$, also $\sum y_i^2=rm$ für ein $m\in\mathbb{N}$.

Die LHS ist $\le r^2$, also $m\le r$.

- $m>0$, da sonst alle $y_i=0$, also alle x_i teilbar durch $r\Rightarrow r\mid p\Rightarrow r=1$ oder $r=p$ ↯.
- $m\neq r$, da sonst alle $y_i=\frac{r}{2}$, also $pr\equiv(4\frac{r^2}{4}=r^2) \pmod{r^2}\Rightarrow r\mid p$ ↯.

$pr^2m=y_1^2+y_2^2+y_3^2+y_4^2$

Jedes der z_i ist teilbar durch r (siehe Formel oben) $\Rightarrow pm=(\frac{z_1}{r})^2+(\frac{z_2}{r})^2+(\frac{z_3}{r})^2+(\frac{z_4}{r})^2$ ■

Bemerkung 1.11
Die Identität kommt so zustande: **Quaternionen**: $\mathbb{H}:=\mathbb{R}1\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k$. Multiplikation $i^2=j^2=k^2=-1$. $ij=k, jk=i, ki=j, ji=-k, kj=-i, ik=-j$.

Das ist eine sogenannte Divisionsalgebra, d. h. alle Körperaxiome bis auf die Kommutativität der Multiplikation gelten.

$$q=a+bi+cj+dk, \overline{q}=a-bi-cj-dk$$
$$\|q\|=q\overline{q}=\overline{q}q=a^2+b^2+c^2+d^2$$

$\|q_1q_2\|=\|q_1\|\|q_2\|$ impliziert obige Identität.

Bemerkung 1.12
Ein weit eindrucksvollerer Beweis durch Jacobi um 1870: Formel für die Anzahl der Vektoren $(x_1, x_2, x_3, x_3) \in \mathbb{Z}^4$ mit $\sum_{i=1}^{4} x_i^2 = n$.

$$r_4(n) = 8 \sum_{\substack{d|n \\ d>0}} d$$

für n ungerade. Also z. B. $r_4(7) = 8 \cdot (1 + 7) = 64$. $7 = 4 + 1 + 1 + 1$ im Wesentlichen die einzige Möglichkeit, die anderen 63 entstehen durch Permutation und Vorzeichenwechsel.

Analog für $r_4(n)$ mit n ungerade.

$$\sum_{n=0}^{\infty} r_4(n) x^n = \Big(\sum_{n=-\infty}^{\infty} x^{n^2} \Big)^4$$

2 Der Dirichletsche Primzahlsatz

Er besagt: In jeder primen Restklasse liegen unendlich viele Primzahlen.

Spezialfall: Seien $p_1, \ldots, p_n$ Primzahlen $\equiv 1 \pmod 4$. Sei $N = \prod_{i=1}^{n} p_i$ und $M = 4N^2 + 1$. Sei p Primteiler von M. Dann ist $\forall i\colon p \neq p_i$ und $p \equiv 1 \pmod 4$:

$$4N^2 + 1 \equiv 0 \pmod p \Rightarrow 4N^2 \equiv -1 \pmod p$$

Also $(\frac{-1}{p}) = 1 = (-1)^{\frac{p-1}{2}} \Rightarrow p \equiv 1 \pmod 4$.

2.1 Dirichlet-Charaktere

Das sind Verallgemeinerungen des Legendre-Symbols.

Definition 2.1
Ein Dirichlet-Charakter $\pmod m$ (mit $m \geq 2$) ist eine Abbildung $\chi\colon (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ mit der Eigenschaft $\chi(xy) = \chi(x)\chi(y)$ Man setzt χ gern auf $\mathbb{Z}$ fort durch

$$\chi(a) = \begin{cases} \chi(\overline{a}) & : (a, m) = 1 \\ 0 & : \text{sonst} \end{cases}$$

Fakt 2.1

1. Die Werte von χ sind $\varphi(m)$-te Einheitswurzeln.
2. Die Dirichlet-Charaktere $(\mathrm{mod}^*\, m)$ bilden eine abelsche Gruppe.

Beweis:

1. In $(\mathbb{Z}/m\mathbb{Z})^*$ gilt $x^{\varphi(m)} = 1$. Also $\chi(x)^{\varphi(m)} = 1 \Rightarrow$ qed.
2. Mit φ, ψ ist auch $\varphi \circ \psi$ Dirichlet-Charaktere. $\chi_0 \equiv 1$ ist die Gruppeneins $\chi^{-1} = \overline{\chi}$.∎

Bemerkung 2.1 (Übungsaufgabe)
Sei $p > 2, m = p^f$, dann ist $(\mathbb{Z}/p^f\mathbb{Z})^*$ auch zyklisch. Ist x Erzeuger von $(\mathbb{Z}/p^f\mathbb{Z})^*$ und $\zeta \in \mathbb{C}^*$ Einheitswurzel der Ordung $\varphi(p^f) = p^f - p^{f-1}$ so erhält man durch $\chi(x^a) = \zeta^a$. Dirichlet-Charakter $(\mathrm{mod}^*\, m)$.

Analog für $p = 2$: $(\mathbb{Z}/2^f\mathbb{Z})^* = \{\pm 1\} \times$ zyklische Gruppe der Ordnung 2^{f-2} $(f \geq 2)$.

Fakt 2.2
Die Dirichlet-Charaktere ($\mathrm{mod}^* m$) bilden abelsche Gruppen der Ordnung $\varphi(m)$, sie ist (nicht kanonisch) isomorph zu $(\mathbb{Z}/m\mathbb{Z})^*$.

Beweis:
Jede endliche abelsche Gruppe ist direktes Produkt von zyklischen. Für $(\mathbb{Z}/m\mathbb{Z})^*$ ist das klar:

$$m = \prod p^{f_p} \to (\mathbb{Z}/m\mathbb{Z})^* = \ \times(\mathbb{Z}/p^{f_p}\mathbb{Z})^*$$

Sei also A direktes Produkt zyklischer Gruppen $\hat{A} = \mathrm{Hom}(A, \mathbb{C}^*)$ (– Pontriagin-duale Gruppe).

Wir zeigen:

1. Für A zyklisch gilt $\hat{A} = \ A$,
2. $\widehat{A \times B} = \hat{A} \times \hat{B}$.

Daraus folgt dann der Fakt.

1. Sei $(A : 1) = n, x \in A$ Erzeuger , dann ist

   $$\hat{A} \to \mu_n \subset \mathbb{C}^* \colon \chi \mapsto \chi(x)$$

   ein Isomorphismus. (μ_n ist die n-te Einheitswurzel)

   Injektivität ist klar, Surjektivität auch.

2. Wir haben einen kanonischen Homomorphismus

   $$\widehat{A \times B} \to \hat{A} \times \hat{B} \colon \chi \mapsto (\chi \mid A, \chi \mid B)$$

   und

   $$\hat{A} \times \hat{B} \to \widehat{A \times B} \colon (\varphi, \psi) \mapsto \chi$$

   mit

   $$\chi(a, b) := \varphi(a)\psi(b)$$

   Diese sind invers. ∎

Fakt 2.3 (Orthogonalitätsrelation)

$$\sum_{a \bmod^* m} \chi(a) = \begin{cases} \varphi(m) & : \chi = 1 = \chi_0 \\ 0 & \text{sonst} \end{cases} \tag{2.1}$$

$$\sum_{\chi \bmod^* m} \chi(a) = \begin{cases} \varphi(m) & : a = 1 \in (\mathbb{Z}/m\mathbb{Z})^* \\ 0 & \text{sonst} \end{cases} \tag{2.2}$$

Beweis:
Beweis von Gleichung 2.1 Für $\chi = \chi_0$ ist jeder Summand gleich Eins. Sei also $\chi \neq \chi_0$, dann existiert $x \in (\mathbb{Z}/m\mathbb{Z})^*$ mit $\chi(x) \neq 1$. Es folgt

$$\chi(x) \sum_a \chi(a) = \sum_a \chi(ax) = \sum \chi(y)$$

$\Rightarrow \sum \chi(a) = 0$.

Beweis für Gleichung 2.2 Genauso: $\forall \chi\colon \chi(1) = 1$. Sei also $a \neq 1$. Wir zeigen, dass es ein χ gibt mit $\chi(a) \neq 1$

Sei $H = \mathbb{C}$ Vektorraum der komplexwertigen Funktionen auf $(\mathbb{Z}/m\mathbb{Z})^*$ mit $\dim H = \chi(m)$.

Für $f, g \in H$ sei $\langle f, g\rangle = \frac{1}{\varphi(m)} \sum_{a \bmod^* m} f(a)\overline{g(a)}$ ein Skalarprodukt auf H.

Nach Gleichung 2.1 sind die Dirichlet-Charaktere orthonormal in H, also Orthonormalbasis. Wäre $\chi(a) = 1$ für alle χ, so würde folgen $\chi(a) = \chi_0(a) \Rightarrow (\chi - \chi_0)(a) = 0$ und $(\chi - \chi_0)(1) = 0$. $\chi - \chi_0$ für $\chi \neq \chi_0$ spannen den Raum der Codimension 1 auf in H und verschwinden in 1 und a.

$\Rightarrow$ Jede Funktion in diesem Raum ist $= 0$ in 1 und a (da das eine Basis ist) $\Rightarrow$ Die Codimension des Raums muss größer als Eins sein ↯.

$\chi(a) \neq 1 \Rightarrow$

$$\varphi(a) \sum_\chi \chi(a) = \sum_{\varphi\chi} (\varphi\chi)(a) = \sum_\chi \chi(a) \qquad \blacksquare$$

Alternativer Beweis von Gleichung 2.1:
Für $a \neq 1$ existieriert χ mit $\chi(a) \neq 1$.

Die χ bilden in $\mathrm{L}^2((\mathbb{Z}/m\mathbb{Z})^*, \mathbb{C})$ eine ON-Basis. Wäre $\chi(a) = 1$ für alle χ, so würde folgen $\chi(a) = \chi(1)\ \forall\chi \Rightarrow f(a) = f(1)$ ↯ $\forall f \in \mathrm{L}^2$

Sei also $\rho(a) \neq 1$

$$\rho(a) \sum_\chi \chi(a) = \sum_\chi (\chi\rho)(a) = \sum_\chi \chi(a)$$

todo: hier fehlt was

Beispiel 2.1

1. $m = 4$ $(\mathbb{Z}/m\mathbb{Z})^*$ hat zwei Elemente: 1, 3.

$$\chi_0(x) = 1 \quad \text{für alle } x$$
$$\chi_1(1) = 1, \chi_1(3) = -1$$

Oder $\chi_1\colon \mathbb{Z} \to \mathbb{C}$ mit

$$\chi_1(m) = \begin{cases} 1 & m \equiv 1 \pmod 4 \\ -1 & m \equiv 3 \pmod 4 \\ 0 & \text{sonst} \end{cases}$$

2. $m = 8$ $(\mathbb{Z}/m\mathbb{Z})^* = c_2 \times c_2$ Es gibt drei nichttriviale Charaktere

	1	3	5	7
χ_1	1	-1	1	-1
χ_2	1	1	-1	-1
χ_3	1	-1	-1	1

3. $m = 7$ $(\mathbb{Z}/m\mathbb{Z})^* = c_6$ Erzeuger ist z. B. 3. Es gibt einen Charakter der Ordnung 2 (=Legendre-Symbol), 2 Charaktere der Ordnung 3, 2 Charaktere der Ordnung 6.

2.1.1 Dirichlet-Reihen

Die Mutter aller Dirichlet-Reihen ist die Riemannsche Zetafunktion

Definition 2.2

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, s > 1$$

Fakt 2.4

1. $\zeta\colon (1,\infty) \to \mathbb{R}$ ist wohldefiniert und stetig
2. todo: hier fehlt was

Beweis:

1.
2. $\zeta(s) \geq 1 + \frac{1}{2^s} + 2\frac{1}{4^s} + 4\frac{1}{8^s} + \cdots + 2^{N-1}\frac{1}{2^{Ns}}$ ζ ist stetig monoton fallend in s, also

$$\liminf_{s \to 1+0} \zeta(s) \geq 1 + \frac{1}{2} + 2\frac{1}{4} + \cdots + 2^{N-1}\frac{1}{2^N} = 1 + \frac{N}{2} \to \infty$$

3.

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s}\,dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}\,dt$$

$$\Longrightarrow \zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s}\,dt\right) = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\,dt$$

Sei $\varphi_n(s) = \int_n^{n+1}(n^{-s} - t^{-s})\,dt$. $|\varphi_n(s)| \leq \sup_{n \leq t \leq n+1} |n^{-s} - t^{-s}|$.

$|n^{-s} - t^{-s}| = n^{-s} - t^{-s}$ auf $[n, n+1]$, Ableitung ist $st^{-s-1} \Rightarrow |n^{-s} - t^{-s}| \leq \frac{s}{\tau^{s+1}}$ mit $\tau \in [n, n+1]$, d. h. die Reihe $\sum \varphi_n(s)$ konvergier absolut und gleichmäßig auf jedem Intervall $[\varepsilon, \infty)$. Inbesondere existiert todo: hier fehlt was. ∎

Definition 2.3

$$\zeta(s) = \prod_{p\in\mathbb{P}} (1 - \frac{1}{p^s})^{-1}, s > 1$$

Beweis:
Sei

$$\begin{aligned} a_N = a_N(s) &= \prod_{p\leq N} (1 - \frac{1}{p^s})^{-1} \\ &= \prod_{p\leq N} \sum_{k=0}^{\infty} \frac{1}{p^{ks}} \\ &= \sum \frac{1}{n^s} \end{aligned}$$

n läuft über alle natürlichen Zahlen > 0, welche keine Primteiler $> N$ besitzen. Also $0 < \zeta(s) - a_N \leq \sum_{n>N} \frac{1}{n^s}$. Die RHS geht gegen null für $N \to \infty$ ∎

Fakt 2.5 (Euler)

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$$

Beweis:
log ist stetig, also gilt

$$\lim_{s\to 1+0} \log \zeta(s) = \infty$$

$$\log \zeta(s) = \sum_{p\in\mathbb{P}} -\log(1 - \frac{1}{p^2}) = \sum_{p\in\mathbb{P}} \sum_{m=1}^{\infty} \underline{todo : hier fehlt was}$$

$$= \sum_{p\in\mathbb{P}} \frac{1}{p^s} + \sum_{p\in\mathbb{P}} \sum_{m=2}^{\infty} \frac{1}{mp^{ms}}$$

Die zweite Summe ist

$$\leq \sum_{p\in\mathbb{P}} \sum_{m\geq 2} \frac{1}{p^{ms}} = \sum_{p\in\mathbb{P}} \frac{1}{p^{2s}} \frac{1}{1 - \frac{1}{p^s}} = \sum_{p\in\mathbb{P}} \frac{1}{p^s(p^s - 1)}$$

$$\leq \sum_{p\in\mathbb{P}} \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

Das gilt für alle $s > 1$.

Es folgt $\lim_{s\to 1+0} \sum \frac{1}{p^s} = \infty$.

Da $\sum_{p\leq N} \frac{1}{p} \geq \sum_{p\leq N} \frac{1}{p^s}$ gilt, folgt $\sum \frac{1}{p} = \infty$ ∎

Bemerkung 2.2
Wir zeigen den Dirichletschen Primzahlsatz in der folgenden Art:

$$\sum_{p \equiv a (\mathrm{mod}^* m)} \frac{1}{p} = \infty$$

Definition 2.4
Sei $m \geq 1$, χ Dirichlet-Charakter $\mathrm{mod}^* m$, dann ist die Dirichletsche **L-Reihe** $L(s, \chi)$ definiert durch

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

Fakt 2.6
Ist $\chi = \chi_0 \equiv 1$, so ist

$$L(s, \chi_0) = \prod \textit{todo : hier fehlt was}$$

Insbesondere ist $\lim_{s \to 1+0} L(s, \chi_0) = \infty$.

Beweis:
Wie für ζ sieht man:

$$L(s, \chi_0) = \prod_{p \nmid m} (1 - \frac{1}{p^s})^{-1}$$

∎

Fakt 2.7
Sei $\chi = \chi_0$, dann konvergiert $L(s, \chi)$ sogar für alle $s > 0$ (allergdings nicht absolut).

Beweis:

$$\sum_{n=M}^{N} a_n b_n = \sum_{n=M}^{N-1} s_n (b_n - b_{n+1}) + s_N b_N$$

mit $s_n = a_M + a_{M+1} + \cdots + a_n$.

Wir wenden das an auf $\sum_M^N \frac{\chi(n)}{n^s} = s_{M,N}$. Dies ist also gleich

$$s_{M,N} = \sum_{n=M}^{N-1} s_n (\frac{1}{n^s} - \frac{1}{(n+1)^s}) + s_N \cdot \frac{1}{N^s}$$

$$s_n = \sum_{a=M}^{n} \chi(a)$$

wegen $\chi \neq \chi_0$ und Orthogonalität folgt $|s_n|$ todo: hier fehlt was

∎

Bemerkung 2.3
Die Konvergenz ist also sogar gleichmäßig für alle $s \geq \varepsilon > 0$. Insbesondere sind die $L(s,\chi), \chi \neq \chi_0$ stetige Funktionen auf $(0,\infty)$.

Fakt 2.8

$$L(s,\chi) = \prod_{p\in\mathbb{P}} (1 - \frac{\chi(p)}{p^s})^{-1} \quad \forall s > 1$$

Beweis:
Wie für ζ. ∎

Fakt 2.9
Für $s > 1$ gilt

$$\log L(s,\chi) = \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s} + R(s,\chi)$$

und $R(s,\chi)$ ist beschränkt für $s \to 1 + 0$.

Beweis:

$$\sum_{p,m} \frac{\chi(p)^m}{m p^{ms}} = \sum -\log(1 - \frac{\chi(p)}{p^s}) = \log L(s,\chi)$$

(Man sieht leicht: Definiert man $\log L(s,\chi)$ durch die LHS, so gilt $c^{\log L(s,\chi)} = L(s,\chi)$.)

Wie für ζ sieht man

$$\sum_{p\in\mathbb{P}} \sum_{m\geq 2} |\frac{\chi(p)^m}{p^{ms}}| \leq 1 \quad \forall s \geq 1$$ ∎

Folgerung 2.1
Sei a prim zu m, dann gilt

$$\sum_{p\equiv a(\mathrm{mod}^*\, m)} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_{\chi mod^* m} \overline{\chi}(a) \log L(s,\chi) + R(s)$$

mit $R(s)$ beschränkt für $s \to 1 + 0$.

$$\sum_{\chi \,\mathrm{mod}^*\, m} \overline{\chi}(a) \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s} = \sum_{p\in\mathbb{P}} \frac{1}{p^s} \sum_{\chi} \underbrace{\overline{\chi}(a)\chi(a)}_{\chi(a^{-1}p)}$$

Satz 2.1 (Dirichlet)

$$\sum_{p \equiv a (\mathrm{mod}^* m)} \frac{1}{p} = \infty$$

Bemerkung 2.4
Wenn wir wissen, dass $L(1, \chi) \neq 0$ ist $\forall \chi \neq \chi_0$, dann folgt dies sofort: log ist stetig, also $\lim_{s \to 1+0} \log L(s, \chi) = \log L(1, \chi)$. Also

$$\sum_{p \equiv a (\mathrm{mod}^* m)} \frac{1}{p^s} = \frac{1}{\varphi(m)} \log L(1, \chi_0) + R_1(s)$$

mit $R_1(s)$ beschränkt für $s \to 1+0$. $\lim_{s \to 1+0} \log L(s, \chi_0) = \infty$. Also $\lim_{s \to 1+0} \sum_{p \equiv a (\mathrm{mod}^* m)} \frac{1}{p^s} = \infty \Rightarrow \sum_{p \equiv a (\mathrm{mod}^* m)} \frac{1}{p} = \infty$

Kern des Problems: Man zeige, $L(1, \chi) = 0 \, \forall \chi \neq \chi_0$. Mindestens drei Methoden:

1. Mit Funktionentheorie (E. Landau)

2. Mit elementaren Methoden (ziemlich verwickelt)

3. Man zeigt, das $L(1, \chi)$ arithmetische Bedeutung hat: Gruppenordnung.

2.2 Das Nichtverschwinden von $L(1, \chi)$ für $\chi \neq \chi_0$

Fakt 2.10
Sei $\chi \neq \chi_0$. Dann ist $L(s, \chi)$ auf $(0, \infty)$ sogar stetig differenzierbar und es gilt

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

Beweis:
Wir zeigen, dass die Reihe rechts gleichmäßig für $s \geq \delta > 0$ konvergiert.

$$s_{M,N} = \sum_{n=M}^{N} \frac{\chi(n)\ln n}{n^s} = \sum_{n=M}^{N-1} s_n\left(\frac{\ln n}{n^s} - \frac{\log(n+1)}{(n+1)^s}\right) + \frac{s_N \ln N}{N^s}$$

$$s_n = \sum_{x=M}^{n} \chi(x)$$

$$|s_{M,N}| \leq \varphi(m)\left(\sum_{n=M}^{n+1} \left|\frac{\ln n}{n^s}\right| - \frac{\ln(n+1)}{(n+1)^s} + \frac{\ln N}{N^s}\right)$$

$$\varphi\colon [1,\infty) \to \mathbb{R}\colon t \mapsto \frac{\ln t}{t^s}, s \geq \delta > 0$$

$$\varphi'(t) = \frac{1}{t^{s+1}} - s\frac{\ln t}{t^{s+1}} = (1 - s\ln t)t^{-s-1}$$

$\varphi'(t) = 0$ für $t = e^{\frac{1}{s}}$ und < 0 für $t > e^{\frac{1}{s}}$. Also ist φ streng monoton fallend für $t \geq e^{\frac{1}{\delta}}$.

$$\Rightarrow |s_{M,N}| \leq \varphi(m)\frac{\ln M}{M}$$

$\Rightarrow$ Reihe konvergiert gleichmäßig für $s \geq \delta$. ∎

Fakt 2.11
Sei $\zeta_m(s) := \prod_{\chi(\mathrm{mod}^* m)} L(s,\chi)$ $(s > 1)$. Dann ist $\zeta_m(s)$ reell und ≥ 1.

Beweis:

$$\begin{aligned}
\ln \zeta_m(s) &= \sum_{\chi} \ln L(s,\chi) \\
&= \sum_{\chi} \sum_{p\in\mathbb{P}} \sum_{r=1}^{\infty} \frac{\chi(p)^r}{p^{rs}} = \sum_{p\in\mathbb{P}} \sum_{r=1}^{\infty} \frac{1}{rp^{rs}} \sum_{\chi} \underbrace{\chi(p)^r}_{\chi(p^r)} \\
&= \sum_{r=1}^{\infty} \sum_{p^r \equiv 1(\mathrm{mod}^* m)} \varphi(m)\frac{1}{rp^{rs}} \geq 0 \\
&\Rightarrow \zeta_m(s) \geq 1.
\end{aligned}$$

todo: hier fehlt was ∎

betrachte

$$\frac{\zeta_m(s)}{s-1} = (s-1)L(s,\chi)\frac{L(s,\chi)}{s-1}\frac{L(s,\overline{\chi})}{s-1}\prod L(s,\chi')$$

Rechts haben alle Faktoren endlichen Grenzwert für $s \to 1+0$ im Widerspruch zu $\zeta_m(s) \geq 1$.

2.3 Elementarer Beweis von $L(1,\chi) \neq 0$ für reelles χ

(d'après ГЕЛБФОНД 1956)

Sei also $\chi \neq \chi_0$, $\chi^2 = \chi_0$ Charakter $(\mathrm{mod}^* m)$.

$$F(t) := \sum_{n=1}^{\infty} \chi(n) \frac{t^n}{1-t^n}$$

F konvergiert absolut für $0 < t < 1$: klar.

Es folgt

$$\begin{aligned} F(t) &= \sum_{n=1}^{\infty} \chi(n) \sum_{m=1}^{\infty} t^{mn} \\ &= \sum_{N=1}^{\infty} d_\chi(N) t^N \quad \text{mit } d_\chi(N) = \sum_{d|N} \chi(d) \end{aligned}$$

Fakt 2.12

1. d_χ ist muliplikativ, d. h. für $\mathrm{ggT}(r,s) = 1$ gilt $d_\chi(rs) = d_\chi(r) d_\chi(s)$
2. $d_\chi(n) \geq 0$
3. $d_\chi(n^2) \geq 1$

Beweis:

1. $\delta \mid rs \Leftrightarrow \delta = \kappa\nu$ und $\kappa \mid r, \nu \mid s$.

$$d_\chi(rs) = \sum_{\delta|rs} \chi(\delta) = \sum_{\kappa|r} \sum_{\nu|s} \chi(\kappa\nu) = d_\chi(r) d_\chi(s)$$

2. nun noch für Primzahlpotenzen wegen (i): Ist $n = p^k$, so ist $d_\chi(n) = \chi_(1) + \chi(p) + \cdots + \chi(p)^k$. Für $p \mid m$ ist $\chi(p) = 0$, also $d_\chi(n) = 1$. Für $\chi(p) = +1$ ist $\delta_\chi(p^k) = k+1$. Für $\chi(p) = -1$ ist $d_\chi(p^k) = \begin{cases} 0 & 2 \nmid k \\ 1 & 2 \mid k \end{cases}$
3. folgt sofort ∎

Folgerung 2.2

$$\lim_{t \to 1-0} F(t) = \infty$$

Beweis:
$F(t)$ hat die Minorante $\sum_{n=1}^{\infty} t^{n^2}$, diese divergiert für $t \to 1-0$:

$$\sum_{1}^{N} t^{n^2} \to N \Rightarrow \liminf F(t) \geq N \quad \forall N$$

Wir nehmen nun an: $L(1,\chi) = 0$. Sei $\varphi_n(t) = \frac{1}{n(n-t)} - \frac{t^n}{1-t^n}, 0 < t < 1$. Dann gilt

$$F(t) = -\sum_{n=1}^{\infty} \chi(n)\varphi_n(t)$$

Es gilt $\varphi_n(t) \geq \varphi_{n+1}(t)\ \forall t \in (0,1)$.

$$\begin{aligned}(1-t)(\varphi_n(t)) - \varphi_{n+1}(t) &= \frac{1}{n} - \frac{1}{n+m} - (1-t)\frac{t^n}{1-t^n} + (1-t)\frac{t^{n+1}}{1-t^{n+1}} \\ &= \frac{1}{n(n+1)} - (1-t)\frac{t^n(1-t^{n+1}) - t^{n+1}(1-t^n)}{(1-t^n)(1-t^{n+m})} \\ &= \frac{1}{n(n+1)} - \frac{t^n(1-t)^2}{(1-t^n)(1-t^{n+m})} \\ &= \frac{1}{n(n+1)} - \frac{t^n}{(1+t+\cdots+t^{n-1})(1+t+\cdots+t^n)}\end{aligned}$$

Zwischenrechnung:

$$1 + t + \cdots + t^{n-1} \geq n\sqrt[n]{t^{\frac{n(n-1)}{2}}} = nt^{\frac{n-1}{2}}$$
$$1 + t + \cdots + t^n \geq (n+1)t^{\frac{n}{2}}$$

Also:

$$(1-t)(\varphi_n(t) - \varphi_{n+1}(t)) \geq \frac{1}{n(n+1)} - \frac{1}{n(n+1)}\frac{t^n}{t^{n-\frac{1}{2}}} = \frac{1}{n(n+1)}(1-t^{\frac{1}{2}}) > 0$$

Wir wenden auf $\sum \chi(n)\varphi_n(t)$ ABELsche Summation an

$$\sum_{n=1}^{N} \chi(n)\varphi_n(t) = \sum_{n=1}^{N-1} s_n(\chi)(\varphi_n(t) - \varphi_{n+1}(t)) + s_N(\chi)\varphi_N(t)$$
$$\Rightarrow |\sum_{n=1}^{N} \chi(n)\varphi_n(t)| \leq \varphi(m) \sum_{n=1}^{N-1} (\varphi_n(t) - \varphi_{n+1}(t)) + \varphi_N(t) = \varphi(m)\varphi_1(t)$$
$$\varphi_1(t) = \frac{1}{1-t} - \frac{t}{1-t} = 1$$

Also

$$|\sum_{n=1}^{N} \chi(n)\varphi_n(t)| \leq \varphi(n) \quad \forall N \geq 1$$

im Widerspruch zu $\lim_{t\to 1-0} F(t) = \infty$. ∎

3 Quadratische Zahlenkörper

3.1 Grundbegriffe

Definition 3.1
Ein **quadratischer Zahlenkörper** $\mathbb{Q}(\sqrt{D}), D \in \mathbb{Z}, D \notin \{0,1\}$ D **quadratfrei** ist definiert als Menge durch

$$\mathbb{Q}(\sqrt{D}) = \{\alpha + \beta\sqrt{D} \colon \alpha, \beta \in \mathbb{Q}\} \subseteq \mathbb{C}$$

Fakt 3.1
$\mathbb{Q}(\sqrt{D})$ ist Körper.

Beweis:
Das die Addition, Subtraktion und Multiplikation nicht aus dem Körper führen ist klar.
$\frac{1}{\alpha+\beta\sqrt{D}} = \frac{\alpha-\beta\sqrt{D}}{\alpha^2-D\beta^2}$ D quadratfrei impliziert $\alpha^2 - D\beta^2 \neq 0$. ∎

Bemerkung 3.1

1. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D})$ und $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{D}) = 2$
2. Für $D_1 \neq D_2$ ist $\mathbb{Q}(\sqrt{D_1}) \neq \mathbb{Q}(\sqrt{D_2})$

Fakt 3.2
Auf $\mathbb{Q}(\sqrt{D})$ existiert ein Automorphismus

$$\sigma \colon \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}(\sqrt{D}) \colon \alpha + \beta\sqrt{D} \mapsto \alpha - \beta\sqrt{D}$$

Es gilt:

1. $\sigma(a \pm b) = \sigma(a) \pm \sigma(b)$
2. $\sigma(ab) = \sigma(a)\sigma(b)$
3. $\sigma^2 = Id$

Definition 3.2
Für $D > 1$ heißt $\mathbb{Q}(\sqrt{D})$ **reellquadratisch**. todo: hier fehlt was

$$N \colon \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}, \quad N(a) = a \cdot \sigma(a)$$
$$Tr \colon \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}, \quad Tr(a) = a + \sigma(a)$$

Bemerkung 3.2

$$N(\alpha + \beta\sqrt{D}) = \alpha^2 - D\beta^2$$
$$N(ab) = N(a)N(b)$$
$$N(\alpha a) = \alpha^2 N(a) \quad \text{für } \alpha \in \mathbb{Q}^*$$
$$Tr(\alpha + \beta\sqrt{D}) = 2\alpha$$
$$Tr(a \pm b) = Tr(a) \pm Tr(b)$$
$$Tr(\alpha a) = \alpha Tr(a) \quad \text{für } \alpha \in \mathbb{Q}$$

3.2 Die ganzen Gaussschen Zahlen

Definition 3.3
Sei $\mathbb{Z}[i] := \{a + bi \colon a, b \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{-1})$ $(\sqrt{-1} = i)$.

1. Einheiten von $\mathbb{Z}[i]$ sind $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

   Denn $\varepsilon = a + bi$ Einheit bedeutet, $\varepsilon \cdot \eta = 1$ für ein $\eta \in \mathbb{Z}[i] \Rightarrow N(\varepsilon)N(\eta) = 1$ $(a^2 + b^2)(c^2 + d^2) = 1$ mit $a, b, c, d \in \mathbb{Z}$.

2. Teilbarkeit: $x, y \in \mathbb{Z}[i], x \mid y :\Leftrightarrow \exists z \in \mathbb{Z}[i], y = xz$

3. $\pi \in \mathbb{Z}[i], \pi \neq 0$, keine Einheit heißt Primzahl $:\Leftrightarrow$ die einigen Teiler sind die Einheiten und π mal Einheiten.

Fakt 3.3
Seien $a, b \in \mathbb{Z}[i], b \neq 0$, dann existieren $q, r \in \mathbb{Z}[i]$, so dass

$$a = qb + r$$
$$N(r) < N(b)$$

Beweis:
Sei $x = \frac{a}{b} \in \mathbb{Q}(i)$. $\mathbb{Z}[i]$ bildet in $\mathbb{C}$ ein quadratisches Gitter, also existiert ein $q' \in \mathbb{Z}[i]$, so dass x in dem Quadrat mit der linken unteren Ecke q' liegt. todo: Bild mit Quadrat Der Abstand von x zu mindestens einer Ecke ist $\leq \frac{1}{2}\sqrt{2} < 1$. Diese Ecke heiße q. Dann ist $\frac{a}{b} = x = q + s$ und $N(s) \leq (\frac{1}{2}\sqrt{2})^2 = \frac{1}{2} < 1$. Es folgt $a = qb + r, N(r) = N(bs) < N(b)$ ∎

Folgerung 3.1
Zu je zwei Zahlen $a, b \in \mathbb{Z}[i]$, wobei mindestens eine $\neq 0$ ist, existiert der größte gemeinsame Teiler, d. h. eine ganze Zahl $d =: (a, b) =: \mathrm{ggT}(a, b)$, so dass

1. $d \mid a, d \mid b$
2. für $\delta \mid a, \delta \mid b$ folgt $\delta \mid d$.

d ist bis auf Einheiten eindeutig bestimmt.

Beweis:
Siehe todo: link: Kapitel 1 ∎

Definition 3.4
$x, y \in \mathbb{Z}[i]$ heißen **assoziiert** :$\Leftrightarrow$ unterscheiden sich nur um Einheiten

Folgerung 3.2
Sei π Primzahl und $\pi \mid a \cdot b$ $(a, b \in \mathbb{Z})$, dann folgt $\pi \mid a$ oder $\pi \mid b$.

Beweis:
Nehmen wir an $\pi \mid a$: Der Euklid'sche Algorithmus für a, π:

$$\begin{aligned} a &= q_0\pi + r_0 \\ \pi &= q_1 r_0 + r_1 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

$r_n = \mathrm{ggT}(a, \pi) \Rightarrow r_n =: \varepsilon$ ist eine Einheit.

Wir multiplizieren alle Gleichungen mit b und erhalten so einen Euklid'schen Algorithmus für ab und πb:

$$N(r_j b) = N(r_j)N(b) < N(r_{j-1})N(b) = N(r_{j-1}b)$$

Also gilt $(ab, \pi b) = \varepsilon b$.

π teil ab, $\pi b \Rightarrow \pi \mid \varepsilon b \Rightarrow \pi \mid b$ ∎

Fakt 3.4
In $\mathbb{Z}[i]$ gilt der Hauptsatz der elementaren Arithmetik: Jede Zahl $\neq 0$ ist eindeutig darstellbar als Produkt von Primzahlpotenzen (bis auf das Vorzeichen und die Reihenfolge.)

Beweis:
Jede Zahl $\neq 0$ ist Produkt von Primzahlen: Ist $a = bc$ mit b, c keine Einheit, so ist $N(b), N(c) < N(a)$. Eindeutigkeit: $\pi_1 \cdots \pi_m = \pi_1' \cdots \pi_n'$. π_1 teile RHS, also ist π_1 assoziert zu einem der π_j' auf der LHS. Wir kürzen die heraus $\Rightarrow$ IV. ∎

Fakt 3.5

1. Jede Primzahl π in $\mathbb{Z}[i]$ teilt genau eine Primzahl $p \in \mathbb{P}$.
2. Die Norm einer Primzahl $\pi \in \mathbb{Z}[i]$ ist gleich p oder p^2.

Beweis:

1. π teilt ganze Zahlen $\neq 0$ aus $\mathbb{Z}$: z. B. $m = N(\pi) = \pi\overline{\pi}$.

   Sind $a, b \in \mathbb{Z}$ und $(a, b) = 1$ in $\mathbb{Z}$, so ist auch $(a, b) = 1$ in $\mathbb{Z}$. Begründung: Sei $x \in \mathbb{Z}[i], x \mid a, x \mid b$ in $\mathbb{Z}[i] \Rightarrow a = ux, b = vx \Rightarrow a^2 = N(u)N(x), b^2 = N(v)N(x) \Rightarrow N(x) \mid a^2, N(x) \mid b^2$ in $\mathbb{Z}$.

$(a^2, b^2) = 1$ in $\mathbb{Z} \Rightarrow N(x) = 1 \Rightarrow x$ ist eine Einheit.

Wenn $\pi \mid m$, dann $\pi \mid \prod p^{a_p(m)} \Rightarrow \exists! p\colon \pi \mid p^{a_p(m)}$. $p = \pi_1 \cdots \pi_r \Rightarrow \pi = \pi_j \Rightarrow \pi \mid p$.

$\Rightarrow p^2 = N(\pi_1) \cdots N(\pi_r)$ Da LHS ganze Zahlen sind, sind also nur möglich:

a) $p = \pi$ ist Primzahl in $\mathbb{Z}[i]$ und $N(\pi) = p^2$

b) $p = \pi_1 \cdot \pi_2$ mit zwei Primzahlen $\pi_1, \pi_2 \in \mathbb{Z}[i]$ und dann $N(\pi_1) = N(\pi_2) = p$.

Aus $\pi \mid p$ folgt $\overline{\pi} \mid p$. Also zwei Unterfälle:

i. $\overline{\pi} = \varepsilon\pi, \varepsilon \in \mathbb{Z}[i]^*$, dann ist $p = \varepsilon\pi^2$

ii. $\overline{\pi}$ ist nicht assoziert zu π, dann ist $p = \pi \cdot \overline{\pi}$. ∎

Beispiel 3.1

1. $2 = -i(1+i)^2, \pi_2 = 1 + i, 2 = -i\pi_2^2$
2. $3 = \pi \cdot \overline{\pi}, \pi = a + bi \Rightarrow 3 = N(\pi) = a^2 + b^2$ geht nicht. $\Rightarrow 3$ bleibt prim
3. $5 = (2+i)(2-i) \Rightarrow \pi_5 = 2 + i$ ist Primzahl

Fakt 3.6 (Zerlegungsgesetz der rationalen Primzahlen in $\mathbb{Z}[i]$)

1. 2 ist bis auf Vorzeichen Quadrat der Primzahl $1 + i$.
2. Die Primzahlen $p \equiv 1 \pmod 4$ zerfallen in Produkte zweier nicht assoziierter Primzahlen:

$$p = \pi_p \cdot \overline{\pi_p}, \quad \pi_p \not\simeq \overline{\pi_p}$$

3. Die Primzahlen $p \equiv 3 \pmod 4$ bleiben prim in $\mathbb{Z}[i]$.

Beweis:

1. letztes Beispiel
2. Sei also $p \equiv 1 \pmod 4$. $\exists a, b \in \mathbb{Z}$, so dass $p = a^2 + b^2 = (a + bi)(a - bi) = \pi \cdot \overline{\pi} \Rightarrow$ $\pi \cdot \overline{\pi}$ Primzahlen in $\mathbb{Z}[i]$.

   π und $\overline{\pi}$ sind nicht assoziiert: $a + bi = \varepsilon(a - bi), \varepsilon \in \mathbb{Z}[i]^*$

   $\varepsilon = 1 \Rightarrow b = 0$ ↯
   $\varepsilon = -1 \Rightarrow a = 0$ ↯
   $\varepsilon = i \Rightarrow a = b \Rightarrow p = 2a^2$ ↯
   $\varepsilon = -i \Rightarrow a = -b \Rightarrow p = 2a^2$ ↯
3. Sei also $p \equiv 3 \pmod 4$ und $p = \pi \cdot \overline{\pi}, \pi \not\simeq \overline{\pi}$ ($p = \varepsilon\pi \cdot \overline{\pi}$ impliziert $\varepsilon = 1$) $\pi = a + bi \Rightarrow p = a^2 + b^2$ ↯

   $\pi = \varepsilon\pi^2 = \varepsilon(a + bi)^2$
   $p^2 = (a^2 + b^2)^2 \Rightarrow p = a^2 + b^2$ ↯ $\Rightarrow p$ prim in $\mathbb{Z}[i]$. ∎

3.3 Ganze Zahlen in quadratischen Zahlkörper

Eine fundamentale Definition:

Definition 3.5
$x = \alpha + \beta\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ heißt **ganz** := Norm und Spur sind aus $\mathbb{Z}$.

Beispiel 3.2
$x \in \mathbb{Q}(i), x = \alpha + \beta i$ ist ganz $\Leftrightarrow \alpha^2 + \beta^2 \in \mathbb{Z}, 2\alpha \in \mathbb{Z}$. Setze $\alpha = \frac{1}{2}a, a \in \mathbb{Z} \Rightarrow \alpha^2 = \frac{a^2}{4} \Rightarrow \beta^2 \in \frac{1}{4}\mathbb{Z} \Rightarrow \beta = \frac{1}{2}b, b \in \mathbb{Z} \Rightarrow \alpha^2 + \beta^2 = \frac{a^2+b^2}{4}$. $a^2 + b^2 \equiv 0 \pmod 4$ gdw a und b gerade $\Rightarrow \alpha, \beta \in \mathbb{Z}$. Also ganze Zahlen $= \mathbb{Z}[i]$.

Fakt 3.7
Sei $K = \mathbb{Q}(\sqrt{D}), D \neq 0{,}1$ quadratfrei. Für $D = 2{,}3 \pmod 4$ ist $x = \alpha + \beta\sqrt{D}$ ganz $\Leftrightarrow \alpha, \beta \in \mathbb{Z}$.

Für $D = 1 \pmod 4$ ist x ganz $\Leftrightarrow x = \frac{1}{2}(a + b\sqrt{D}), a, b \in \mathbb{Z}, a \equiv b \pmod 2$.

Beweis:
x ganz $\Leftrightarrow 2\alpha \in \mathbb{Z}, \alpha^2 - D\beta \in \mathbb{Z}, \alpha = \frac{1}{2}a, a \in \mathbb{Z}, \frac{a^2}{4} - D\beta^2 \in \mathbb{Z} \Rightarrow D\beta^2 \in \frac{1}{4}\mathbb{Z}$. Also auch $\beta = \frac{1}{2}b, b \in \mathbb{Z}$.

Zwischenbilanz: x ganz $\Leftrightarrow x = \frac{1}{2}(a + b\sqrt{D})$ mit $a, b \in \mathbb{Z}$, $a^2 - Db^2 \equiv 0 \pmod 4$.

Sei $D \equiv 1 \pmod 4$: $\Leftrightarrow a^2 \equiv b^2 \pmod 4 \Leftrightarrow a \equiv b \pmod 2$.

$D \equiv 2 \pmod 4$: $a^2 \equiv Db^2 \pmod 4 \Rightarrow a$ gerade $\Rightarrow a^2 \equiv 0 \pmod 4 \Leftrightarrow b$ gerade.

$D \equiv 3 \pmod 4$: $a^2 \equiv -b^2 \pmod 4 \Leftrightarrow a, b$ gerade ∎

Folgerung 3.3
Die Menge O_K der ganzen Zahlen in $K = \mathbb{Q}(\sqrt{D})$ ist gleich

- $\mathbb{Z} \cdot 1 + \mathbb{Z}\sqrt{D} = \{a + b\sqrt{D} \colon a, b \in \mathbb{Z}\}$ für $D = 2{,}3 \pmod 4$
- $\mathbb{Z} \cdot 1 + \mathbb{Z}\frac{1+\sqrt{D}}{2} = \{a + b\frac{1+\sqrt{D}}{2} \colon a, b \in \mathbb{Z}\}$ für $D \equiv 1 \pmod 4$.

Folgerung 3.4
O_K ist kommutativer Ring mit 1, integer, der O_K ist K. O_K ist bezüglich Addition freie abelsche Gruppe mit Basis. $1, \sqrt{D}$ für $S \equiv 2{,}3 \pmod 4$: $1, \frac{1+\sqrt{D}}{2}$ für $D \equiv 1 \pmod 4$.

Bezeichnung:

$$\omega = \begin{cases} \sqrt{D} & D \equiv 2{,}3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod 4 \end{cases}$$

Beispiel 3.3

$$(\frac{1+\sqrt{D}}{2})^2 = \frac{(1+\sqrt{D}^2}{)}\ 4 = \frac{1+D+2\sqrt{D}}{4} = \frac{1}{2}(\underbrace{\frac{1+D}{2}}_{\in\mathbb{Z}} + \sqrt{D})$$

Definition 3.6
Die **Diskriminante** von $K = \mathbb{Q}(\sqrt{D})$ ist $d_K = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega) \\ \mathrm{Tr}(\omega) & \mathrm{Tr}(\omega^2) \end{pmatrix}$

Bemerkung 3.3
Für eine andere Ganzheitsbasis (=Basis der additiven Gruppe von O_K) kommt dasselbe heraus.

(ÜA: Zeige

$$\begin{pmatrix} \mathrm{Tr}(\omega_1^2) & \mathrm{Tr}(\omega_1\omega_2) \\ \mathrm{Tr}(\omega_1\omega_2) & \mathrm{Tr}(\omega_2^2) \end{pmatrix} = d_K$$

Fakt 3.8
Für $D \equiv 1 \pmod 4$ ist $d_K = D$ und für $D \equiv 2{,}3 \pmod 4$ ist $d_k = 4D$.

Beweis:
$D = 1 \pmod 4, \mathrm{Tr}(1) = 2, \mathrm{Tr}(\omega) = 1, \mathrm{Tr}(\omega^2) = \mathrm{Tr}(\frac{1+D}{4} + \frac{\sqrt{D}}{2}) = \frac{1+D}{2}$

$$\det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{pmatrix} = D$$

$D \equiv 2{,}3 \pmod 4, \mathrm{Tr}(\omega) = 0, \mathrm{Tr}(\omega^2) = 2D$

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D$$

■

Bemerkung 3.4

1. $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d_K})$.
2. Die quadratischen Zahlenkörper isnd eindeutig duch ihre Diskriminanten bestimm:
   - Ist $d_K \equiv 1 \pmod 4$, so ist $D = d_k$.
   - Ist $d_K \equiv 0 \pmod 4$, so ist $D = \frac{1}{4}d_k$.
3. Die Mende aller d_K ist also charakterisiert: Entweder ist $d_K \equiv 1 \pmod 4$ und quadratfrei oder $d_K \equiv 0 \pmod 4$, $\frac{d_k}{4}$ quadratfrei und $\equiv 2{,}3 \pmod 4$.
4. Man nummeriert die quadratischen Zahlenkörper gern durch ihrer Diskriminanten statt durch die D.

Beispiel 3.4

1. reellquadratische Zahlenkörper:

D	2	3	5	6	7	10
d_K	8	12	5	24	28	40

2. imaginarquadratische Zahlenkörper:

D	-1	-2	-3	-5	-6	-7	-10
d_K	-4	-8	-3	-20	-24	-7	-40

3.4 Einheiten

Wir bestimmen die Gruppe E_K (oder auch U_K) der Einheiten in O_K.

Fakt 3.9
$\varepsilon = a + b\omega \in \mathrm{O}_K$ ist Einheit $\Leftrightarrow N(\varepsilon) = \pm 1$.

Beweis:
Ist $N(\varepsilon) = \varepsilon\sigma(\varepsilon) = \pm 1$, so ist ε Einheit. Sei $\varepsilon \cdot \eta = 1$ für ein $\eta \in \mathrm{O}_K \Rightarrow N(\varepsilon) \cdot N(\eta) = 1$
$\Rightarrow N(\varepsilon) = \pm 1$. ∎

Beispiel 3.5
$x^2 = 13y^2 + 1$ $N(x + \sqrt{13}y) = 1$ Viel Hokuspokus, den ich nicht verstehe, und wir erhalten:
$18^2 - 13 \cdot 5^2 = -1$

$\varepsilon = 18 + 5\sqrt{13}$, $\varepsilon^2 = 649 - 180\sqrt{13}$, $N(\varepsilon^2) = 1$.

Fakt 3.10
Sei $d_K < 0$, dann gibt es in O_K nur folgende Einheiten:

$$O_K^* = \begin{cases} \{\pm 1, \pm i\} & d_K = -4 \\ \{\pm 1, \pm e^{\frac{2\pi i}{6}}, \pm (e^{\frac{2\pi i}{6}})^2\} & d_K = -3 \\ \{\pm 1\} & d_K < -4 \end{cases}$$

Beweis:
$d_K = -4$ hatten wir bereits

sei $d_K = -3$ $\omega = \frac{1+\sqrt{-3}}{2}$, $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab + b^2\omega\overline{\omega} = a^2 + ab + b^2$

$N(x) \geq 0 \forall x \in O_K \Rightarrow$ Lösungen von $a^2 + ab + b^2 = 1$

a	± 1	0	1	-1
b	0	± 1	-1	1

Es gilt: $\omega^6 = 1, \omega^3 = -1$

Sei $d_K < -4$, also $D < 0, D \neq -1, -3$ Sei $d_K \equiv 1 \pmod 4 \Rightarrow D \leq -7$

$$\begin{aligned} N(a+b\omega) &= a^2 + ab + b^2\omega\overline{\omega} \\ &= a^2 + ab + \underbrace{\frac{1-D}{4}}_{\geq 2} b^2 \\ &= (a + \frac{1}{2}b)^2 + \underbrace{(\frac{1-D}{4} - \frac{1}{4})}_{>1} b^2 = 1 \end{aligned}$$

$\Rightarrow b = 0$

Sei $d_K \equiv 0 \pmod 4, D \leq -2, N(a+b\omega) = a^2 - Db^2 = 1 \Rightarrow b = 0.$ ∎

Satz 3.1
Sei $d_K > 0, E_K = O_K^*$. Dann existiert eine eindeutig bestimmte Eiheit $\varepsilon_K > 0$ in E_K, Oder: E_K ist direktes Produkt einer zyklischen Gruppe der Ordnung 2 (nämlich ± 1) und einer unendlichen zyklischen Gruppe (nämlich $\{\varepsilon^m : m \in \mathbb{Z}\}$).

ε_K heißt **Fundamentaleinheit** von K.

Beweis:
Sei $K = Q(\sqrt{D}), D > 1$, quadratfrei. Die geometrische Abbildung ist $K \to \mathbb{R}^2 : \alpha \mapsto (\alpha, \alpha')$. Sie ist offensichtlich injektiv. Das Bild von O_K ist ein Gitter in $\mathbb{R}^2$. Es besteht aus den $\mathbb{Z}$-Linearkombinationen von (1,1) und (ω, ω'). Diese beiden Vektoren sind $\mathbb{R}$-linear unabhängig. Inbesondere ist das Bild von O_K diskret: In jeder beschränkten Teilmenge von $\mathbb{R}^2$ liegen nur endlich viele Gitterpunkte: Annahme: $|x| \leq c, |x'| \leq c$ für $x \in O_K$, $x = a + b\omega$, sei $\omega = \sqrt{D}$, es gilt:

$$\begin{aligned} |x + x'| &\leq 2c & \qquad |x - x'| &\leq 2c \\ |a| &\leq c & \qquad |b|\sqrt{D} &\leq c \end{aligned}$$

Analog für $\omega = \frac{1+\sqrt{D}}{2}$.

$\varepsilon \in O_K \Rightarrow$ Bild von ε liegt auf den 4 Hyperbelästern $xy = \pm 1$. Abbildung 3.1

Angenommen, es gibt Einheiten $\neq \pm 1$. Diese treten als Quartett auf: $\varepsilon, \frac{1}{\varepsilon}, -\varepsilon, -\frac{1}{\varepsilon}$. Also genau eine > 1.

Betrachten alle $\eta \in E_K$ mit $\eta > 1$. Unter diesen gibt es eine kleinste. Sei ihr Name ε und η weiter Einheit > 1. Dann existier eine natürliche Zahl n, so dass $\varepsilon^n \leq \eta < \varepsilon^{n+1}$ gilt $(\varepsilon^n \to \infty) \Rightarrow 1 \leq \eta\varepsilon^{-n} < \varepsilon \Rightarrow \eta = \varepsilon^n$. ∎

Der Kern des Beweises: Existenz nichttrivialer Einheiten.

Lemma 3.1
$\forall t \in \mathbb{R} \forall n > 1 \exists a, b \in \mathbb{Z}, b > 0$ so, dass $|t - \frac{a}{b}| < \frac{1}{nb}$ und $b \leq n$.

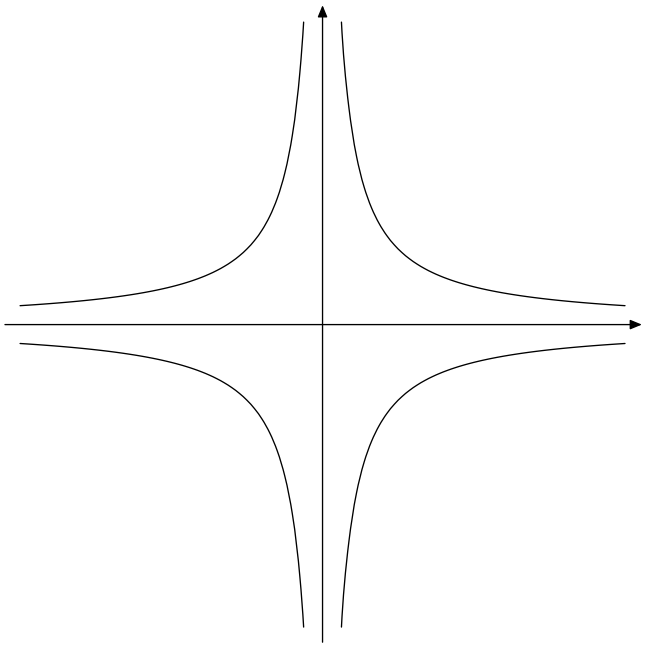


Abbildung 3.1: todo: Was ist das eigentlich?

BEWEIS:
Betrachte die $n+1$ Zahlen bt, $b = 0{,}1, \ldots, n$. Sei $a = [bt]$, dann gilt

$$0 \leq bt - a < 1$$

Wir unterteilen $[0{,}1)$ in $[\frac{k}{n}, \frac{k+1}{n})$, $k = 0{,}1, \ldots, n-1$. Also existieren zwei Zahlen $bt - a$, die im selben Unterintervall liegen:

$$|(b_1 t - a_1) - (b_2 t - a_2)| < \frac{1}{n}$$
$$\Rightarrow |t - \frac{a_1 - a_2}{b_1 - b_2}| < \frac{1}{n|b_1 - b_2|}$$

und $1 \leq |b_1 - b_2| \leq n$. ∎

Bemerkung 3.5
z. B.

$$|\pi - \frac{22}{7}| = 0{,}001\,264 \ldots |\pi - \frac{1}{700}| \qquad = 0{,}001\,428 \ldots$$

→ Theorie der DIOPHANTischen Approximationen.

Folgerung 3.5
Sei $n \geq 1$ fixiert, dann existiert $\alpha \in O_K, \alpha \neq 0$ so, dass

$$|\alpha| < \frac{1}{n}$$
$$|N(\alpha)| \leq 1 + 2\sqrt{D}$$

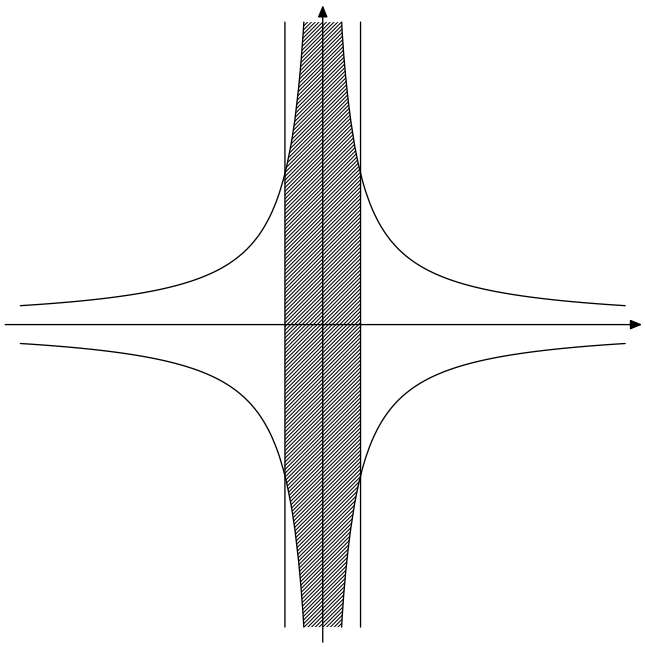


Abbildung 3.2: todo: Was ist das?

Beweis:
Setze $t = \omega$, nach dem Lemma 3.1 existieren ganze Zahlen $a, b \in \mathbb{Z}$ mit $0 < b \leq n$ und $|\omega + \frac{a}{b}| < \frac{1}{bn} \Rightarrow |a + b\omega| < \frac{1}{n}$.

Sei $\alpha := a + b\omega', \alpha \neq 0$ wegen $b > 0$. $N(\alpha) = \alpha\alpha', \alpha' = a + b\omega' = a + b\omega + b(\omega' - \omega)$.

$$\omega = \sqrt{D} \qquad \Rightarrow \omega' - \omega = -2\sqrt{D}$$
$$\omega = \frac{1+\sqrt{D}}{2} \qquad \Rightarrow \omega' - \omega = -\sqrt{D}$$

Also folgt $|\alpha| < \frac{1}{n} + 2b\sqrt{D} \leq \frac{1}{n} + 2n\sqrt{D} \Rightarrow N(\alpha) = |\alpha\alpha'| < \frac{1}{n^2} + 2\sqrt{D} \leq 1 + 2\sqrt{D}$. ∎

Bemerkung 3.6
Geometrische Deutung Abbildung 3.2 Man kann den Schlauch um $x = 0$ immer schmaler machen, aber man findet immer ganze Zahlen.

Beweis: (Existenz nichttrivialer Einheiten)
Es existieren unendlich viele Einheiten $\alpha \in O_K, \alpha \neq 0, |N(\alpha)| \leq c \ (= 1 + 2\sqrt{D})$. Also existiert auch eine ganze Zahl $m \in \mathbb{Z}$ mit $0 < m \leq c$, so dass für unendlich viele $\alpha \in O_K$ gilt $|N(\alpha)| = m$.

Wir betrachten für diese $\alpha = a + b\omega$ die zugehörigen Restklassen von a und b modulo m. Dies unterteilt die α in m^2 disjunkte Teilmengen. Wenigstens eine von ihnen enthält

unendliche viele α. Wir wählen zwei verschiedene aus: α, β und dürfen vorrausetzen $\beta \neq -\alpha$. Also gilt

$$|N(\alpha)| = |N(\beta)| = m$$
$$\alpha \equiv \beta \pmod{m} \quad \text{im obigen Sinne}$$
$$\alpha \neq \pm\beta$$

Aus Existenz nichttrivialer Einheiten 61 folgt $\alpha = \beta + m\gamma$ mit $\gamma \in O_K$. Also auch $\alpha\beta' = N(\beta) + m\gamma\beta'$.

$N(\beta) = \pm m \Rightarrow \alpha\beta' = m\delta, \delta = \beta'\gamma \pm 1 \in O_K \Rightarrow N(\alpha\beta') = m^2 N(\delta)$ und $N(\alpha\beta') = \pm m^2$

Somit ist δ eine Einheit.

Angenommen $\delta = \pm 1$, dann folgt

$$\alpha\beta' = \pm m \Rightarrow \alpha\beta\beta' = \pm m\beta$$
$$\pm m\alpha = \pm m\beta$$
$$\Rightarrow \alpha = \pm\beta \text{`}$$

Somit ist δ nichttriviale Einheit. ∎

Beispiel 3.6

D	Fundamentaleinheit
2	$1 + \omega$
3	$2 + \omega$
5	ω
6	$5 + 2\omega$
7	$8 + 3\omega$
10	$3 + \omega$

Beispiel 3.7

D	Fundamentaleinheit
15	$74335 + 3588\omega$
67	$48842 + 5967\omega$
94	$2143295 + 221064\omega$
2006	$638145 + 14248\sqrt{2006}$

3.5 Multiplikative Arithmetik in O_K – Ideale

Die Arithmetik in den O_K ist nicht so leicht wie in $\mathbb{Z}$ oder $\mathbb{Z}[i]$.

Beispiel 3.8
$K = Q(\sqrt{5}), d_K = -20$ Es gilt $21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$. Wir zeigen: $3{,}7, 4 \pm \sqrt{-5}$ sind Primzahlen in O_K.

$N(3) = 9$, hätte 3 den nichttrivialen Teiler $x = a + b\sqrt{-5}$ (also x keine Einheit und $\neq \pm 3$), so wäre $N(x) = 3 \Rightarrow a^2 + 5b^2 = 3$ – hat keine $\mathbb{Z}$-Lösungen.

Analog für $a^2 + 5b^2 = 7$.

$N(4 \pm \sqrt{-5}) = 21$, echte Teiler hätten Norm 3 oder 7. $\lightning$

Idee von Kummer zur Rettung der Arithmetik in O_K: Man nehme zu den Elementen von O_K noch ideale Zahlen hinzu, so dass die Eindeutigkeit wieder vorhanden ist: $3 = \mathfrak{p}_1 \cdot \mathfrak{p}_2, 7 = \mathfrak{p}_3 \cdot \mathfrak{p}_4, 4 + \sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, 4 - \sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$.

3.6 Fundamentaleinheiten und Kettenbrüche

3.6.1 Allgemeine Theorie der Kettenbrüche

Kettenbrüche im Englischen continues fractions.

Definition 3.7
Seien a_0, a_1 Unbestimmte. Ein Kettenbruch sieht dann so aus:

$$[a_0; a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{+\cdots}}}$$

Bemerkung 3.7

1. Sind die a_n positive natürliche Zahlen für $n \geq 1$, so ist das eine rationale Zahl.
2. Dind die a_n positive reelle Zahlen für $n \geq 1$, so ist das eine reelle Zahl.
3. $[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}$ mit $p_n, q_n \in \mathbb{Z}$-Polynome in den a_i

$$[a_0] = a_0 = \frac{a_0}{1}, [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$$

Fakt 3.11
Setzt $p_{-1} = 1, q_{-1} = 0, p_0 = a_1, q_0 = 1$. Dann gilt:

1. $p_{n+2} = a_{n+2}p_{n+1} + p_n$
2. $q_{n+2} = a_{n+2}q_{n+1} + q_n$
3. p_n, q_n teilerfremd in $\mathbb{Z}[a_0; a_1, \ldots, a_n]$

Beweis:
Induktion: $\frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}$ – stimmt.

$\frac{p'_n}{q'_n} = [a_0; a_1, \ldots, a_n]$.

$$\frac{p_{n+2}}{q_{n+2}} = a_0 + \frac{1}{\frac{p'_{n+1}}{q'_{n+1}}} = \frac{a_0 p'_{n+1} + q'_{n+1}}{p'_{n+1}}$$

Rechts sind Zähler und Nenner teilerfremd, also

$$\begin{aligned} p_{n+2} &= a_0 p'_{n+1} + q'_{n+1} \\ q_{n+2} &= p'_{n+1} \end{aligned} \tag{3.1}$$

Es folgt

$$p_{n+2} = a_0(a_{n+2}p'_n + p'_{n-1}) + a_{n+2}q'_n + q'_{n-1} = a_{n+2}\underbrace{(a_0 p'_n + q'_n)}_{p_{n+1}} + \underbrace{(a_0 p'_{n-1} + q'_{n-1})}_{=p_n}$$

Analog für q_{n+2}. Teilerfremdheit folgt aus Gleichung 3.1. ∎

Folgerung 3.6
Sind die $a_n \in \mathbb{N}^*$ für $n \geq 1$, so sind die oben rekursiv definierten Zahlen p_n und q_n auch teilerfrem (in $\mathbb{Z}$).

Fakt 3.12
Seien $a_0, a_1, \ldots \in \mathbb{Z}, \forall j \geq 1 \colon a_j > 0$.

1. p_n, q_n streng monoton wachsend,
2. $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$
3. $p_n q_{n+2} - p_{n+2} q_n = (-1)^{n+1} a_{n+2}$
4. Die Brüche mit geradem Index sind streng monoton wachsend, die mit ungeradem Index sind streng monoton fallend
5. $\frac{p_n}{q_n}$ konvergiert

Beweis:
1. folgt aus Fakt 3.11
2. $p_0 q_1 - p_1 q_0 = a_0 a_1 - (a_0 a_1 + 1) = -1$

$$\begin{aligned} p_n q_{n+1} - p_{n+1} q_n &= p_n(a_{n+1} q_n + q_{n-1}) - (a_{n+1} p_n - p_{n-1}) q_n \\ &= p_n q_{n-1} - p_{n-1} q_n \end{aligned}$$

3. $p_{-1}q_1 - q_{-1}q_1 = a_1 - 0 = a_1$

$$\begin{aligned} p_n q_{n+2} - p_{n+2}q_n &= p_n(a_{n+2}q_{n+1} + q_n) - q_n(a_{n+2}p_{n+1} + p_n) \\ &= a_{n+2}(p_n q_{n+1} - p_{n+1}q_n) \end{aligned}$$

Zum Schluss nochmal den 2. Punkt anwenden.

4.

$$\frac{p_n}{q_n} - \frac{p_{n+2}}{q_{n+2}} = \frac{(-1)^{n+1}a_{n+2}}{q_n q_{n+2}}$$

5. Wir zeigen: Beide Folgen sind beschränkt

$$\begin{gathered} \frac{p_{2r}}{q_{2r}} < \frac{p_{2n}}{q_{2n}} \qquad \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2s+1}}{q_{2s+1}} \quad \text{für } n \gg 1 \\ \frac{p_{2n}}{q_{2n}} - \frac{p_{2n+1}}{q_{2n+1}} = \frac{(-1)^{2n+1}}{q_{2n}q_{2n+1}} = -\frac{1}{q_{2n}q_{2n+1}} \\ \frac{p_{2n}}{q_{2n}} + \frac{1}{q_{2n}q_{2n+1}} = \frac{p_{2n+1}}{q_{2n+1}} \end{gathered}$$

$\Rightarrow$ Beide Folgen konvergent

$$\left|\frac{p_{2n}}{q_{2n}} - \frac{p_{2n+1}}{q_{2n+1}}\right| = \frac{1}{q_{2n}q_{2n+1}} \xrightarrow{n\to\infty} 0$$

■

3.6.2 Kettenbrüche zu reellen Zahlen

Fakt 3.13
Sei $\alpha \in \mathbb{R}$, wir definieren rekursiv zwei Folgen a_n und α_n durch

$$\begin{aligned} \alpha &= a_0 + \frac{1}{a_1}, a_1 > 1, a_0 = [\alpha] \\ \alpha_n &= a_n + \frac{1}{\alpha_{n+1}}, \alpha_{n+1} > 1, a_n = [\alpha_n] \end{aligned}$$

Solange, wie $a_n \neq \alpha_n$ ist.

1. Der Prozess stoppt $\Leftrightarrow \alpha \in \mathbb{Q}$
2. Im Fall $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ gilt $\frac{p_n}{q_n} \to \alpha$; d. h. Kettenbrüche eignen sich genauso gut wie Dezimalzahlen zur Approximation von irrationalenhelp: heißen die irrational? Zahlen. Sie konvergieren sogar schneller als Dezimalzahlen ($\to$ besser als Dezimalzahlen), aber dafür ist die Addition kompliziert.
3. $\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n] = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$

4. $|a_n - \alpha_n| < 1$

BEWEIS:

1. Sei n so, dass $\alpha_n = a_n \Rightarrow \alpha = [a_0; a_1, \ldots, a_n] \in \mathbb{Q}$.

   Sei $\alpha \in \mathbb{Q}, \alpha_n = \frac{p}{q}, p < q$

   $$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} = a_n + \frac{p'}{q}, p' < q$$

   $\Rightarrow \alpha_{n+1} = \frac{q}{p'} \Rightarrow$ der Nenner von α_{n+1} ist kleiner als der Nenner von α_n.

2. $$\begin{aligned}\alpha - \frac{p_{n+1}}{q_{n+1}} &= \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} - \frac{p_n a_{n+1} + p_{n-1}}{q_n a_{n+1} + q_{n-1}} \\ &= \frac{(p_n\alpha_{n+1} + p_{n-1})(q_n a_{n+1} - q_{n-1}) - (p_n a_{n+1} + p_{n-1})(q_n\alpha_{n+1} + q_{n-1})}{(q_n\alpha_{n+1} + q_{n+1})(q_n a_{n+1} + q_{n-1})} \\ &= \frac{(p_n q_{n-1} - q_n p_{n-1})}{} \textit{todo : hier fehlt was}\end{aligned}$$

3. folgt aus Fakt 3.11. $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$

   $\Rightarrow [a_0; a_1, \ldots, a_{n-1}, \alpha_n] = [a_0; a_1, \ldots, a_n + \frac{1}{\alpha_{n+1}}]$ ∎

Folgerung 3.7

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}}$$

BEWEIS:

$$|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = \frac{1}{q_n q_{n+1}}$$

α liegt dazwischen ∎

Folgerung 3.8 (The law of the best approximation)
Sei $\alpha \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}, p \in \mathbb{Z}, q \in \mathbb{N}^*, \text{ggT}(p, q) = 1$.

Dann ist $\frac{p}{q}$ ein Näherungsbruch der Kettenbruchentwicklung von α.

BEWEIS:
Sei $\frac{a}{b}$ weiterer Bruch, $\text{ggT}(a, b) = 1, a \in \mathbb{Z}, b \in \mathbb{N}^*$, sowie $\frac{a}{b} \neq \frac{p}{q}$, $|b\alpha - a| \leq |q\alpha - p| < \frac{1}{2q}$.

Wir zeigen. Damit ist $b > q$:

$$\frac{1}{bq} \leq |\frac{a}{b} - \frac{p}{q}| \leq |\frac{a}{b} - \alpha| + |\alpha - \frac{p}{q}| < \frac{1}{2bq} + \frac{1}{2q^2} = \frac{a+b}{2bq^2}$$

$\Rightarrow 2q < q + b \Rightarrow b > q$

Fall 1: $\frac{p}{q}$ liegt zwischen zwei Näherungsbrüchen, ist verschieden von ihnen: todo: zeichnung $\frac{p_0}{q_0}$, $\frac{p_2}{q_2}$, $\frac{p_4}{q_4} \to \alpha \leftarrow \frac{p_3}{q_3}$, $\frac{p_1}{q_1}$

Also $\frac{p}{q}$ zwischen $\frac{p_{n-1}}{q_{n-1}}$ und $\frac{p_{n+1}}{q_{n+1}}$

$$\frac{1}{qq_{n-1}} \leq |\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}| < |\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}} \Rightarrow q > q_n$$

$$\frac{1}{qq_{n+1}} < |\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}| \leq |\alpha - \frac{p}{q}| \Rightarrow \frac{1}{q_{n+1}} \leq |\alpha q - p|$$

Nach Fakt 3 und Folgerung ist $|\alpha q_n - p_n| < \frac{1}{q_{n+1}} \Rightarrow |\alpha q_n - p_n| < |\alpha q - p|, q_n < q$.
Das ist ein Wiederpruch zu der Aussage oben.

Fall 2: $\frac{p}{q} < \frac{p_0}{q_0}$ oder $> \frac{p_1}{q_1} \to$ Übungsaufgabe ∎

Beispiel 3.9
$e = [2; 1,2,1,1,4,1,1,6,1,1, \dots]$ Für π hat man noch keinen Kettenbruch gefunden.

Fakt 3.14
Sei $D \equiv 2,3 \pmod 4$, quadratfrei, $D \neq 2,3$. $\varepsilon = a + b\sqrt{D}$ Fundamentaleinheit von $\mathbb{Q}(\sqrt{D})$. (Dann ist $a > 0, b > 0, a, b \in \mathbb{Z}$). Dann gilt:

$$|\sqrt{D} - \frac{a}{b}| < \frac{1}{2b^2}$$

Beweis:
$N_\varepsilon = (a - b\sqrt{D})(a + b\sqrt{D}) = \pm 1$, also

$$|\sqrt{D} - \frac{a}{b}| = \frac{1}{b(a + b\sqrt{D})} = \frac{1}{b^2(\frac{a}{b} + \sqrt{D})}$$

$\frac{a}{b} + \sqrt{D} > \sqrt{D} > 2$ ∎

Folgerung 3.9
$\varepsilon = p_n + q_n\sqrt{D}$, wobei $\frac{p_n}{q_n}$ der erste Näherungsbruch todo: hier fehlt was

Beispiel 3.10
$D = 22$

$$\sqrt{22} = 4 + (\sqrt{22} - 4)$$
$$\frac{1}{\sqrt{22} - 4} = \frac{\sqrt{22} - 4}{6} = 1 + \frac{\sqrt{22} - 2}{6}$$

todo : hierkommtnochwas

Ergebnis: $\sqrt{22}$ hat einen periodischen Kettenbruch

$$\sqrt{22} = [2; \overline{1,2,4,2,1,8}]$$

n	-1	0	1	2	3	4	5	6
a_n		4	1	2	4	2	1	8
p_n	1	4	5	14	61	136	197	$*$
q_n	0	1	1	3	13	29	42	$*$
$p_n^2 - 22q_n^2$	1	-6	3	-2	3	-6	1	

$\varepsilon_K = 197 + 42\sqrt{22}$ $\sqrt{13} = [3; \overline{1,1,1,1,6}]$

Dinge die auffallen: 1,2,4,2,1 sind symetrisch, die letzte Ziffer ist immer das Doppelte der ersten, in der Tabelle ergibt sich immer die Fundamentaleinheit.

$$\sqrt{2003} = [44; \overline{1,3,12,1,1,6,2,1,2,1,3,6,7,1,43,1,7,6,3,1,2,1,2,6,1,1,12,3,1,88}]$$
$$\text{Fundamentaleinheit: } 4\,344\,427\,204\,728\,362 + 97\,071\,569\,134\,791 \cdot \sqrt{2003}$$

3.6.3 Die Kettenbruchentwicklung reellquadratischer irrationaler Zahen

Sei $K = \mathbb{Q}(\sqrt{D}), D > 1$, quadratfrei. Sei $\alpha \in K \setminus \mathbb{Q}$, dann existiert eine eindeutig bestimmte $a, b, c \in \mathbb{Z}$ mit

1. $a > 0$
2. $\mathrm{ggT}(a, b, c) = 1$
3. $a\alpha^2 + b\alpha + c = 0$

Definition 3.8
Die **Diskriminante** $\mathrm{Disc}(\alpha)$ ist $:\Leftrightarrow \mathrm{Disc}(\alpha) = b^2 - 4ac$. Es gilt $\mathrm{Disc}(\alpha) > 0$.

Definition 3.9
$\alpha \in K \setminus \mathbb{Q}$ heißt **reduziert** $:\Leftrightarrow \alpha > 1, -1 < \alpha' < 0$ ($a = r + s\sqrt{D} \Rightarrow \alpha' = r - s\sqrt{D}, r, s \in \mathbb{Q}$)

Bemerkung 3.8
1. Äquivalent: $\alpha > 1, -\frac{1}{\alpha'} > 1$
2. Mit α ist auch $-\frac{1}{\alpha'}$ reduziert
3. $\sqrt{D}$ ist nicht reduziert, $-\sqrt{D} < -1$

4. Sei $\alpha = (\sqrt{D} - [\sqrt{D}])^{-1}, \alpha > 1, \alpha' = \frac{1}{-\sqrt{D}-[\sqrt{D}]} < 0, \alpha' > -1$ ist auch klar.

Fakt 3.15
Für eine gegebene natürliche Zahl m existieren nur endlich viele redzierte Zahlen α_i mit $\mathrm{Disc}(\alpha_i) = m$.

Beweis:
Sei α reduziert und $\mathrm{Disc}(\alpha) = m$.

$$\alpha = \frac{-b + \varepsilon\sqrt{m}}{2a}, \quad \varepsilon \in [-1,1]$$

Für $\varepsilon = -1$ folgt $-b - \sqrt{m} > 0, \alpha' = \frac{-b+\sqrt{m}}{2a} < 0$. Widerspruch. Also $\varepsilon = +1$. Dann folgt

$$-b + \sqrt{m} > 2a > b + \sqrt{m} \qquad (0 > \alpha' > -1)$$

Somit ist $b < 0$ und $0 < -b < \sqrt{m}$. Also nur endlich viele b. $2a < -b + \sqrt{m}, a > 0 \Rightarrow$ nur endlich viele a. $m = b^2 - 4ac \Rightarrow$ nur endlich viele c. ∎

Definition 3.10
Sei $GL(2,\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M(2,2;\mathbb{Z})\colon \det = \pm 1\}$.

6 ist unendlich: $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ hat undenliche Ordnung.

$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ ist Torsionselement. Sei $\alpha \in K\backslash\mathbb{Q}$ $g_n := \left(\begin{smallmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{smallmatrix}\right), \det g_n = (-1)^{n+1}$

Wir hatten gesehen

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$$

$GL(2,\mathbb{Z})$ operiert auf $K \setminus \mathbb{Q}$ vermöge

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha := \frac{a\alpha + b}{c\alpha + d}$$

(gebrochenlineare Substitutionen)

Definition 3.11
$\alpha, \beta \in K \setminus \mathbb{Q}$ heißen **äquivalent** $:\Leftrightarrow \exists g \in GL_2\mathbb{Z}\colon \beta = g\alpha$.

Bemerkung 3.9
Ist $\alpha \in K\backslash\mathbb{Q}$ und α_n der n-te Rest der Kettenbruchentwicklung, also $\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n]$, so ist α_n äquivalent zu α.

Fakt 3.16
Sei $\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n]$ wie oben, dann ist die Diskriminante von α_n gleich der von α.

BEWEIS:
Setze $h_n = \left(\begin{smallmatrix} a_n & 1 \\ 1 & 0 \end{smallmatrix}\right) \in GL_2\mathbb{Z}$

$$h_n(\alpha_{n+1}) = \frac{a_n\alpha_{n+1}+1}{\alpha_{n+1}} = a_n + \frac{1}{\alpha_{n+1}} = \alpha_n$$

Das heißt $h_n(\alpha_{n+1}) = \alpha_n$.

Wir zeigen: Die zahlen β und $\gamma = \frac{m\beta+1}{\beta}$ haben dieselbe Diskriminante ($m \geq 1$).

Sei dazu $a\gamma^2 + b\gamma + c = c. \Rightarrow a(m\beta+1)^2 + b(m\beta+1)\beta + c\beta^2 = 0 \Rightarrow (\underbrace{am^2+bm+c}_{=A})\beta^2 + (\underbrace{2am+b}_{=B})\beta + \underbrace{a}_{=C} = 0.$

$$\begin{aligned} B^2 + 4AC &= 4a^2m^2 + 4abm + b^2 - 4a^2m^2 - 4abm - 4ac \\ &= b^2 - 4ac \end{aligned}$$

Das heißt Disc(β) teil Disc(γ)

Die analoge Recchnugn für γ und $\beta = \left(\begin{smallmatrix} m & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1}$ zu γ. todo: hfw ∎

Fakt 3.17

1. Ist α reduziert, so auch alle α_n.

2. Die α_n sind reduziert für $n \gg 1$.

BEWEIS:

1. $\alpha = a_n + \frac{1}{\alpha_{n+1}}$ ($a_n = [\alpha_n]$), $\alpha_{n+1} > 1$.

   Ist $\alpha > 1$, $-1 < \alpha < 0$ und β definiert durch $\alpha = [\alpha] + \frac{1}{\beta}$, so ist $\beta > 1$ und $-\frac{1}{\beta'} = [\alpha] - \alpha' > 1$

2. $$\begin{aligned} \alpha &= \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-1}} \Rightarrow \\ \alpha_n &= \frac{q_{n-2}\alpha - p_{n-2}}{-q_{n-1}\alpha + p_{n-1}} \qquad (-I \text{ operiert trivial}) \\ \alpha_n' &= \frac{q_{n-2}\alpha' - p_{n-2}}{-q_{n-1}\alpha' + p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}} \frac{\alpha' - \frac{p_{n-2}}{q_{n-2}}}{\alpha' - \frac{p_{n-1}}{q_{n-1}}} \end{aligned}$$

   Der rechte Bruch geht gegen 1, also $\alpha_n' < 0$ für $n \gg 1$. $\alpha_n > 1$ ist klar.

$$\begin{aligned}
\alpha'_n &= -\frac{q_{n-2}}{q_{n-1}}\Big(\underbrace{\frac{\alpha' - \frac{p_{n-1}}{q_{n-1}}}{\alpha' - \frac{p_{n-1}}{q_{n-1}}}}_{=1} + \frac{\frac{p_{n-1}}{q_{n-1}} - \frac{p_{n-2}}{q_{n-2}}}{\alpha' - \frac{p_{n-1}}{q_{n-1}}}\Big) \\
&= -\frac{q_{n-2}}{q_{n-1}}\Big(1 + \frac{(-1)^n}{q_{n-1}q_{n-2}(\alpha' - \frac{p_{n-1}}{q_{n-1}})}\Big) \\
&= -\frac{1}{q_{n-1}}\Big(\frac{(-1)^n}{q_{n-1}(\alpha' - \frac{p_{n-1}}{q_{n-1}})}\Big)
\end{aligned}$$

$\Rightarrow$

$$\alpha'_{n+1} = \frac{1}{q_{n-1}}\Big(\underbrace{q_{n-1} - q_{n-2}}_{\geq 1} - \underbrace{\frac{(-1)^n}{q_{n-1}(\alpha' - \frac{p_{n-1}}{q_{n-1}})}}_{\to 0}\Big)$$

$\Rightarrow \alpha'_n + 1 > 0$ für $n \gg 1$. ∎

Definition 3.12
$[a_0; a_1, \ldots, a_n]$ heißt **periodisch** $:\Leftrightarrow \exists k > 0, n_0 \in \mathbb{N}$, so dass $\forall n \geq n_0\ a_{n+k} = a_n$. Das minimale k heißt **Periode**.

Der Kettenbruch heißt **reinperiodisch** $:\Leftrightarrow$ für alle $n \geq 0$ gilt $a_{n+k} = a_n$.

Schreibweise: $[a_0; a_1, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+k}}]$ respektive $[\overline{a_0; a_1, \ldots, a_{k-1}}]$.

Beispiel 3.11

$$\begin{aligned}
\sqrt{3} &= 1 + \sqrt{3} - 1 \\
\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} &= 1 + \frac{\sqrt{3}-1}{2} \\
\frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} &= \sqrt{3} + 1 = 2 + (\sqrt{3} - 1) \\
\sqrt{3} &= [1; \overline{1,2}] \\
\sqrt{3} - 1 &= [\overline{1,2}]
\end{aligned}$$

Satz 3.2 (Euler, Lagrange)

1. Für alle $\alpha \in K \setminus \mathbb{Q}$ ist die Kettenbruchentwicklung periodisch
2. Ist α reduziert, so ist sie reinperiodisch.

Beweis:

1. Für $n \gg 1$ ist α_n reduziert und hat dieselbe Diskriminante wie α, als sind dises α_n aus einer endlichen Menge $\Rightarrow \exists n, k$, so dass $a_{n+k} = a_n \Rightarrow a_{m+k} = a_m\ \forall m \geq n$.

2. Ist α reduziert, so auch alle α_n.

$$\alpha_n = [\alpha_n] + \frac{1}{\alpha_{n+1}}$$

Wir zeigen: Sind α, β reduziert und $\alpha = N + \frac{1}{\beta}$ mit positiven natürlichen Zahlen N, so gilt $N = [-\frac{1}{\beta'}]$.

Hieraus würde folgen: α_n ist eindeutig bestimmt durch α_{n+1}

$$\alpha > 1, -1 < \alpha' < 0 \Leftrightarrow -\frac{1}{\alpha'} > 1$$
$$\beta > 1, -1 < \beta' < 0 \Leftrightarrow -\frac{1}{\beta'} > 1$$

$-\frac{1}{\beta'} = N - \alpha' = N + \frac{1}{-\frac{1}{\alpha'}} \Rightarrow [-\frac{1}{\beta'}] = N$ Somit folgt aus $\alpha_{n+k} = \alpha_n$ auch $\alpha_{n-1+k} = \alpha_{n-1}$ und damit $a_{n-1+k} = a_{n-1}$ ∎

Bemerkung 3.10
Die Umkehrung gilt auch: Jeder periodische Kettenbruch konvergiert gegen eine quadratische Irrationalität.

Rein periodisch gegen reduzierte.

$$\alpha = [\overline{a_0; a_1, \ldots, a_n}] \Rightarrow \alpha = [a_0, \ldots, a_n, \alpha]$$

$\Rightarrow \alpha = g\alpha$ für eine $g \in GL_2\mathbb{Z}$.

$\alpha = g\alpha$ ist quadratische Gleichung für α.

Fakt 3.18
Ist α reduziert und $\alpha = [\overline{a_0, \ldots, a_{k-1}}]$, so ist $-\frac{1}{\alpha'} = [\overline{a_{k-1}, a_{k-2}, \ldots, a_0}]$.

Beweis:
$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} \Rightarrow -\frac{1}{\alpha'_{n+1}} = a_n + (-\alpha'_n) \Rightarrow a_n = [-\frac{1}{\alpha'_{n+1}}]$ $(0 < -\alpha'_n < 1$ wegen Red.)

Also $-\frac{1}{\alpha'_k} = [a_k, a_{k-1}, \ldots, a_0, -\frac{1}{\alpha'}]$ Nun ist $\alpha_k = \alpha \Rightarrow -\frac{1}{\alpha} = [a_{k-1}, \ldots, a_0, -\frac{1}{\alpha'}] \Rightarrow -\frac{1}{\alpha'} = [\overline{a_{k-1}, \ldots, a_0}]$. ∎

Fakt 3.19
Ist $\alpha = \sqrt{D}$ mit Nichtquadrat $D > 1$, so gilt mit $g = [\sqrt{D}]$:

$$\alpha = [g, \overline{a_1, \ldots, a_{k-1}, 2g}] = [g, \overline{a_{k-1}, \ldots, a_1, 2g}]$$

Beweis:
$\alpha = g + \frac{1}{\alpha_1}, \alpha_1 > 1, -\frac{1}{\alpha'_1} = g + \alpha$ wegen $\alpha' = -\alpha$. Somit ist $-\frac{1}{\alpha'_1} > 2g > 1$ und damit ist α_1 reduziert. $[-\frac{1}{\alpha'_1}] = 2g$

$$\alpha_1 = [\overline{a_1, \ldots, a_k}], -\frac{1}{\alpha_1} = [\overline{a_k, \ldots, a_1}], a_k = 2g$$
$$\Rightarrow \alpha = -\frac{1}{\alpha'_1} - g = [\underbrace{a_k - g}_{=g}, \overline{a_{k-1}, \ldots, a_1, 2g}]$$ ∎

Fakt 3.20
Sei $D > 1$ quadratfrei, $D \equiv 2{,}3 \pmod 4$. Dann ist für $\sqrt{D} = [g; \overline{a_1, \ldots, a_{k-1}, 2g}]$ die Zahl $\varepsilon = p_{k-1} + q_{k-1}\sqrt{D}$ eine Einheit.

Beweis:

$$\begin{aligned}
\sqrt{D} &= [g; a_1, \ldots, a_{k-1}, [2g, a_1, \ldots, a_?]] \\
&= [g; a_1, \ldots, a_{k-1}, \sqrt{D} + g] \\
&= \frac{p_{n-1}(g + \sqrt{D}) + p_{n-2}}{q_{k-1}(g + \sqrt{D} + q_{k-2})} \\
\Rightarrow &\sqrt{D}(q_{k-1}g + q_{k-2} + q_{k-1}\sqrt{D}) = p_{k-1}g + p_{k-2} + p_{k-1}\sqrt{D} \\
\Rightarrow &Dq_{k-1} = p_{k-1}g + p_{k-2} \qquad q_{k-1} \\
&p_{k-1} = q_{k-1}g + q_{k-2} \qquad p_{k-1}
\end{aligned}$$

$$p_{k-1}^2 - Dq_{k-1}^2 = p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^k$$

$\Rightarrow \varepsilon = pk_{-1} + q_{k-1}\sqrt{D}$ ist Einheit. ∎

Bemerkung 3.11
Die Periodenlänge ist $\leq 2D$.

Wie groß kann eine Fundamentaleinheit werden? $\ln \varepsilon_D \leq \sqrt{D}, \varepsilon_D \leq e^{\sqrt{D}}$.

[Der Abschnitt über Kettenbrüche war nur eingeschoben. Jetzt weiter im Programm.]

help: Sollen die O_K $\mathcal{O}_K$ sein? Kummers Idee: Eine Zahl $x \in O_K$ ist hinsichtlich ihrer Teilbarkeitslehre charakterisiert durch ihre Ringvielfachen, also $x \cdot O_K = (x)$, wobei $x \cdot O_K$ folgende Eigenschaften:

1. bzgl. Addition abelsche Gruppe
2. bzgl. Multiplikation gilt $y \cdot O_K, z \in O_K \Rightarrow yz \in O_K$

Definition 3.13
Eine Teilment $I \subset O_K$ heißt **Ideal** :⇔

1. I ist abelsche Gruppe bzgl. Addition
2. $x \in I, y \in O_K \Rightarrow xy \in I$

Ist $I = O_K$, so heißt I **Hauptideal**

Beispiel 3.12
1. Kleinstes Ieal ist $(0) = 0 \cdot O_K$, größtes ist $O_K = (1) = (\varepsilon)$ für jede Einheit ε.
2. $\mathbb{Z}$ besitzt folgende Ideale: $(m) = m\mathbb{Z}$ für $m = 0{,}1{,}2, \ldots$

Beweis:
Sei $I \subset \mathbb{Z}$ Ideal $\neq 0$, mit $a \in I$ ist auch $a \in I$. I enthält also alle natürliche Zahlen > 0.

Sei m die kleinest. Wir zeigen $I = (m)$. Klar ist $(m) \subset I$, sei $k \in I, K = q \cdot m + r, 0 \leq r < m \Rightarrow r \in I \Rightarrow r = 0$.

Dito für $\mathbb{Z}[i]$: Ein Ring, dessen Ideale alle Hauptideale sind, heißen **Hauptidealring**. ∎

Bemerkung 3.12
Sei $R = O_K$ und I Ideal, dann ist R/I abelsche Gruppe bzgl. Addition.

Multiplikation auf R/I: $(a + I)(b + I) := ab + I$.

Sei

$$\begin{aligned} a + I = a_1 + I \quad &\Leftrightarrow a_1 - a \in I \\ b + I = b_1 + I \quad &\Leftrightarrow b_1 - b \in I \end{aligned}$$

zu zeigen ist $ab - a_1 b_1 \in I$

$$ab - a_1 b_1 = \underbrace{(a - a_1)}_{\in I} b - a_1 \underbrace{(b - b_1)}_{\in I} \in I$$

Der kannonische Homomorphismus $R \to R/I$ ist surjektiv mmit Kern I.

$$1 = 1 + I$$

Traditionelle Schreibweise für Ideale: $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \mathfrak{e}$

Fakt 3.21
Es sei $\mathfrak{p} \subset O_K$ Ideal $\neq 0$, dann hat $\mathfrak{p}$ endlichen Index, d. h. $O_K/\mathfrak{p}$ ist endlich.

Beweis:
Sei $x \in \mathfrak{p}, x \neq 0$. Dann ist auch $xx' \in \mathfrak{p}$. Sei $m = |xx'|$, das ist positive natürliche Zahl. O_K/mO_K ist endlich: Elemente sind $a + b\omega + mO_K, 0 \leq a, b < m$. Es gilt $(m) \subset \mathfrak{p}$, also folgt $(O_K \cdot \mathfrak{p})$ endlich. ∎

Definition 3.14
Die **Absolutnorm** eines Ideals ist

$$\mathbb{N}\mathfrak{p} = \operatorname{card}(O_K/\mathfrak{p})$$

Multiplikation von Idealen: Für Hauptideal klar: $(x)(y) = (xy)$.

Naive Definition: $\mathfrak{ab} = \{ab \colon a \in \mathfrak{a}, b \in \mathfrak{b}\}$. Aber ist dann $a_1 b_1 + a_2 b_2 \in \mathfrak{ab}$? Nein.

Richtige Defintion: $\mathfrak{ab} = \{\sum a_i b_i \colon a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$.

Fakt 3.22
Dies ist dann ein Ideal. Beweis: Übungsaufgabe.

Fakt 3.23
1. $\mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c}$
2. $\mathfrak{ab} = \mathfrak{ba}$
3. $R\mathfrak{p} = \mathfrak{p}$
4. $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$, im Allgemeinen keine Gleichheit.
5. $\mathfrak{a} \subset \mathfrak{b} \Rightarrow \mathfrak{ac} \subset \mathfrak{bc}$
6. $(x)\mathfrak{p} = x\mathfrak{p}$
7. $x \mid y$ in $O_K \Leftrightarrow (y) \subset (x)$

Die Beweise sind einfach.

Fakt 3.24
In O_K gilt: Jede aufsteigende Folge von Idealen stabilisiert sich:

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \Rightarrow \exists n_0 \forall n \geq n_0 \colon \mathfrak{p}_n = \mathfrak{p}_{n_0}$$

(O_K ist **Noethersche Ring**.)

Beweis:
Es folgt $\mathbb{N}\mathfrak{p}_1 \geq \mathbb{N}\mathfrak{p}_2 \geq \cdots$ stabilisiert sich. Genügt zu zeigen: $\mathfrak{a} \subset \mathfrak{b}, \mathbb{N}\mathfrak{a} = \mathbb{N}\mathfrak{b} \Rightarrow \mathfrak{a} = \mathfrak{b}$. Das ist klar. ∎

Fakt 3.25
Sei $\mathfrak{p} \subset O_K$ Ideal $\neq (0)$ und $x \in K$, sowie $x\mathfrak{p} \subset \mathfrak{p}$. Dann folgt $x \in O_K$. (O_K ist **ganzabgeschlosen**.)

Beweis:
$\mathfrak{p} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset O_K$ Nach Vorraussetzung ist

$$\begin{aligned} x\omega_1 &= a\omega_1 + b\omega_2 & a, b \in \mathbb{Z} \\ x\omega_2 &= c\omega_1 + b\omega_2 & c, d \in \mathbb{Z} \end{aligned}$$

Da ω_1, ω_2 $\mathbb{Q}$-linearunabhängig sind, ist die Determinante $\det\left(\begin{smallmatrix} a-x & b \\ c & d-x \end{smallmatrix}\right) = 0$, also $x^2 - (a+d)x + (ad - bc) = 0$. Daraus ergibt sich $\operatorname{Tr} x \in \mathbb{Z}$ und $N(x) \in \mathbb{Z}$ und somit ist $x \in O_K$. ∎

Fakt 3.26
Sei $A \subset O_K$ additive Untergruppe von endlich Index. Dann existieren ganze Zahlen $a, b, c, \in \mathbb{Z}, b > 0, c > 0$, so dass $a + b\omega$ und c eine Basis von A bilden: Jedes Element aus A ist eindeutig darstellbar auf $\mathbb{Z}$-Linearkombination von $a + b\omega$ und c.

Beweis:
Wähle unter allen $r + s\omega$ aus A ein solches mit minimales $s > 0$, wir nennes es $a + b\omega$. Dann sind alle s durch b teilbar:

$$s = qb + r_0, 0 \leq r_0 < b$$

$\Rightarrow r + s\omega - q(a + b\omega) = \star + r_0\omega \in A \Rightarrow r_0 = 0.$

$\mathbb{Z} \cap A$ ist Untermenge in $\mathbb{Z}$.

$\text{card}(O_K/A) = m \Rightarrow mO_K \subset A \Rightarrow A \cap \mathbb{Z} \supset m\mathbb{Z}.$

Also $\mathbb{Z} \cup A = c \cdot \mathbb{Z}$ für ein $c > 0$.

Wir haben a, b, c konstruiert und wissen: $a + b\omega$ und c erzeugen A. Eindeutigkeit ist klar:

$$r(a + b\omega) + sc = r'(a + b\omega) + s'c$$

für $r, s, r', s' \in \mathbb{Z} \Rightarrow b(r - r') = 0 \Rightarrow r' = r \Rightarrow s' = s.$ ∎

Folgerung 3.10
Setzt man noch vorraus, dass $-\frac{c}{2} < a \leq \frac{c}{2}$, so ist diese Basis eindeutig.

Beweis:
Zwei Basen von A haben Übergangsmatrix aus $GL(2, \mathbb{Z})$

$$\begin{pmatrix} a & c \\ b & 0 \end{pmatrix} \underbrace{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}}_{\in GL(2,\mathbb{Z})} = \begin{pmatrix} a' & c' \\ b' & 0 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} \alpha & b \\ \gamma & \delta \end{pmatrix} = \frac{1}{bc} \begin{pmatrix} 0 & -c \\ -b & a \end{pmatrix} \begin{pmatrix} a' & c' \\ b' & 0 \end{pmatrix} = \begin{pmatrix} -\frac{b'}{b} & 0 \\ \frac{ab' - a'b}{bc} & -\frac{c'}{c} \end{pmatrix}$$

$$\Rightarrow c \mid c', b \mid b' \Rightarrow b' = b, c' = c$$

$$\Rightarrow a \equiv a' \pmod{c}, -\frac{c}{2} < a, a' \leq \frac{c}{2} \Rightarrow a = a'$$ ∎

Definition 3.15
$a + b\omega$ und c heißt **kannonische Basis** von A.

Fakt 3.27
Sei $\mathfrak{p} \subset O_K$ Ideal $\neq (0)$, $a + b\omega$ und c seine eine kannonische Bais. Dann gilt

1. $b \mid a$,
2. $b \mid c$ und
3. $bc \mid N(a + b\omega)$

Umgekehrt: Sei $A \subset O_K$ additive Untergruppe von endlich Index mit kannonischer Basis, welche die oberen Eigenschaften erfüllt. Dann ist A ein Ideal.

Beweis:

1. Es gilt $\omega\mathfrak{p} \subset \mathfrak{p}$, also

$$\begin{aligned} \omega(a+b\omega) &= A(a+b\omega) + B \cdot c \\ \omega c &= c(a+b\omega) + D \cdot c \end{aligned}$$

   $A, B, C, D \in \mathbb{Z}$

2. $D_K = 2{,}3 \pmod 4 \Rightarrow \omega^2 = D_K$.

$$\begin{aligned} bD_K &= Aa + Bc & c &= Cb \\ a &= A \cdot b & Ca + Dc &= 0 \end{aligned}$$

   $\Rightarrow b \mid a, b \mid c$.

   $D = -{}^{Ca}/_{c}, A = {}^{a}/_{b}, C = {}^{c}/_{b}$

   $\Rightarrow D = -{}^{ac}/_{bc} = -{}^{a}/_{b}$

$$\begin{aligned} cB = bD_k - Aa = bD_K = {}^{a^2}/_{b^2} = \frac{b^2 - D_K a^2}{b} = -\frac{1}{b}N(a+b\omega) \\ -bcB = N(a+b\omega) \end{aligned}$$

   Analog für $D_K \equiv 1 \pmod 4$ Übungsaufgabe.

3. Sei $A = \mathbb{Z}(a+b\omega) + \mathbb{Z}c$, sowie $b \mid a, b \mid c, bc \mid N(a+b\omega)$. Dann ist A ein Ideal.

   Gzz. $\omega \cdot A \subset A$

$$\begin{aligned} \omega(a+b\omega) &= A(a+b\omega) + Bc & A, B &\in \mathbb{Q} \\ wc &= c(a+b\omega) + Dc & D, C &\in \mathbb{Q} \end{aligned}$$

   Dieselbe Rechnung wie oben nur rückwärst zeigt $A, B, C, D \in \mathbb{Z}$. ∎

Folgerung 3.11
Jedes Ideal $\mathfrak{a} \subset O_K$ hat die Form. $\mathfrak{a} = (b)\mathfrak{b}$, $\mathfrak{b}$ mit kannonischer Basis $a + b\omega$ und c. $-\frac{c}{2} < a \leq \frac{c}{2}$ und $c \mid N(a+b\omega)$

Beweis:
Übungsaufgabe ∎

Fakt 3.28
Sei $\mathfrak{p}$ Ideal mit kannonischer Basis $a + b\omega$ und c. Dann ist $\mathbb{N}\mathfrak{p} = bc$.

Beweis:
$x = r + s\omega, y = r' + s'\omega \in O_K$

$$\begin{aligned} x \equiv y \pmod{\mathfrak{p}} &\Leftrightarrow (r - r') + (s - s')\omega \in \mathfrak{p} \\ &\Leftrightarrow (r - r') + (s - s')\omega = m(a + b\omega) + ncm, n \in \mathbb{Z} \\ &\Leftrightarrow s \equiv s' \pmod{b} \Rightarrow m = \frac{s - s'}{b} \\ &\qquad r - r' \equiv ma \pmod{c} \end{aligned}$$

Also sind die bc Restklassen die Elemente von ${}^{O_k}/_{\mathfrak{p}}$. ∎

Bemerkung 3.13
Mit $\mathfrak{p}$ ist auch $\mathfrak{p}' = \{a' \colon a \in \mathfrak{p}\}$ ein Ideal.

Fakt 3.29 (Hauptfakt)
$\mathfrak{p} \cdot \mathfrak{p}' = (n)$ für eine natürliche Zahl $n \in \mathbb{N}^*$.

Beweis:
Sei $a + b\omega, c$ kannonischer Basis von $\mathfrak{p}$. $\mathfrak{p}\mathfrak{p}'$ besteht aus allen O_K-Linearkomibationen der vier Zahlen $c^2, c(a + b\omega), c(a + b\omega'), N(a + b\omega) = (a + b\omega)(a + b\omega')$. Sei n der ggT (in $\mathbb{Z}$) der ganzen Zahlen (aus $\mathbb{Z}$). $c^2, c \operatorname{Tr}(a + b\omega), N(a + b\omega)$.

Wir zeigen: $\mathfrak{p} \cdot \mathfrak{p}' = (n)$. Jedenfalls ist $n \in \mathfrak{p} \cdot \mathfrak{p}'$ als $\mathbb{Z}$-Linearkomibation der drei Zahlen oben, also $(n) \subset \mathfrak{p} \cdot \mathfrak{p}'$. $c^2, N(a + b\omega) \in (n)$.

Bleibt zu zeigen, das $c(a + b\omega) \in (n) = nO_K \Leftrightarrow \frac{c(a+b\omega)}{n} \in O_K$

$$\begin{aligned} \operatorname{Tr}(\frac{c(a + b\omega)}{n}) = \frac{2ac + bc \operatorname{Tr} \omega}{n} = \frac{c \operatorname{Tr}(a + b\omega)}{n} \in \mathbb{Z} \\ N(\frac{c(a + b\omega)}{n}) = \frac{c^2}{n^2} N(a + b\omega) \in \mathbb{Z} \end{aligned}$$

∎

Ab jetzt ist das Nullideal verboten! [Anm. d. A.: Das war bestimmt vorher auch schon so.]

Für eine kanonische Basis $A \subset O_K$ ist $a+b\omega, c$ mit $b, c > 0$ und $-\frac{c}{2} < a \leq \frac{c}{2}$.

$\mathfrak{p} \subset A \Leftrightarrow b \mid a, b \mid c$ und $bc \mid N(a + b\omega)$

$\mathbb{N}\mathfrak{p} = bc$

Fakt 3.30
$\mathfrak{p} \cdot \mathfrak{p}' = (n)$

Fakt 3.31
Genauer gilt: Das n aus dem vorigen Fakt ist gleich $\mathbb{N}\mathfrak{p} = bc$.

Beweis:
zu zeigen ist, dass $\mathrm{ggT}(c^2, c\,\mathrm{Tr}(a+b\omega), N(a+b\omega)) = bc. \Leftrightarrow \mathrm{ggT}(\frac{c^2}{b}, \frac{c}{b}\,\mathrm{Tr}(\frac{a}{b}+\omega), N(\frac{a}{b}+\omega)) = \frac{c}{b}$

Setze: $c := \frac{c}{b}$ und $a := \frac{a}{b}$.

$$\mathrm{ggT}(c^2, c\,\mathrm{Tr}(a+\omega), N(a+\omega)) = \omega$$

Dabei gilt $-\frac{c}{2} < a \geq \frac{c}{2}$ und $c \mid N(a+\omega)$ Jedenfalls ist c gemeinsamer Teiler.

Gzz. $\mathrm{ggT}(c, \mathrm{Tr}(a+\omega), N(a+\omega))$

Fall 1: $D_K \equiv 2{,}3 \pmod 4$

$\mathrm{ggT}(c{,}2a, \frac{a^2-D_K}{c}) = 1$ Sei c gerade, und $\frac{a^2-D_K}{c}$ gerade, dann ist $s^2 - D_K \equiv 0 \pmod 4 \Rightarrow D_K \equiv a^2 \pmod 4$ ↯

Sei $p > 2$ Primteiler aller drei Zahlen. Dann teilt p^2 die Zahl $a^2 - D_K$ und a^2, mithin teilt p^2 die Zahl D_K ↯

Fall 2: $D_K \equiv 1 \pmod 4$ geht analog. ∎

Folgerung 3.12
$\mathbb{N}(\mathfrak{p}_1\mathfrak{p}_2) = \mathbb{N}\mathfrak{p}_1 \cdot \mathbb{N}\mathfrak{p}_2$

Beweis:
$m = \mathbb{N}\mathfrak{p}_1$ und $n = \mathbb{N}\mathfrak{p}_2$. $\mathfrak{p}_1\mathfrak{p}_1' = (m), \mathfrak{p}_2\mathfrak{p}_2' = (n) \Rightarrow \mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_2\mathfrak{p}_2' = (mn) = (\mathbb{N}(\mathfrak{p}_1\mathfrak{p}_2))$ ∎

Folgerung 3.13
$\mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_1\mathfrak{p}_3 \Rightarrow \mathfrak{p}_2 = \mathfrak{p}_3$

Beweis:
Mutliplikation mit $\mathfrak{p}_1'$ gibt

$$(\mathbb{N}\mathfrak{p}_1) \cdot \mathfrak{p}_2 = (\mathbb{N}\mathfrak{p}_1)\mathfrak{p}_2 \Rightarrow \mathbb{N}\mathfrak{p}_1 \cdot \mathfrak{p}_2 = \mathbb{N}\mathfrak{p}_1\mathfrak{p}_3 \Rightarrow \mathfrak{p}_2 = \mathfrak{p}_3$$ ∎

Folgerung 3.14
$\mathfrak{p}_1 \subset \mathfrak{p}_2 \Rightarrow \exists \mathfrak{p}_3 \colon \mathfrak{p}_1 = \mathfrak{p}_2 \cdot \mathfrak{p}_3$.

Beweis:
Multiplikation mit $\mathfrak{p}_2'$ gibt

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subset \mathfrak{p}_2 \cdot \mathfrak{p}_2' = (\mathbb{N}b) = (m)$$

Also sind alle Elemente aus $\mathfrak{p}_1 \cdot \mathfrak{p}_2'$ in O_K teilbar durch m.

Dies zeigt: $\mathfrak{p}_3 := \frac{1}{m}\mathfrak{p}_1\mathfrak{p}_2'$ ist Ideal in O_K. Also $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3 = \mathfrak{p}_1 \cdot \mathfrak{p}_2'$ wegen $m\mathfrak{p}_3 = \mathfrak{p}_1\mathfrak{p}_2'$. Nach todo: Link: Fogerung 2 impliziert das $\mathfrak{p}_2\mathfrak{p}_3 = \mathfrak{p}_a$ ∎

Fakt 3.32
Für $x \in O_K \setminus \{0\}$ gilt $\mathbb{N}(\,(x)\,) = |N(x)|$.

Beweis:

1. Sei $\omega_1 = a + b\omega$ und $\omega_2 = c + d\omega$ eine $\mathbb{Z}$-Basis von $\mathfrak{p} \subset O_K$, $\mathfrak{p}$ ist Ideal. Dann gilt $\mathbb{N}\mathfrak{p} = |\det(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix})|$. Wir wissen das für die kanonische Basis von $\mathfrak{p}$. Die RHS ist dieselbe für jede Basis von $\mathfrak{p}$.

2. Sei $x = a + b\omega$ mit $a, b \in \mathbb{Z}$. Eine $\mathbb{Z}$-Basis von $(x) = xO_K$ ist

$$\begin{aligned} x &= a + b\omega \\ x\omega &= a\omega + b\omega^2 \\ \omega &= \begin{cases} D_K & : D_K \equiv 2{,}3 \pmod 4 \\ \frac{D_K - 1}{4} + \omega & D_K \equiv \pmod 4 \end{cases} \end{aligned}$$

   Also $\mathbb{N}(\,(x)\,) = |\det(\begin{smallmatrix} a & bD_K \\ b & a \end{smallmatrix})| = |a^2 - b^2 D_K|$ $N(x) = a^2 - b^2 D_K$.

   Der andere Fall geht analog. ∎

3.7 Multiplikative Arithmetik in O_K – Primideale

Definition 3.16
$\mathfrak{p} \subset O_K$ heißt **Primideal** $\Leftrightarrow$ ${}^{O_K}/_{\mathfrak{p}}$ ist **integer**, d. h. ohne Nullteiler.

Lemma 3.2
Eine endliche Integritätsbereich ist eine Körper.

Beweis:
Sei R endlich und integer und weiterhin sei $x \in R \setminus \{0\}$. Multiplikation mit x verursacht injektive Abbildung $R \setminus \{0\} \to R \setminus \{0\}$. Diese Abbildung ist also bijektiv, somit ist $1 \in R$ ein Bild. ∎

Fakt 3.33
Die Primideale, außer dem Nullideal ($\neq (0)$) in O_K sind maximal, d. h. zwischen $\mathfrak{p}$ und O_K gibt es keine weiteren Ideale.

Beweis:
Sei $\mathfrak{p} \subset \mathfrak{p}_2 \subset O_K$ und $\mathfrak{p} \neq \mathfrak{p}_2$. Sie $x \in \mathfrak{p}_2 \setminus \mathfrak{p}$, dann existiert $y \in O_K$, so dass $(x+\mathfrak{p})(y+\mathfrak{p}) = 1 + \mathfrak{p}$ in ${}^{O_K}/_{\mathfrak{p}}$. Also $xy - 1 \in \mathfrak{p}$. Nun ist aber $xy \in \mathfrak{p}_2$, also $1 \in \mathfrak{p}_2 \Rightarrow \mathfrak{p}_2 \in O_K$. ∎

Bemerkung 3.14
Wir haben über O_K die Dinge gezeigt:

1. O_K ist Noethersch,

2. O_K ist ganzabgeschlossen und
3. die Primideale $\neq 0$ sind maximal.

Solche Ringe heißen **Dedekind-Ringe**.

Definition 3.17
$\mathfrak{p}_1 \mid \mathfrak{p}_2 := \exists \mathfrak{p}_3 \colon \mathfrak{p}_2 = \mathfrak{p}_1 \cdot \mathfrak{p}_3$.

Dann gilt $\mathfrak{p}_1 \mid \mathfrak{p}_2 \Leftrightarrow \mathfrak{p}_2 \subset \mathfrak{p}_1$.

Satz 3.3 (Hauptsatz der Arithmetik in O_K)
Jedes Ideal in O_K ist Produkt von Primidealen. Diese Darstellung ist bis auf die Reihenfolge eindeutig.

Beweis:
Maximale Ideale sind prim, jedes Ideal $\neq O_K$ liegt in einem maximalen Ideal, dann zwischen ihm und O_K liegen nur endlich viele Ideal.

1. Jedes Ideal $\neq O_K$ ist Produkt ein von Primidealen: Durch Induktion über die Absolutnorm $\mathbb{N}\mathfrak{a}$.

   Sei $\mathfrak{p}$, so dass $\mathfrak{a} \subset \mathfrak{p} \subset O_K$, $\mathfrak{p}$ prim. Dann existiert $\mathfrak{b} \subset O_K$ mit $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$.

   $$\mathbb{N}\mathfrak{a} = \mathbb{N}\mathfrak{b} \cdot \mathbb{N}\mathfrak{p}, \mathbb{N}\mathfrak{p} > 1 \Rightarrow \mathbb{N}\mathfrak{b} < \mathbb{N}\mathfrak{a}$$

   $\Rightarrow \mathbb{N}$ greift.

2. Wir zeigen: $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \vee \mathfrak{p} \mid \mathfrak{b}$. Aus $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ folgt $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{p}$. Sei $\mathfrak{a} \not\subset \mathfrak{p}, \mathfrak{b} \not\subset \mathfrak{p}$ und $x \in \mathfrak{a} \setminus \mathfrak{p}$ und $y \in \mathfrak{b} \setminus \mathfrak{p}$. Dann ist $xy \notin \mathfrak{p}$ wegen ${}^{O_K}/_{\mathfrak{p}}$ integer. Aber $xy \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ ↯
3. Sei $\mathfrak{p}_1 \mid \mathfrak{a}_1 \cdots \mathfrak{a}_n \Rightarrow \mathfrak{p}_1 \mid \mathfrak{a}_1 \Rightarrow \mathfrak{a} \subset \mathfrak{p}_1$, beide maximal somit $\mathfrak{p}_1 = \mathfrak{a}_1$. Es folgt $\mathfrak{p}_2, \ldots, \mathfrak{p}_m = \mathfrak{q}_2 \ldots \mathfrak{q}_n$.

   Aus todo: Link: Fakt im Abschnitt 3.5 letzten $\Rightarrow$ Induktionsvorraussetzung greift. ∎

Beispiel 3.13
$(3) = 3O_K$ ist kein Primideal:

$$O_K/3O_K = \{a + b\sqrt{-5} \colon a, b \in \mathbb{F}_3\}$$
$$(1 + \sqrt{-5})(2 + \sqrt{-5}) = 2 - 5 + 3\sqrt{-5} = -3 + 3\sqrt{-5}$$

$\Rightarrow {}^{O_K}/_{3O_K}$ hat Nullteiler.

Also zerfällt $(3) = 3O_K$ nicht trivial in Primideale.

$\mathbb{N}(\,(3)\,) = 9$, also $(3) = \mathfrak{p}\mathfrak{q}$ und $\mathbb{N}\mathfrak{p} = \mathbb{N}\mathfrak{q} = 3$.

Kanonische Basis von $\mathfrak{p}$: $a + b\sqrt{-5}, c$

$$b, c > 0, bc = 3, -1 \leq a \leq 1, b \mid a, b \mid c, bc \mid N(a + b\sqrt{-5})$$

a	b	c	$N(a+b\sqrt{-5}) = a^2+5b^2$
-1	1	3	6
0	1	3	5
1	1	3	6

Es gibt also genau zwei Ideale mit der Absolutnorm 3:

$$\mathfrak{p}_1 = \mathbb{Z}(-1+\sqrt{-5}) + \mathbb{Z}3$$
$$\mathfrak{p}_1' = \mathbb{Z}(1+\sqrt{-5}) + \mathbb{Z}3 = \mathbb{Z}(-1-\sqrt{-5}) + \mathbb{Z}3$$

Es folgt $(3) = 3O_K = \mathfrak{p}_1 \cdot \mathfrak{p}_1'$. Überdies gilt $\mathfrak{p}_1 \neq \mathfrak{p}_1'$, da verschiedene kanonische Basen.

Beispiel 3.14
(7) ist nicht prim: $(3+\sqrt{-5})(4+\sqrt{-5}) = 12+7\sqrt{-5}-5 = 7(1+\sqrt{-5})$

$\Rightarrow (7) = \mathfrak{p}\cdot\mathfrak{q}$ für zwei Primideale mit Absolutnorm 7.

$bc = 7, b \mid c \Rightarrow b = 1, c = 7, -3 \leq a \leq 3$

a	$b=1, c=7$	$N(a+b\sqrt{-5}) = a^2+5b^2$
-3		$14*$
-2		9
-1		6
0		5
1		6
2		9
3		$14*$

$\mathfrak{p}_2 = \mathbb{Z}(-3+\sqrt{-5}) + \mathbb{Z}7$
$\mathfrak{p}_2' = \mathbb{Z}(3+\sqrt{-5}) + \mathbb{Z}7 = \mathbb{Z}(-3-\sqrt{-5}) + \mathbb{Z}7.$

$(7) = 7O_K = \mathfrak{p}_2 \cdot \mathfrak{p}_2'$

$\mathfrak{p}_2 \neq \mathfrak{p}_2'$, da verschiedene kanonische Basen vorliegen. Somit $(21) = \mathfrak{p}_1 \cdot \mathfrak{p}_1' \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_2'$.

Nun zerlegen wir $\mathfrak{a} = (4+\sqrt{-5})$. $\mathbb{N}\mathfrak{a} = 21$. Klar ist $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$ oder $\mathfrak{p}_1\mathfrak{p}_2'$ oder $\mathfrak{p}_1'\mathfrak{p}_2$ oder $\mathfrak{p}_1'\mathfrak{p}_2'$. Wir schauen in welchen der 4 Ideal $\mathfrak{p}_1, \mathfrak{p}_1', \mathfrak{p}_2, \mathfrak{p}_2'$ die Zahl. $4+\sqrt{-5}$ auftritt:

$$\begin{aligned} 4+\sqrt{-5} &= A(-3+\omega) + 7B \\ &= -3A + 7B + A\omega \\ &\Rightarrow A = 1, 7B - 3 = 4, B = 1 \\ &\Rightarrow 4+\sqrt{-5} \in \mathfrak{p}_2 \end{aligned}$$

$4+\sqrt{-5} = C(3+\sqrt{-5}) + 7D$
$4 = 3C + 7D \Rightarrow 7D = 1$ und $C = 1 \lightning 4+\sqrt{-5} \notin \mathfrak{p}_2'$

$4+\sqrt{-5} = E(-1+\sqrt{-5}) + 3F$
$E = 1, 3F = 5 \lightning \Rightarrow 4+\sqrt{-5} \notin \mathfrak{p}_1$

$4+\sqrt{-5} = G(1+\sqrt{-5}) + 3H$
$G = 1, H = 1 \Rightarrow 4+\sqrt{-5} =\in \mathfrak{p}_1'$

Also $(4+\sqrt{-5}) = \mathfrak{p}_1'\mathfrak{p}_2$ und $(4-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2'$.

3.8 Das Zerlegungsgesetz in quardatischen Zahlenkörpern

Wie zerfallen die Primzahlen aus $\mathbb{Z}$ in O_K? Wir hatten es schon mit elementaren Methoden für $K = \mathbb{Q}(\sqrt{-1})$ gesehen.

Bemerkung 3.15
Sei $K/\mathbb{Q}$ quadratisch, $p \in \mathbb{P} \subset \mathbb{Z}$, $\mathbb{N}(pO_K) = p^2$. Also gibt es nur drei Möglichkeiten:

- $pO_K = \mathfrak{p}^2, \mathbb{N}\mathfrak{p} = p$,
- pO_K ist prim oder
- $pO_K = \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1 \neq \mathfrak{p}_2$.

Da auch $\mathfrak{p}_1'$ das Ideal pO_K teil, gilt $\mathfrak{p}_1' \neq \mathfrak{p}_2$ oder $\mathfrak{p}_1' = \mathfrak{p}_2', \mathfrak{p}_2' = \mathfrak{p}_2$.

Aber $\mathfrak{p}_1 \cdot \mathfrak{p}_1' = pO_K$ (letzte Vorlesung) $\Rightarrow \mathfrak{p}_1' = \mathfrak{p}_2$.

Definition 3.18
Sei $p \in \mathbb{P}$

1. p heißt **verzeweigt** in $K :\Leftrightarrow pO_K = \mathfrak{p}^2$
2. p heißt **zerlegt** in $K :\Leftrightarrow pO_K = \mathfrak{p} \cdot \mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$
3. p heißt **träge** (engl. inert) in $K :\Leftrightarrow pO_K$ ist Primideal

Bemerkung 3.16
Für 1. gilt $\mathbb{N}\mathfrak{p} = p$. Für 2. gilt $\mathbb{N}\mathfrak{p} = p = \mathbb{N}\mathfrak{p}'$ Für $\mathbb{N}pO_K = p^2$

Beispiel 3.15
In $\mathbb{Z}[i]$ ist zwei verzweigt, die $p \equiv 1 \pmod 4$ zerlegt, die $p \equiv 3 \pmod 4$ träge.

Fakt 3.34
$K = \mathbb{Q}(\sqrt{D_K}), D_K \in \mathbb{Z}, \neq 0{,}1$ quadratfrei, Sei $p > 2$ prim.

1. p verzeigt $\Leftrightarrow p \mid D_K \Leftrightarrow (\frac{D_K}{p}) = 0$,

2. p zerlegt $\Leftrightarrow (\frac{D_K}{p}) = 1$
3. p träge $\Leftrightarrow (\frac{D_K}{p}) = -1$

BEWEIS:

1. Sei $pO_K = \mathfrak{p}^2$ also $\mathbb{N}\mathfrak{p} = p^2$.

$$\mathfrak{p} = \mathbb{Z}(a + b\omega) + \mathbb{Z}c, bc = p, b \mid c$$

$\Rightarrow b = 1, c = p$. Weiter ist $\mathfrak{p}' = \mathfrak{p}$ ($\mathfrak{p}^2 = (\mathfrak{p}')^2 \Rightarrow \mathfrak{p} = \mathfrak{p}'$) Für $D_K \equiv 2{,}3 \pmod 4$ ist $\omega = \sqrt{D_K}$, also $\omega' = -\omega$.

$\mathfrak{p} = \mathfrak{p}' = \mathbb{Z}(a - b\omega) + \mathbb{Z}c = \mathbb{Z}(-a + b\omega) + \mathbb{Z}c$. Wegen der Eindeutigkeit der kannonischen Basis folgt $a = 0$. Für $D_K \equiv 1 \pmod 4$ ist $\omega' = \frac{1-\sqrt{D_K}}{2} = 1 - \omega$.

Also ist

$$\begin{aligned}\mathfrak{p} = \mathfrak{p}' &= \mathbb{Z}(a + b(1 - \omega)) + \mathbb{Z}c \\ &= \mathbb{Z}(a + b - b\omega) + \mathbb{Z}c \\ &= \mathbb{Z}(-a - b + b\omega) + \mathbb{Z}c \\ \mathfrak{p} &= \mathbb{Z}(a + b\omega) + \mathbb{Z}c\end{aligned}$$

$\Rightarrow -a - b \equiv a \pmod c \Rightarrow 2a \equiv -1 \pmod p \Rightarrow a = \frac{p-1}{2}$. Wir haben noch $bc \mid N(a + b\omega) \Rightarrow p \mid N(a + \omega)$.

Ist $D_K \equiv 2{,}3 \pmod 4$, so ist $a = 0$, also $N(a + \omega) = -D_K \Rightarrow p \mid D_K$.

Ist $D_K \equiv 1 \pmod 4$, so ist

$$\begin{aligned}N(\frac{p-1}{2} + \omega) &= (\frac{p-1}{2} + \omega)(\frac{p-1}{2} + \omega') \\ &= (\frac{p-1}{2})^2 + \frac{p-1}{2}(\omega + \omega') + \omega\omega' \\ &\frac{1}{4}(p^2 - 2p + 1 + 2p - 2 + 1 - D_K) \\ &= \frac{1}{4}(p^2 - D_K)\end{aligned}$$

$p \mid \frac{1}{4}(p^2 - D_K) \Rightarrow p \mid D_K$.

2. Sei $p \mid D_K$. Definier $\mathfrak{p} := \mathbb{Z}\omega + \mathbb{Z}p$ für $D_K \equiv 2{,}3 \pmod 4$ und $\mathfrak{p} := \mathbb{Z}(\frac{p-1}{2} + \omega) + \mathbb{Z}p$ für $D_K \equiv 1 \pmod 4$.

   Dann ist $\mathbb{N}\mathfrak{p} = p$ ($= bc$ für die kannaonischen Basen). Also ist $\mathfrak{p}$ eine Primideal.

   Weiter ist $\mathfrak{p}' = \mathfrak{p}$: Klar im ersten Fall.

$$\begin{aligned}\frac{p-1}{2} + \omega' = \frac{p-1}{2} + \frac{1-\sqrt{D_K}}{2} &= \frac{p-1}{2} + 1 - \omega \\ &= -(-\frac{p-1}{2} + \omega) = -(-p + \frac{p-1}{2} + w)\end{aligned}$$

$\Rightarrow \mathfrak{p}' = \mathfrak{p}$.

$\mathfrak{p}\mathfrak{p}' = pO_K \Rightarrow pO_K = \mathfrak{p}^2$.

3. Sei p träge, also $pO_K = \mathfrak{p}$ – Primideal. $\mathfrak{p}$ hat kanonische Basis: $a = 0, b = c = p$:

$$\mathfrak{p} = \mathbb{Z}p\omega + \mathbb{Z}p$$

Für $O_K \equiv 2{,}3 \pmod 4$ ist $\omega^2 = D_K$.

O_K/pO_K (ein Körper aus p^2 Elementen) ist quadratische Erweiterungskörper von $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

$O_K/pO_K = \mathbb{F}_p \cdot \overline{\omega} + \mathbb{F}_p, \overline{\omega} = Bildvon\omega$, d. h. $\overline{1}$ und $\overline{\omega}$ bilden $\mathbb{F}_p$-Basis von O_K/pO_K. Demnach ist $\overline{\omega}$ kein Element aus $\mathbb{F}_p$. Also ist $\overline{D_K} = \overline{\omega}^2$. $\Rightarrow (\frac{D_K}{p}) = -1$. $D_K \equiv 1 \pmod 4$ analog.

4. Sei $(\frac{D_K}{p}) = -1$ und $\mathfrak{p} := pO_K$. Jedenfalls ist $\mathbb{N}\mathfrak{p} = p^2$. Eir zeigen: O_K/pO_K hat keine Nullteiler (das impliziert $\mathfrak{p}$ prim). Sei $(r + s\omega)(t + u\omega) \in pO_K$, zu zeigen ist, dass wenigstens ein Faktor auch in pO_K liegt.

Indirekt: beide nicht in pO_K.

Fall 1: $D_K \equiv 2{,}3 \pmod 4$.

$$\begin{aligned} & rt + (st + ru)\omega + D_K su \in pO_K \\ \Rightarrow\ & rt + suD_K \equiv 0 \pmod p \qquad \mid \cdot s \\ & st + ru \equiv 0 \pmod p \qquad \mid \cdot r \\ \Rightarrow\ & (r^2 - s^2 D_K)_u \equiv 0 \pmod p \end{aligned}$$

Sei $p \mid u \Rightarrow p \mid st$ und $p \mid rt$. p teilt höchstene eine der Zahlen r und $s \Rightarrow p \mid t$ ↯ weil p sonst bereits in O_K wäre. Mithin $p \mid (r^2 - D_K s^2)$.

Angenommen $p \mid s$, dann $p \mid ru$ und $p \mid rt \Rightarrow p \mid r$ ↯ wie eben.

Es folgt nun daraus, dass $D_K \equiv (\frac{r}{s})^2 \pmod p \Rightarrow (\frac{D_K}{p}) = 1$. ↯, da wir vorrausgesetzt hatten, dass $? = -1$.

5. $D_K \equiv 1 \pmod 4$ analog. ∎

Beispiel 3.16
$K = \mathbb{Q}(\sqrt{-2006})$, $D_K = -2006 = -2 \cdot 1003 = -2 \cdot 17 \cdot 59$.

Ist $p = 23$ träge oder reduziert?

$$\left(\frac{-2006}{23}\right) = \left(\frac{2300 - 2006}{23}\right) = \left(\frac{294}{23}\right) = \left(\frac{64}{23}\right) = \left(\frac{-5}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{5}{23}\right) = -\left(\frac{5}{23}\right) = -\left(\frac{23}{5}\right) = -\left(\frac{3}{5}\right) = 1$$

$\Rightarrow 23$ ist zerlegt.

Fakt 3.35
Sei d_K die Diskiminante von $\mathbb{Q}(\sqrt{D_k})$.

1. 2 ist verzweigt in $K \Leftrightarrow 2 \mid d_K$
2. 2 ist träge in $K \Leftrightarrow d_K \equiv 5 \pmod 8$
3. 2 ist zerlegt in $K \Leftrightarrow d_K \equiv 1 \pmod 8$

Beweis:
Sei 2 träge in K, d. h. $2O_K$ ist Primideal. Dann ist d_K ungerade wegen (i), also $D_K \equiv 1 \pmod 4$, sowie $d_K = D_K$.

$$\omega^2 = (\frac{1+\sqrt{D_K}}{2})^2 = \frac{D_K+1+2\sqrt{D_K}}{4} = \frac{D_K-1}{4} + \omega \tag{3.2}$$

$\Rightarrow {}^{O_K}/_{2O_K}$ ist ein Körper aus 4 Elementen: $\overline{0}, \overline{1}, \overline{\omega}, \overline{1}+\overline{\omega}$.

Gleichung 3.2 liefert $\overline{\omega}^2 = \overline{(\frac{D_K-1}{4})} + \overline{\omega}$.

Angenommen $\frac{D_K-1}{4}$ ist gerade, dann folgt $\overline{\omega}^2 = \overline{\omega} \Rightarrow \overline{\omega}(\overline{\omega}-1) = 0$ ↯

Somit ist $\frac{D_K-1}{4}$ ungerade $\Rightarrow D_K \equiv 5 \pmod 8$.

Das war nur eine von vier Implikationen. Die anderen drei selber machen! ∎

Fakt 3.36
Sei $m \geq 2$ und $\varphi\colon \mathbb{Z} \to \mathbb{C}^* \cup \{0\}$, so dass

1. Für alle $(a,m) > 1$ ist $\varphi(a) = 0$.
2. Für alle $a \in \mathbb{Z}$ ist $\varphi(a+m) = \varphi(a)$
3. $\varphi(ab) = \varphi(a)\varphi(b)\ \forall a,b \in \mathbb{Z}$
4. $\varphi(1) = 1$

Dann induziert φ einen Dirichlet-Charakter modulo m. Umgekehrt induziert jeder Dirichlet-Charakter modulo m via Fortsetzung durch 0 einen solche Funktion auf $\mathbb{Z}$.

Beweis:
$\chi(\overline{a}) := \varphi(a)$ für $\overline{a} \in ({}^{\mathbb{Z}}/_{m\mathbb{Z}})^*$ ∎

Definition 3.19
$\chi_K\colon \mathbb{N}^* \to \{-1,0,1\}$ sei definiert durch

$$\chi_K(p) = \begin{cases} (\frac{D_K}{p}) & p > 2 \\ +1 & p = 2, d_K = D_K \equiv 1 \pmod 8 \\ -1 & p = 2, d_K = D_K \equiv 5 \pmod 8 \\ 0 & p = 2, 2 \mid d_K \end{cases}$$

und dann multiplikativ fortsetzen.

Fakt 3.37
χ_K ist eine Dirichlet-Charakter modulo $|d_K|$. Er heißt **Charakter von K**.

Beweis:

D_K	-1	2	-2
d_K	-4	8	-8

Es gibt genau einen nicht trivialen Dirichlet-Charakter modulo 4

n	1	3
$\chi(n)$	1	-1

$\chi_{\mathbb{Q}(i)}(p) = (\frac{-4}{p}) = (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ für $p > 2$. $\chi_{\mathbb{Q}(i)}$ und χ stimmen auf den primzahlen $p > 2$ überein und sind beide Null auf den geraden natürlichen Zahlen $\Rightarrow$ sind gleich auf $\mathbb{N}^*$.

Setze $\chi_{\mathbb{Q}(i)}$ durch χ auf $\mathbb{Z}$ fort unf nenne es χ_{-4}. Es gibt nicht triviale Charaktere modulo 8.

	1	3	5	7	
φ_1	1	-1	1	-1	$\leftarrow$ kommt von obigem χ (mod 4)
φ_2	1	-1	-1	1	
φ_3	1	1	-1	-1	

$$\chi_{\mathbb{Q}(\sqrt{2})}(p) = (\frac{8}{p}) = (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \varphi_2(p) \quad (p > 2)$$
$$\chi_{\mathbb{Q}(\sqrt{-2})}(p) = (\frac{-8}{p}) = (\frac{-2}{p}) = (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}} = \varphi_3(p)$$

$\Rightarrow \chi_8 = \chi_{\mathbb{Q}(\sqrt{2})} = \varphi_2$ auf $\mathbb{Z}$. $\chi_{-8} = \chi_{\mathbb{Q}(\sqrt{-2})} = \varphi_3$ auf $\mathbb{Z}$.

Sei nun $K = \mathbb{Q}(\sqrt{D_K})$.

$$D_K = (-1)^{\varepsilon} 2^{\eta} p_1 \cdots p_r \qquad \varepsilon, \eta \in \{0,1\}, p_j > 2$$

Sei weiter $p \neq 2, p \neq p_j \forall j$.

$$\begin{aligned}\chi_K(p) = (\frac{D_K}{p}) &= (\frac{-1}{p})^{\varepsilon}(\frac{2}{p})^{\eta}(\frac{p_1}{p}) \cdots (\frac{p_r}{p}) \\ &= \chi_{-4}(p)^{\varepsilon}\chi_8(p)^{\eta}(-1)^{\frac{p-1}{2}\cdot\sum_i \frac{p_i-1}{2}}(\frac{p}{p_1}) \cdots (\frac{p}{p_r}) \\ &= \chi_{-4}(p)^{\varepsilon+\sum_i \frac{p_i-1}{2}}\chi_8(p)^{\eta} \cdot (\frac{p}{p_1}) \cdots (\frac{p}{p_r})\end{aligned}$$

Rechts steht ein Dirichlet-Charakter modulo $8 \cdot p_1 \cdots p_r$

Fall 1: $D_K \equiv 1 \pmod 4 \Rightarrow \eta = 0, \varepsilon + \sum \frac{p_i - 1}{2}$ ist gerade. $\Rightarrow$

$$\chi_K(p) = (\frac{p}{p_1}) \cdots (\frac{p}{p_r})$$

Charakter modulo $|d_k|$.

Fall 2: $D_K \equiv 3 \pmod 4 \Rightarrow d_K = 4D_K, \eta = 0$. Dann ist $\varepsilon + \sum \frac{p_i - 1}{2}$ ungerade. $\Rightarrow$ $\chi_K = \chi_{-4}(\frac{\cdot}{p_1}) \cdots (\frac{\cdot}{p_r})$ Charakter modulo $\underbrace{4p_1 \cdots p_r}_{=|d_K|}$

Fall 3: $D_K \equiv 2 \pmod 4$ analog ∎

Satz 3.4
Sei K quadratischer Zahlenkörper mit Diskiminante d_K, χ_K der zugehörige Charakter. Dann ist χ_K Dirichlet-Charakter modulo $|d_K|$ und

- p verzeigt $\Leftrightarrow \chi_K(p) = 0$,
- p zerlegt $\Leftrightarrow \chi_K(p) = 1$,
- p träge $\Leftrightarrow \chi_K(p) = -1$.

3.9 Die Idealklassengruppe

Definition 3.20
Zwei Ideale $\mathfrak{p}_1, \mathfrak{p}_2$ $(\neq 0)$ in O_K heißen **äquivalent** $:\Leftrightarrow \exists \alpha, \beta \in O_K \setminus \{0\}, (\alpha)\mathfrak{p}_1 = (\beta)\mathfrak{p}_2$

Fakt 3.38
Die Klassen bezüglich dieser Äquivalenzrelation bilden eine abelsche Gruppe.

Beweis:
Sei $\overline{\mathfrak{p}}$ die Klasse von $\mathfrak{p}$. $\overline{\mathfrak{p}_1} \cdot \overline{\mathfrak{p}_2} := \overline{\mathfrak{p}_1 \cdot \mathfrak{p}_2}$. Zeigen wir die Korrektheit der Definition: $\mathfrak{p}_1 \sim \mathfrak{p}_3, \mathfrak{p}_2 \sim \mathfrak{p}_4 \Rightarrow (\alpha)\mathfrak{p}_1 = (\alpha_1)\mathfrak{p}_3, (\beta)\mathfrak{p}_2 = (\beta_1)\mathfrak{p}_4 \Rightarrow (\alpha\beta)\mathfrak{p}_1\mathfrak{p}_2 = (\alpha_1\beta_1)\mathfrak{p}_3\mathfrak{p}_4$.

Die Hauptideale bilden eine Klasse. Dies ist neutrales Element der Multiplikation der Klassen $\mathfrak{p} \cdot \mathfrak{p}' = (m), m = \mathbb{N}\mathfrak{p}$ (3.5). ∎

Definition 3.21
Diese Gruppe heißt **Idealklassengruppe** von K. Bezeichnung: Cl_K.

Beispiel 3.17
1. $K = \mathbb{Q}(\sqrt{-1}), Cl_K = 1$ (O_K ist Hauptidealring)
2. $K = \mathbb{Q}(\sqrt{-5}), Cl_K \neq 1$: es gibt auch Nichthauptideale.

Wir zeigen: Cl_K ist endlich.

Bemerkung 3.17
Hat Γ die Basis $\omega_1, \ldots, \omega_n$, so ist $F = \{\sum \alpha_i \omega_i \colon 0 \leq \alpha_i < 1\}$ sogenannte Fundamentalbereich für Γ: $\mathbb{R}^n = \coprod_{\gamma \in \Gamma} F + \gamma$.

Das Volumen ist definiert als

$$vol(\frac{\mathbb{R}^n}{\gamma}) := vol(F)$$

Lemma 3.3
Ω wie oben

$$\bigcap_{\varepsilon > 0} (1+\varepsilon)\Omega = \Omega$$

Beweis:
Da Ω konvex und zentralsymetrich, $\Omega \subset (1+\varepsilon)\Omega$. Sei $x \notin \Omega \Rightarrow dist(x, \Omega) = \eta > 0$. Sei $c = \max\{|y| \colon y \in \Omega\}, \varepsilon < \frac{\eta}{c}$.

Wäre $x \in (1+\varepsilon)\Omega$, so wäre $x = (1+\varepsilon)y, y \in \Omega$ also $|x-y| = \varepsilon|y| \leq \varepsilon c < \eta$ Widerspruch.∎

Satz 3.5 (Minkowskis Gitterpunktsatz)
Sei $\Gamma \subset \mathbb{R}^n$ Gitter (freie abelsche Gruppe, diskret, vom Rang n). Sei $\Omega \subset \mathbb{R}^n$ kompakt, konvex und zentralsymetrich ($x \in \Omega \Rightarrow -x \in \Omega$).

Ist dann das Volumen $vol(\Omega) \geq 2^n vol(\frac{\mathbb{R}^n}{\gamma})$, so enthält Ω nicht triviale Gitterpunkte.

Beweis:
Sei zuerst $vol(\Omega) > 2^n vol(F)$

$$\mathbb{R}^n = \coprod_{\gamma \in \Gamma} F + \gamma \Rightarrow$$
$$\frac{1}{2}\Omega = \coprod_{\gamma \in \Gamma} \frac{1}{2}\Omega \cap (F + \gamma)$$

$$\begin{aligned} vol(F) < 2^{-n} vol(\Omega) &= vol(\frac{1}{2}\Omega) \\ &= \sum_{\gamma \in \Gamma} vol(\frac{1}{2}\Omega \cap (F+\gamma)) \\ &= \sum_{\gamma \in \Gamma} vol((\frac{1}{2}\Omega - \gamma) \cap F) \end{aligned}$$

Es folgt: Die Mengen $\frac{1}{2}\Omega - \gamma, \gamma \in F$ sind nicht alle disjunkt: $\exists x_1, x_2 \in \Omega \colon \gamma_1, \gamma_2 \in \Gamma \colon \gamma_1, \gamma_2$

$$\frac{1}{2}x_1 - \gamma_1 = \frac{1}{2}x_2 - \gamma_2 \Rightarrow \frac{1}{2}(x_1 - x_2) \in \Gamma \setminus \{0\}$$

Aus $x_2 \in \Omega$ folgt $-x_2\Omega$. Aus Konvexität folgt $\frac{1}{2}(x_1 - x_2) \in \Omega$.

Sei $vol(\Omega) = 2^n vol(F)$. In jedem $(1+\varepsilon)\Omega$ liegt ein nicht trivialer Gitterpunkt. Wähle $\varepsilon_n \downarrow 0$, $\gamma_n \Gamma \setminus \{0\}$, die Folge (γ_n) beschränkt, enthält konvergente Teilfolge, Γ diskret $\Rightarrow$ Teilfolge ist konstant. Lemma 3.3 $\Rightarrow$ liegt in Ω. ∎

Folgerung 3.15
Sei K imaginar quadrat mit Diskriminate d_K. Dann existiert in jeder Idealklasse ein Ideal $\mathfrak{p}$ mit

$$\mathbb{N}\mathfrak{p} \leq \frac{2}{\pi}\sqrt{|d_K|}$$

Sei $\Omega_a \subset \mathbb{C}$ definiert durch $|z| \leq a$, $a > 0$. $vol(\Omega_a) = \pi a^2$. Ω_a ist kompakt, konvex und zentralsymetrich. Sei $\mathfrak{p} \subset O_K$ Ideal $\neq (0)$. Ist $\mathfrak{p} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, so ist $F = \{\alpha_1\omega_1 + \alpha_2\omega_2 \colon 0 \leq \alpha_1, \alpha_2 < 1\}$ Fundamentalbereich, kanonische Basis von $\mathfrak{p}$.

Sei $\mathfrak{p} = \mathbb{Z}(a + b\omega) + \mathbb{Z}c$, dann ist $vol(F) = c \mid m(a + b\omega) = bc \mid m(\omega)$.

$D_K \equiv 2{,}3(4) \Rightarrow \omega = \sqrt{D_K}, d_K = 4D_K \Rightarrow \Im\omega = \sqrt{|D_K|}$, $\Im(\omega) = \frac{1}{2}\sqrt{|D_K|}$.

$\mathbb{N}\mathfrak{p} = bc \Rightarrow vol(F) = \mathbb{N}\mathfrak{p} \cdot \frac{1}{2}\sqrt{|d_K|}$

Wir wählen a so, dass $vol(\Omega_a) = 4vol(F) \Leftrightarrow \pi a^2 = 2\mathbb{N}\mathfrak{p}\sqrt{|d_K|}$, $a^2 = \frac{2}{\pi}\sqrt{|d_K|}\mathbb{N}\mathfrak{p}$. Dann existiert $x \in \mathfrak{p}, x \neq 0$, so dass $x \in \Omega_a$, also $|x^2| \leq a^2$.

Es gilt $xO_K = \mathfrak{p}_1\mathfrak{p}_2$ für ein Ideal $b \subset O_K$

$$\mathbb{N}(xO_K) = |N(x)| = |x^2| = \mathbb{N}\mathfrak{p}_1 \cdot \mathbb{N}\mathfrak{p}_2 \leq \frac{2}{\pi}\sqrt{|d_K|}$$

$\Rightarrow \mathbb{N}\mathfrak{p}_2 \leq \frac{2}{\pi}\sqrt{|d_K|}$. Sei $x \in Cl_K$, wähle $\mathfrak{p} \in x^{-1}$.

Folgerung 3.16
Sei K reellquadratisch, dann existiert in jeder Idealklasse ein Ideal $\mathfrak{p}$ mit

$$\mathbb{N}\mathfrak{p} \leq \frac{1}{2}\sqrt{|d_K|}$$

Beweis:
$K \to \mathbb{R}^2 \colon x \mapsto (x, x')$ $\Omega_a := \{(x, y) \in \mathbb{R}^2 \colon |x| + |y| \leq a\}$. Ω_a ist todo: Bildchen von Ω_a offensichtlich kompakt, zentralsymetrich und konvex. $vol(\Omega_a) = 2a^2$.

$O_K \to \mathbb{Z}(1{,}1) + \mathbb{Z}(\omega, \omega')$. Sei $\mathfrak{p} \subset O_K$ Ideal, $vol(F_\mathfrak{p}) = bc|\omega' - \omega| = \mathbb{N}\mathfrak{p}\sqrt{|d_K|}$. Übungsaufgabe.

Wähle a, so dass $vol(\Omega_a) = 4vol(F_\mathfrak{p})$, $2a^2 = 4\mathbb{N}\mathfrak{p}\sqrt{|d_K|}$.

Dann existiert $x \in \mathfrak{p} \setminus (0)$ mit $x \in \Omega_a$, also $|x| + |x'| \leq a$.

$$|N(x))|^{\frac{1}{2}} = \sqrt{|xx'|} \leq \frac{1}{2}(|x| + |x'|) \leq \frac{1}{2}a$$
$$(x) = \mathfrak{p}_1\mathfrak{p}_2, \mathbb{N}(xO_K) \leq \frac{1}{4}a^2$$
$$\mathbb{N}\mathfrak{p}_1 \cdot \mathbb{N}\mathfrak{p}_2 = \mathbb{N}(xO_K) \leq \frac{1}{4}a^2 = \frac{1}{2}\sqrt{|d_K|} \cdot \mathbb{N}\mathfrak{p}_1$$
$$\mathbb{N}\mathfrak{p}_2 \leq \frac{1}{2}\sqrt{|d_K|}$$ ∎

Satz 3.6
Die Idealklassengruppe ist endlich. Ihre Ordnung heißt **Klassenzahl** von K h_K

Beweis:
Es gibt nur endlich viele Ideale mit fester Norm. $\mathbb{N}\mathfrak{p} = m \in \mathbb{N}^*, \mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathbb{N}\mathfrak{p}_i = p_i$ oder p_i^2. $\mathbb{N}\mathfrak{p}_i$ teilt m. Es gibt höchstens zwei $\mathfrak{p}$ mit $\mathbb{N}\mathfrak{p} = p$. ∎

Beispiel 3.18
1. Imagquadratischer Fall

d_K	-3	-4	-7	-8	-11	-15	-19	-20	-23	-24
h	1	1	1	1	1	2	1	2	3	2

In jeder Idealklasse liegen Ideale mit Norm $\mathbb{N} \leq \frac{2}{\pi}\sqrt{|d_K|}$. $\frac{2}{\pi}\sqrt{|d_K|} < 2 \Leftrightarrow \sqrt{|d_K|} \leq \pi$ $\Leftrightarrow |d_K| \leq \pi^2 \Leftrightarrow d_K = -3, -4, -7, -8$.

$\frac{2}{\pi}\sqrt{|d_K|} < 3 \Leftrightarrow |d_K| \leq 22$. 2 ist träge in $\mathbb{Q}(\sqrt{-11})$: $-11 \equiv 4 \pmod 8$, also kein Ideal mit $\mathbb{N} = 2 \Rightarrow h = 1$.

Für $\mathbb{Q}(\sqrt{-15})$ ist 2 zerlegt: $2O_K = \mathfrak{p} \cdot \mathfrak{p}'$. Frage: Ist $\mathfrak{p}$ Hauptideal? Sei $\mathfrak{p} = (a + b\omega), \mathbb{N}\mathfrak{p} = 2$

$$\mathbb{N}(a + b\frac{1 + \sqrt{-15}}{2}) = (a + \frac{b}{2})^2 + \frac{1}{4}15b^2 = 2$$

$\Rightarrow b = 0 \Rightarrow a^2 = 2$ ↯. Also ist $\mathfrak{p}$ kein Hauptideal.

$\mathfrak{p} \cdot \mathfrak{p}' = 2O_K \Rightarrow Cl_K$ ist zyklisch der Ordnung 2.

$-\mathbb{Q}(\sqrt{-19}) \Rightarrow 2$ ist träge $\Rightarrow$ keine Ideale der Norm 2 $\Rightarrow h_K = 1$

Bemerkung 3.18
Es gibt nur 9 imaginärquadratische Zahlkörper mit $h = 1$: $d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$.

Beispiel 3.19
$K = \mathbb{Q}(\sqrt{-2006})$, $d_K = -42006$, jede Idealklasse enthält Ideale mit Absolutnorm $\leq \frac{2}{\pi}\sqrt{42006} < 58$. $2006 = 2 \cdot 17 \cdot 59$

1. Schritt Verzweigt sind 2 und 17, $\Rightarrow 2O_K = \mathfrak{p}_2^2$ und $17O_K = \mathfrak{p}_{17}^2$.

$$\left(\frac{-2006}{3}\right) = \left(\frac{2007-2006}{3}\right) = 1 \Rightarrow 3 \text{ zerlegt}$$

$$\dots$$

$$\left(\frac{-2006}{53}\right) = \left(\frac{8}{53}\right) = \left(\frac{2}{53}\right) = -1 \Rightarrow 53 \text{ träge}$$

zerlegt sind die Primzahlen: 3, 5, 13, 23, 31 und 43. Restträge $\Rightarrow Cl_K$ erzeugt von $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_{13}, \mathfrak{p}_{17}, \mathfrak{p}_{23}, \mathfrak{p}_{31}, \mathfrak{p}_{43}$

2. Schritt Berechnung einiger Normen.

a	$N(a+\sqrt{-2006}) = a^2 + 2006$	Primzahlzerlegung
3	2015	$5 \cdot 13 \cdot 31$
8	2070	$2 \cdot 3^2 \cdot 5 \cdot 23$
10	2106	$2 \cdot 3^4 \cdot 13$
17	2295	$3^3 \cdot 5 \cdot 17$
23	2535	$2 \cdot 5 \cdot 13^2$
31	2967	$13 \cdot 23 \cdot 43$
37	3375	$3^3 \cdot 5^3$

Es folgt: $\mathfrak{p}_{31}, \mathfrak{p}_{23}, \mathfrak{p}_{13}, \mathfrak{p}_{17}, \mathfrak{p}_5, \mathfrak{p}_{43}$ liegen schon in der von $\mathfrak{p}_2$ erzeugten Gruppe. $\Rightarrow \mathfrak{p}_2, \mathfrak{p}_3$ erzeugen $Cl_K \Rightarrow Cl_K$ ist zyklisch oder vom $Typ(2, n)$.

Wir untersuchen, welche Potenz von $\mathfrak{p}_5$ Hauptideal wird.

$$a^2 + 2006 \cdot b^2 = 5^n$$

Für $n = 1{,}3$ keine Lösungen in $\mathbb{Z}$. Für $n = 2{,}4$ nur die trivialen Lösungen $\Rightarrow$ ensprechen $\mathfrak{p}_5\mathfrak{p}_5' = 5O_K$ und $(\mathfrak{p}_5, \mathfrak{p}_5')^2 = 25O_K$. $a^2 + 2006b^2 = 5^5 = 3125 \Rightarrow b^2 = 1$ und $a^2 = 1119$ ist keine Quadratzahl. 5^6 und 5^7 sind es auch nicht.

$5^8 = 319^2 + 2006 \cdot 12^2 = 390\,625 \Rightarrow \mathfrak{p}_5^8 = (319 + 12\sqrt{-2006})$.

$\mathfrak{p}_3^3 \sim \mathfrak{p}_5^{\pm 3}$[1] $\Rightarrow \mathfrak{p}_3^3$ hat auch Ordnung 8 in Cl_K. $\Rightarrow \mathfrak{p}_3$ hat die Ordnung 8 oder 24.

$\mathfrak{p}_3^8 \sim 1 \Rightarrow a^2 + 2006b^2 = 3^8 = 6561$ hat keine Lösung in $\mathbb{Z}$. $\Rightarrow \mathfrak{p}_3$ hat die Ordnung 24.

Ist $\mathfrak{p}_2$ modulo Hauptideal in der von $\mathfrak{p}_3$ erzeugten Gruppe im Cl_K? Dann müßte $\mathfrak{p}_2 \sim \mathfrak{p}_3^{12}$ in Cl_K sein. $\Rightarrow$ Es existiert eine ganze Zahl mit Norm $2 \cdot 3^{12}$:

$$a^2 + 2006b^2 = 2 \cdot 3^{12} = 1\,062\,882$$

Hat keine Lösungen in $\mathbb{Z}$.

$Cl_K \cong C_2 \times C_{24}$, $C_2 = \langle \mathfrak{p}_2 \rangle \langle \mathfrak{p}_3 \rangle = C_{24}$

[1] $\mathfrak{p}_5^{\pm 3}$ heißt $\mathfrak{p}_5^3$ oder $\mathfrak{p}_5^5$, da wir im Ring 8 sind; $5 = -3$

Aus der Zeile mit der 10 in der obigen Tabelle $\Rightarrow \mathfrak{p}_2\mathfrak{p}_3^4\mathfrak{p}_{13} \sim 1 \Rightarrow \mathfrak{p}_{13}^6 \sim 1 \Rightarrow 13^6 = a^2 + 2006b^2$

$$N(1135 + 42\sqrt{-2006}) = 1135^2 + 2006 \cdot 42^2 = 13^6 = 4\,826\,809$$

4 Die Zetafunktion eines quadratischen Zahlkörpers

4.1 Die Zetafunktion eines quadratischen Zahlkörpers

Definition 4.1
Sei $K/\mathbb{Q}$ quadratisch, seine Zetafunktion ist definiert als

$$\zeta_K(s) := \sum_{(0)\neq\mathfrak{p}\subset O_K} \frac{1}{(\mathbb{N}\mathfrak{p})^s}, \quad s \in \mathbb{C}$$

Fakt 4.1
Sei χ_K der Charakter zu K, dann gilt

$$\zeta_K(s) = \zeta(s)L(s,\chi_K)$$

Es folgt: $\zeta_K(s)$ kovergiert absolut für $Res(s) > 1$.

Beweis:
Für $a > 1$ sit $\zeta(s)L(s,\chi_K) = \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \frac{\chi_K(n)}{n^s} = \sum_{m,n=1}^{\infty} \frac{\chi_K(n)}{(mn)^s} = \sum_{d=1}^{\infty} \frac{1}{d^s} \Big(\sum_{r|d} \chi_K(r) \Big) = \sum \frac{a_n}{n^s}$ mit $a_n = \sum_{d|n} \chi_K(d)$.

$[\sum a_m x^m \sum b_n x^n = \sum_{m,n} a_m b_n x^{m+n} = \sum_N (\sum_{nm=N} a_m b_n)$
$\sum_m \frac{a_m}{m^s} \sum_n \frac{b_n}{n^s} = \sum_{m,n} \frac{a_m b_n}{(mn)^s} = \sum_N \frac{1}{N^s} (\sum_{nm=N} a_m b_n)]$

Wir stellen fest: a_n ist multiplikatis: Für $\mathrm{ggT}(m,n) = 1$ ist $a_{m,n} = a_m \cdot a_n$

$$a_{mn} = \sum_{d|mn} \chi_K(d) = \sum_{d_1|m, d_2|n} \chi_K(d_1 d_2) = \sum_{d_1|m} \chi_K(d_1) \cdot \sum_{d_2|n} \chi_K(d_2) = a_m \cdot a_n$$

Andererseits

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}, b_n = \mathrm{card}\{\mathfrak{p} \subset O_K \colon \mathbb{N}\mathfrak{p} = n\}$$

b_n ist multiplikativ: Seien $\mathrm{ggT}(m,n)=1$

$$n=\prod p^{ap}, \mathfrak{a}=\prod \mathfrak{p}^{b_\mathfrak{p}}=\prod_{p \text{ verzeigt}} \mathfrak{p}^{b_p} \prod_{p \text{ träge}} \mathfrak{p}^{b_p} \prod_{p \text{ zerlegt}} \mathfrak{p}^{b_p}\mathfrak{p}'^{b'_p}$$

$$\mathbb{N}\mathfrak{a}=\prod_{p \text{ verzeigt}} p^{b_p} \prod_{p \text{ träge}} p^{2b_p} \prod_{p \text{ zerlegt}} p^{b_p+b'_p}$$

Also $\mathbb{N}\mathfrak{a}=n \Leftrightarrow a_p=b_p$ p verzweigt, $a_p=2b_p$ p träge, $a_p=b_p+b'_p$ p zerlegt.

Somit ist

$$b_n=\begin{cases}0 & a_p\text{ungerade für ein träge } p.\\ \prod_{p \text{ zerlegt}, p|n}(a_p+1) & \text{sonst}\end{cases}$$

Hieraus folgt die Multiplikation sofort.

Wir zeigen $a_{p^n=b_{p^n}} \forall p,n\geq 1$

$$a_{p^n}=\sum_{r=0}^{n}\chi_K(p^r)=1 \quad \text{für } p \text{ verzweigt}$$
$$b_{p^n}=1 \quad \text{für } p \text{ verzweigt}$$

Sei p träge

$$a_{p^n}=\sum_{r=0}^{n}\chi_K(p)^r=\sum_{r=0}^{n}(-1)^r=\begin{cases}0 & n \text{ ungerade}\\ 1 & n \text{ gerade}\end{cases} \quad b_{p^n}=\mathrm{card}\{\mathfrak{p}\subset O_K : \mathbb{N}\mathfrak{p}=p^n\}$$

$\Rightarrow \mathfrak{p}$ Potenz den Primideal $\mathfrak{p}\subset pO_K$, $\mathfrak{p}=p^rO_K, \mathbb{N}\mathfrak{p}=p^{2r}$

Also

$$b_{p^n}=\begin{cases}0 & n \text{ gerade}\\ 1 & n \text{ ungerade}\end{cases}$$

Sie p zerlegt:

$$a_{p^n}=\sum_{r=0}^{n}\chi_K(p)^r=n+1$$
$$b_{p^n}=\mathrm{card}\{\mathfrak{p}^b(\mathfrak{p}')^{b'} : b+b'=n\}=n+1$$

■

Folgerung 4.1
Aus dem vorherigen Beweis folgt

$$\zeta_K(s)=\prod_{\mathfrak{p}}(1-\frac{1}{(\mathbb{N}\mathfrak{p})^s})^{-1} \qquad s>1$$

Das folgt aus der Multiplikativität von b_n.

Folgerung 4.2

$$\lim_{s\to 1+0}(s-1)\zeta_K(s) = L(1,\chi_K)$$

BEWEIS:
$(s-1)\zeta_K(s) = \underbrace{(s-1)\zeta_K(s)}_{\xrightarrow{s\to 1+0}1} \quad \underbrace{L(s,\chi_K)}_{L(1,\chi)\text{ wohldefiniert}}$ ∎

Bemerkung 4.1
$g, f\colon (0,\infty)\to\mathbb{R}$ $f = O(g) :\Leftrightarrow \frac{g(\lambda)}{f(\lambda)}$ beschränkt für $\lambda\to\infty$.

$$\sin(\lambda) = O(1)$$
$$\frac{\sin(\lambda)}{\lambda} = O(\frac{1}{\lambda})$$
$$\log(n!) = n\log n - n + \frac{1}{2}\log 2\pi n + O(\frac{1}{n})$$
$$\zeta(s) = 1 + O(\frac{1}{2^s}) \quad s\to\infty$$
$$e^{-\lambda^2} = O(\frac{1}{\lambda^N}) \quad \forall N$$

Fakt 4.2 (Aus der Theorie der Gitterpunkte)
Sei $\Omega\subset\mathbb{R}^2$ beschränkt, der Rand $\partial\Omega = \overline{\Omega}\cap\overline{\mathbb{R}^2\setminus\Omega}$ sei stückweise glatte Kurve. Sei weiter $\Gamma\subset\mathbb{R}^2$ Gitter. Sei F Fundamentalbereich für Γ. Dann gilt für die Funktion

$$N(\lambda) := \operatorname{card}(\lambda\Omega\cap\Gamma)$$

die Formel

$$N(\lambda) = \frac{vol(\Omega)}{vol(F)}\lambda^2 + O(\lambda)$$

Bemerkung 4.2
Kreisproblem. $\Omega = \{x\in\mathbb{R}^2\colon |x|\geq 1\}$

$$N(\lambda) = \pi\lambda^2 + O(\lambda^{\frac{2}{3}}) \qquad \text{um 1910}$$
$$N(\lambda) = \pi\lambda^2 + O(\lambda^{\frac{7}{11}}) \qquad \text{IWANIEC 1990}$$

Für $\mathbb{R}^1$ ist es trivial und für $\mathbb{R}^n$ mit $n\geq 3$ sind guten Abschätzungen gefunden.

todo: Hier fehlt was

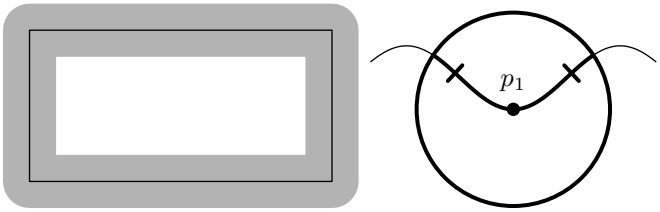


Abbildung 4.1: todo: Was ist das und wo kommt das hin?

Folgerung 4.3
Sei $\Gamma \subset \mathbb{R}^2$ ein Gitter und Ω wie oben. Dann folgt für $N_\Gamma(\Omega) = \operatorname{card} \Gamma \cap \Omega$:

$$|N_\Gamma(\Omega) - \frac{vol(\Omega)}{vol(\Gamma)}| \leq c_1 l(\partial\Omega) + c_2 \qquad (c_1, c_2 > 0)$$

Beweis:
Sei $L\colon \mathbb{R}^2 \to \mathbb{R}^2$ linear, mit $L(\Gamma) = \mathbb{Z}^2$. Dann ist $N_\Gamma(\Omega) = N_{\mathbb{Z}^2}(L(\Omega))$, $vol(L(\Omega)) = |\det L| vol(\Omega)$, $vol(\Gamma) = |\det L|^{-1}$.

$\Rightarrow |N_\Gamma(\Omega) - \frac{vol(\Omega)}{vol(\Gamma)}| = |N_{\mathbb{Z}^2}(L(\Omega)) - vol(L(\Omega))| \leq c_1 l(L(\Omega)) + c_2 \leq c_1' l(\Omega) + c_2$ ∎

Folgerung 4.4
$\exists c = c(\Gamma, \Omega) > 0$, so dass

$$|N_\Gamma(\lambda\Omega) - \frac{vol(\Omega)}{vol(\Gamma)}\lambda^2| \leq c\lambda \qquad \lambda \geq 1$$

Folgerung 4.5

$$\lim_{\lambda\to\infty} \frac{N_\Gamma(\lambda\Omega)}{\lambda^2} = \frac{vol(\Omega)}{vol(\Gamma)}$$

Bemerkung 4.3 (Kreisproblem)
$\Omega = \{x \in \mathbb{R}^2 \colon |x| \leq 1\}, N(\lambda) - \pi\lambda^2 = O(\lambda^a)$. Wir hatten $a = 1$.

Vermutung: Jedes $a + \frac{1}{2}\varepsilon$ ist gut. $a = \frac{1}{2}$ stimmt nicht (Hardy 1916)

Einige Abschätzungen: $a = \frac{2}{3}$ von SIERPINSKI 1906, $a = \frac{7}{11}$ von IWANIEC und MOZZOCHI 1987 und $a = \frac{46}{73}$ HUXLEY 1996

Folgerung 4.6

$$L(1, \chi_K) = \frac{2\pi}{w\sqrt{|d_K|}} h_K \qquad d_K < 0$$

$$L(1, \chi_K) = \frac{2\log \varepsilon_K}{\sqrt{|d_K|}} h_K \qquad d_K > 0$$

Beweis:

$$\zeta_K(s) = \sum_{C \in Cl_K} \underbrace{\sum_{\mathfrak{p} \in C} \frac{1}{(\mathbb{N}\mathfrak{p})^s}}_{=f_C(s)}$$

Wähle $\tilde{\mathfrak{p}} \in C^{-1}$, dann ist für alle $\mathfrak{p} \in C$: $\mathfrak{p} \cdot \tilde{\mathfrak{p}} = (\alpha)$ ein Hauptideal und $\mathbb{N}\mathfrak{p} \cdot \mathbb{N}\tilde{\mathfrak{p}} = |N(\alpha)|$
$\Rightarrow$

$$f_C(s) = (\mathbb{N}\tilde{\mathfrak{p}})^s \sum_{(\alpha), \alpha \in \tilde{\mathfrak{p}}, \alpha \neq 0} \frac{1}{|N(\alpha)|^s}$$

Sei K imaginärquadratisch. $(\alpha) = (\beta) \Leftrightarrow \alpha = \zeta\beta$. $\zeta =$ Einheitswurzel. Also

$$f_C(s) = \frac{1}{w} (\mathbb{N}\tilde{\mathfrak{p}})^s \sum_{\alpha \in \tilde{\mathfrak{p}}, \alpha \neq 0} \frac{1}{|N(\alpha)|^s}$$

Wir ordnen die Zahlen $\alpha \in \tilde{\mathfrak{p}} \setminus 0$ so an, dass $0 < N(\alpha_1) \leq N(\alpha_2) \leq \cdots$

$M(\lambda) = \text{card}\{\alpha \in \tilde{\mathfrak{p}} \setminus 0 \colon N(\alpha) \leq \lambda\} =$ Goiitterpunkte ($\lambda \geq 1$) in Kreisscheibe vom Radius $\sqrt{\lambda}$.

Wir wissen:

$$\lim_{\lambda \to \infty} \frac{M(\lambda)}{\lambda} = \frac{\pi}{vol(\tilde{\mathfrak{p}})}$$

$vol(\tilde{\mathfrak{p}}) = vol(Fundamentalbereich f\ddot{u}r Gitter \tilde{\mathfrak{p}} \subset \mathbb{C})$

Aus todo: Link: Kap 3 §8: $vol(\tilde{\mathfrak{p}}) = \mathbb{N}\tilde{\mathfrak{p}} \cdot \frac{1}{2}\sqrt{|d_K|}$.

Setze $N(\alpha_K) = \lambda_K$, dann gilt

$$M(\lambda_K - \varepsilon) < k \leq M(\lambda_K)$$
$$\frac{M(\lambda_K - \varepsilon)}{\lambda_K - \varepsilon} \frac{\lambda_K - \varepsilon}{\lambda_K} < \frac{k}{\lambda_K} \leq \frac{M(\lambda_K)}{\lambda_K}$$

Für $k \to \infty$ gilt

$$\lim_{k \to \infty} \frac{k}{\lambda_K} = \frac{\pi}{vol(\tilde{\mathfrak{p}})}$$

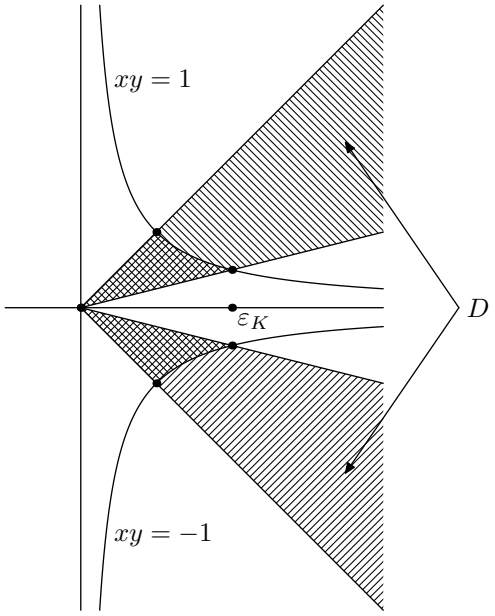


Abbildung 4.2: todo: Was ist das?

also

$$\frac{\pi}{vol(\tilde{\mathfrak{p}})} - \varepsilon < \frac{k}{\lambda_K} < \frac{\pi}{vol(\tilde{\mathfrak{p}})} + s \qquad k \geq k_0$$

$$(\frac{\pi}{vol(\tilde{\mathfrak{p}})^{-s}})^s < \frac{k^s}{\lambda_K^s} < (\frac{\pi}{vol(\tilde{\mathfrak{p}})} + \varepsilon)^s$$

$$\Rightarrow (\frac{\pi}{vol(\tilde{\mathfrak{p}})^{-\varepsilon}})^s \sum_{k_0}^{\infty} \frac{1}{k^s} < \sum_{k_0}^{\infty} \frac{1}{\lambda_K^s} < (\frac{\pi}{vol(\tilde{\mathfrak{p}})^{\varepsilon}})^s \sum_{k_0}^{\infty} \frac{1}{k^s}$$

$$\sum_{k_0}^{\infty} \frac{1}{\lambda_K} = \sum_{k_0}^{\infty} \frac{1}{N(\alpha_K)} = \sum_{\alpha \in \tilde{\mathfrak{p}}, \alpha \neq 0} \frac{1}{N(\alpha)^s} - \text{endlich viele Terme}$$

todo: hfw

Sei nun K reellquadratisch. Geometrische Abbildung $K \to \mathbb{R}^2 \colon \alpha \mapsto (\alpha, \alpha')$.

Wir zeigen nun, dass unter allen zu $\alpha \in \tilde{\mathfrak{p}}$ assoziierten Zahlen β gibt es genau eine, für welche gilt:

1. $\beta > 0$,
2. $\varepsilon_K^{-2} < |\frac{\beta'}{\beta}| \leq 1$

Die assoziierten zu α sind alle Zahlen der Form $\beta = \pm\varepsilon_K^m \alpha, m \in \mathbb{Z}$. $\beta > 0$ erreicht man durch $\pm = \operatorname{sgn} \alpha$. $|\frac{\beta'}{\beta}| = |\varepsilon_K^{-2m} \frac{\alpha'}{\alpha}| = \varepsilon_K^{-2m} |\frac{\alpha'}{\alpha}|$

Das Gebiet mit den Eigenschaften (1) und (2) im $\mathbb{R}^2$ ist in Abbildung 4.2 dargestellt.

$f_C(s) = (\mathbb{N}\tilde{\mathfrak{p}})^s \sum_{\alpha\in\tilde{\mathfrak{p}},\alpha\neq 0} \frac{1}{|N(\alpha)|^s} = (\mathbb{N}\tilde{\mathfrak{p}})^s \sum_{\alpha\in\tilde{\mathfrak{p}}\supset 0,(\alpha,\alpha')\in D} \frac{1}{|N(\alpha)|^s}$

Sei $M(\lambda) := \text{card}\{\alpha \in \tilde{\mathfrak{p}} \setminus 0 \colon (\alpha,\alpha') \in D, |N(\alpha)| \leq \lambda^2\}$.

Wir wählen Gitterpunkte in D, geschnitten mit Hyperbelinneren zu $xy = \lambda^2$

$$\Omega = \{(x,y) \in \mathbb{R}^2 \colon \varepsilon_K^{-2} \leq |\frac{y}{x}| \leq 1, |xy| \leq 1\}$$

Also die Gitterpunkte in $\lambda\Omega$

$$\lim_{\lambda\to\infty} \frac{M(\Omega)}{\lambda^2} = \frac{vol(\Omega)}{vol(\tilde{\mathfrak{p}})}$$

$$\begin{aligned} vol(\Omega) &= 2 \int\limits_{\substack{x,y\geq 0 \\ xy\leq 1 \\ \varepsilon^{-2}\leq\frac{y}{x}\leq 1}} dy\,dx = 2\int_0^1 \int_{\varepsilon^{-2}x}^{x} dy\,dx + 2\int_1^{\varepsilon} \int_{\varepsilon^{-2}x}^{\frac{1}{x}} dy\,dx \\ &= 2\int_0^1 (1-\varepsilon^{-2})x\,dx + 2\int_1^{\varepsilon} \frac{1}{x} - \varepsilon^{-2}x\,dx \\ &= 2(1-\varepsilon^{-2})\frac{1}{2} + 2\log\varepsilon - 2\frac{1}{2} + 2\frac{1}{2}\varepsilon^{-2} \end{aligned}$$

■

Satz 4.1

1. Sei K imaginärquadratisch und w die Anzahl der Einheitswurzeln in K. Dann gilt:

$$\lim_{s\to 1+0}(s-1)\zeta_K(s) = \frac{2\pi h_K}{w\sqrt{|d_k|}}$$

K reellquadratisch und $\varepsilon_K > 1$ Fundamentaleinheit. Dann gilt

$$\lim_{s\to 1+0}(s-1)\zeta_K(s) = \frac{2h_K \log\varepsilon_K}{\sqrt{|d_K|}}$$

Folgerung 4.7

$$L(1,\chi_D) = \begin{cases} \frac{2\pi}{w\sqrt{|d_K|}} h_K & d_K < 0 \\ \frac{2\log\varepsilon_K}{\sqrt{|d_K|}} h_K & d_K > 0 \end{cases}$$

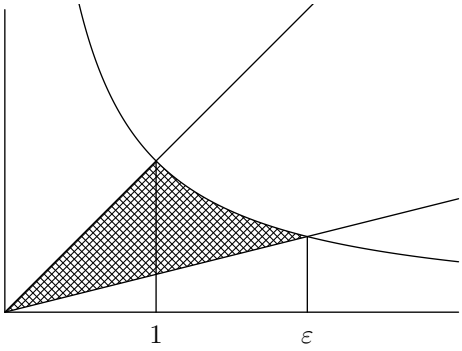


Abbildung 4.3: todo: Was ist das und wo soll das hin?

4.2 Die Berechnung von $L(1, \chi_D)$

Definition 4.2
Sei $m \geq 1$ und χ der Direchlet-Charakter $mod^* m$, ζ fixierte primitive $n.$ Einheitswurzel; z. B.

$$\zeta = e^{\frac{2\pi i}{m}} \in \mathbb{C}$$

Die **Gausssche Summe** $G = G(a, \chi)$ ist definiert durch

$$G(a, \chi) = G_a(\chi) = \sum_{x \pmod m} \chi(x)\zeta^{ax}$$

für $a \in \mathbb{Z}/m\mathbb{Z}$

Bemerkung 4.4
Die **eulersche Gammafunktion**

$$\begin{aligned} \Gamma(s) &= \int_0^\infty e^{-x} x^{s-1}\, dx \\ &= \int_{\mathbb{R}_+^*} e^{-x} x^s \frac{dx}{x} \end{aligned}$$

$\frac{dx}{x}$ ist ein HAAR-Maß, e^{-x} ist ein additiver Charakter auf $\mathbb{R}$ und x^s ist multiplikativer Charakter auf $\mathbb{R}^*$.

$m = p$ $G(a, \chi) = \int_{\mathbb{F}_p} \chi(x)\zeta^{ax}\, dx$

$s\Gamma(s) = \Gamma(s+1)$

$\Gamma(n+1) = n!$, $\Gamma(\frac{1}{2}) = \sqrt{\pi}$

$\Gamma(s)\Gamma(1-s) = \frac{\pi s}{\sin \pi s}$

Fakt 4.3
Sei $\chi + \chi_0$ Direchlet-Charakter *modulo*$^*m$, dann gilt für $s > 1$:

$$L(s,\chi) = \frac{1}{m}\sum_{a=0}^{m-1} G(a,\chi)\sum_{n=1}^{\infty}\frac{\zeta^{-an}}{n^s}$$

Beweis:
Da $s > 1$ im Bereich der absoluten konvergenz, daher können wir fröhlich umordnen.

$$\begin{aligned}\sum_{a=0}^{m-1} G(a,\chi)\zeta^{-an} &= \sum_{a=0}^{m-1}\sum_{x \pmod m}\chi(x)\zeta^{a(x-n)}\\ &= \sum_{x \pmod m}\chi(x)\sum_{a=0}^{m-1}\zeta^{a(x-n)} = \sum_{x \pmod m}\chi(x)\frac{\zeta^{m(x-n)}-1}{\zeta^{x-n}-1} =\\ &= \begin{cases}0 & n \not\equiv x \pmod m\\ m & n \equiv x \pmod m\end{cases}\end{aligned}$$

Also ist das gleich $m\chi(n)$. ∎

Bemerkung 4.5
Man kann $a = 0$ weglassen wegen $G(0,\chi) = \sum_{x \pmod m}\chi(x) = 0$ für $\chi \neq \chi_0$

Fakt 4.4
Sei $0 < \theta < 2\pi$, dann konvergiert

$$\sum_{n=1}^{\infty}\frac{e^{in\theta}}{n^s}$$

für alle $s > 0$ und sogar gleichmäßig für $s \geq \delta > 0$. Insbesonere ist das stetige Funktion auf $(0,\infty)$.

Beweis:
Abelsche Summation

$$\left|\sum_{n=M}^{N} e^{in\theta}\right| = \left|\sum_{n=0}^{N-M} e^{in\theta}\right| = \frac{|e^{i(N-M+1)\theta}-1|}{|e^{i\theta}-1|} \leq \frac{2}{|e^{i\theta}-1|}$$

Weiter wie bei $L(s,\chi)$. ∎

Folgerung 4.8

$$L(1,\chi) = \frac{1}{m}\sum_{a=1}^{m-1} G(a,\chi)\sum_{n=1}^{\infty}\frac{\zeta^{-an}}{n}$$

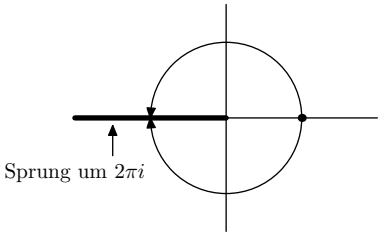


Abbildung 4.4: Monodromie

Bemerkung 4.6
Man hat einen Homomorphismus $\mathbb{C}\colon \mathbb{C}^*\colon z \mapsto e^z = \sum \frac{1}{n} 2^n$. Sie ist surjektiv, aber nicht injektiv, und $e^z = 1 \Leftrightarrow z = 2\pi i m$ mit $m \in \mathbb{Z}$. Insbesondere ist $e^{2\pi i} = 1$. Also hat jedes $z \in \mathbb{C}^*$ unendlich viel Logarithmen $0 \neq z = re^{i\pi}$ mit $r = |z| > 0$ und $0 \leq \varphi < 2\pi$.

$$\log z = \log|z| + i\varphi + 2\pi i m$$

mit $m \in \mathbb{Z}$.

Schlitze $\mathbb{C}$ entlang der negativen reellen Achse auf. Betrachte $\mathbb{C} \setminus (-\infty,0] \ni z = re^{i\varphi}, r > 0, -\pi < \varphi < \pi$. Wir definieren $\log z = \log|z| + i\varphi$. $\log \mathbb{C} \setminus (-\infty,0]) \to \mathbb{C}$ ist stetig und holomorph (**Hauptzweig des Logarithmus**)

Monodromie: Abbildung 4.4.

Betrachten $f(z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$ für $|z| < 1$. f ist stetig (sogar holomorph) und es gilt

$$-\log(1-z) = f(z)$$

log ist der Hauptzweig

Beweis:
Jedenfalls gilt $e^{f(z)} = \frac{1}{1-z}$, denn (wir können ableiten, weil absolutkonvergent)

$$\begin{aligned}((1-z)e^{f(z)})' &= -e^{f(z)} + (1-z)f'(z)e^{f(z)} \\ &= -e^{f(z)} + (1-z)\frac{1}{1-z}e^{f(z)} = 0\end{aligned}$$

$\Rightarrow (1-z)e^{f(z)}$ ist konstant, $z = 0$ zeigt es. ∎

$f(z)$ ist reell für reelles z, also reelles $|z| < 1$ durchläuft $1 - z$ die Kreisscheibe Abbildung 4.5.

Folgerung 4.9

$$\sum_{n=1}^{\infty} \frac{e^{in\theta}}{n} = -\log(1 - e^{i\theta})$$

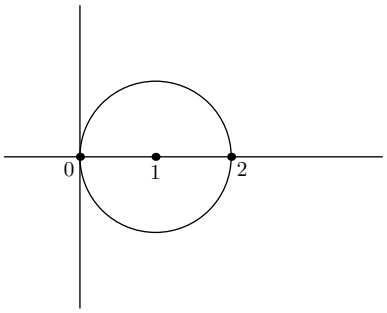


Abbildung 4.5: Darstellung von $f(z)$

Beweis:
Satz von Abel. ∎

Einschub:

Lemma 4.1 (Satz von Abel)
Sei $\sum_{n=0}^{\infty} a_n z^n$ eine Potenzreihe mit Konvergenzradius $R > 0$. $\sum a_n R^n$ konvergiere. Dann gilt für $x \in \mathbb{R}$

$$\lim_{x \to R-0} \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n R^n$$

Beweis:

$$\sum a_n x^n = \sum a_n R^n \big(\frac{x}{R}\big)^n$$

nehmen Teilreihe raus:

$$\sum_{n=M}^{N} a_n R^n \big(\frac{x}{R}\big)^n = \sum_{n=M}^{N-1} s_n \Big(\big(\frac{x}{R}\big)^n - \big(\frac{x}{R}\big)^{n+1}\Big) + s_N \big(\frac{x}{R}\big)^N$$

$$\Rightarrow |\sum_{n=M}^{N} a_n R^n \big(\frac{x}{R}\big)^n| \leq \varepsilon \Big(\sum_{n=M}^{N} \big(\frac{x}{R}\big)^n - \big(\frac{x}{R}\big)^{n+1} + \big(\frac{x}{R}\big)^N\Big) = \varepsilon \big(\frac{x}{R}\big)^M < \varepsilon$$

$\Rightarrow$ absolutkonvergent. für $0 \leq x \leq R \Rightarrow$ Grenze stetig. ∎

Lemma 4.2
Sei $0 < \theta < 2\pi$, dann gilt:

$$\sum_{n=1}^{\infty} \frac{e^{in\theta}}{n} = -\log(2 \sin \frac{\theta}{2}) + i(\frac{\pi}{2} - \frac{\theta}{2})$$

Beweis:

$$\begin{aligned} 1 - e^{i\theta} &= e^{\frac{i\theta}{2}}(e^{-\frac{i\theta}{2}}) - e^{-\frac{i\theta}{2}} \\ &= -2i \sin\frac{\theta}{2} e^{\frac{i\theta}{2}} \\ &= 2\sin(\frac{\theta}{2}) e^{i(-\frac{\pi}{2}+\frac{\theta}{2})} \end{aligned}$$

Dabei gilt $0 < \frac{\theta}{2} < \pi$, also $\sin\frac{\theta}{2} > 0$. $-\frac{\pi}{2} < \frac{\theta}{2} - \frac{\pi}{2} < \frac{\pi}{2}$.

$$\log(1 - e^{i\theta}) = \log(2\sin\frac{\theta}{2}) + i(\frac{\theta}{2} - \frac{\pi}{2})$$

(Hauptzweig)

$$-\log(1 - e^{i\theta}) = -\log(2\sin\frac{\theta}{2}) + i(\frac{\pi}{2} - \frac{\theta}{2})$$ ∎

Beispiel 4.1
Für $\theta = \pi$ ergibt sich die harmonische Reihe:

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n} = -\log 2$$

Folgerung 4.10

$$\sum_{n=1}^{\infty} \frac{\zeta^{-an}}{n} = -\log(2\sin\frac{\pi a}{m}) - \pi i(\frac{1}{2} - \frac{a}{m})$$

für alle $0 < a < m$
Beweis:

$$\sum \frac{\zeta^{an}}{n} = -\log(2\sin\frac{\pi a}{m}) + i(\frac{\pi}{2} - \frac{\pi a}{m})$$
$$\zeta^a = e^{2\pi i \frac{a}{m}}$$

also $\theta = \frac{2\pi a}{m}$. Dabei ist $0 < a < m$ zu nehmen!

Komplexe Konjunktion (wenn eine komplexe Funktion konvergiert, dann konvergiert die konjugiert komplexe Reihe zum konjugiert komplexen Grenzwert) gibt

$$\sum_{n=1}^{\infty} \frac{\zeta^{-an}}{n} = -\log(2\sin\frac{\pi a}{m}) - \pi i(\frac{1}{2} - \frac{a}{m})$$ ∎

Fakt 4.5
Wir haben einen endlichen Ausdruck für $L(1, \chi)$ gefunden:

$$L(1, \chi) = \frac{1}{m} \sum_{a=1}^{m-1} G(a, \chi)(-\log(2\sin\frac{\pi a}{m}) + \pi i(\frac{1}{2} - \frac{a}{m}))$$

4.3 Gausssche Summen

Wir wollen die Zahlen $G(a,\chi)$ berechnen und machen es aus nahliegenden Gründen nur für $\chi = \chi_K$.

Zur Erinnerung: ($p_j > 2$ verschieden)

$$d_K \equiv 1 \pmod 4 \Rightarrow d_K = (-1)^{\varepsilon} p_1 \cdots p_r$$
$$\chi_K = \left(\frac{\cdot}{p_1}\right) \cdots \left(\frac{\cdot}{p_r}\right)$$
$$d_K \equiv 0 \pmod 4, d_K/4 \equiv 2 \pmod 4$$
$$\chi_K = \varepsilon_{\pm 8} \cdot \left(\frac{\cdot}{p_1}\right) \cdots \left(\frac{\cdot}{p_r}\right)$$
$$(\varepsilon_8 \text{ für } d_K/8 \equiv 1 \pmod 4, \varepsilon_{-8} \text{ für } d_K/8 \equiv 3 \pmod 4)$$
$$d_K/4 \equiv 0{,}3 \pmod 4$$
$$\chi_K = \varepsilon_{-4}\left(\frac{\cdot}{p_1}\right) \cdots \left(\frac{\cdot}{p_r}\right)$$

Bemerkung 4.7
Ist χ_1 Charakter modulo m und χ_2 ein Charakter modulo n, so ist $\chi_1\chi_2$ Charakter modulo $m \cdot n$.

Fakt 4.6
Sei $\mathrm{ggT}(m,n) = 1$, χ_1 Charakter modulo m, χ_2 Charakter modulo n und $a \in \mathbb{Z}$. Dann gilt für den Charakter $\chi_1 \cdot \chi_2 \pmod{nm}$

$$G(a, \chi_1 \cdot \chi_2) = \chi_1(n)\chi_2(m)G(a,\chi_1)G(a,\chi_2)$$

Beweis:
$\exists x, y \in \mathbb{Z}$: $mx + ny = 1$. Also $\chi_1(ny) = 1$ und $\chi_2(mx) = 1$.

$$\zeta_{mn} = e^{\frac{2\pi i}{mn}} = e^{\frac{2\pi i(mx+ny)}{mn}}$$
$$e^{\frac{2\pi i x}{n}} e^{\frac{2\pi i y}{m}} = \zeta_n^x \zeta_m^y$$

Durchläuft r die Zahlen $0{,}1, \ldots, m-1$ und s die Zahlen $0{,}1, \ldots, n-1$, so durchläuft $rn + sm$ alle Restklassen modulo m.

$$\begin{aligned} G(a, \chi_1\chi_2) &= \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} \chi_1(rn+sm)\chi_2(rn+sm)\zeta_{mn}^{a(rn+sm)} \\ &= \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} \chi_1(rn)\chi_2(sm)\zeta_n^{ax(rn+sm)}\zeta_m^{ay(rn+sm)} \\ &= \sum_{r=1}^{m-1} \sum_{s=1}^{n-1} \chi_1(n)\chi_2(m)\chi_1(r)\chi_2(s)\zeta_n^{axsm}\zeta_m^{ayrn} \end{aligned}$$

Nun gilt $\mathrm{ggT}(y,m) = \mathrm{ggT}(x,n) = 1$, also durchläuft mit r auch ynr ein Restklassensystem modulo m.

Gleiches gilt für xns. $r_1 = ynr$ und $s_1 = xms$. Somit

$$\begin{aligned} G(a,\chi_1\chi_2) &= \sum_{r_1}\sum_{s_1} \chi_1(n)\chi_1(y^{-1}n^{-1}r_1)\chi_2(m)\chi_2(x^{-1}m^{-1}s_1)\zeta_m^{ar_1}\zeta_n^{as_1} \\ &= \chi_1(y^{-1})\chi_2(x^{-1})\sum_{r_1}\chi_1(r_1)\zeta_m^{ar_1}\sum_{s_1}\chi_2(s_1)\zeta_n^{as_1} \\ &= \chi_1(n)\chi_2(m)G(a,\chi_1)G(a,\chi_2) \end{aligned}$$

■

Folgerung 4.11
$m = m_1 \cdots m_r$, $\mathrm{ggT}(m_i,m_j) = 1\ \forall i \neq j$. $\chi_i \pmod{m_i}$, $\chi = \prod \chi_i$. Dann gilt für $a \in \mathbb{Z}$:

$$G(a,\chi) = \prod_{i=1}^{r}(G(a,\chi_i)\cdot\chi_i(\frac{m}{m_i}))$$

Beweis:
Induktion über r für dem Indukitionsanfang siehe oben. ■

Satz 4.2 (nach Gauss)

$$G(1,(\tfrac{\cdot}{p})) = \begin{cases} \sqrt{p} & p \equiv 1 \pmod 4 \\ i\sqrt{p} & p \equiv 3 \pmod 4 \end{cases}$$

Beweis:

$$\begin{aligned} G\overline{G} &= \sum_{x,y=1}^{p-1}(\frac{xy}{p})\zeta_p^{x-y} && \text{substituiere } y = xz \\ |G|^2 &= \sum_{x,z=1}^{p-1}(\frac{x^2z}{p})\zeta_p^{(1-z)} \\ &= \sum_{x,z=1}^{p-1}(\frac{z}{p})\zeta_p^{x(1-z)} \\ &= \sum_z(\frac{z}{p})\sum_{x=1}^{p-1}\zeta_p^{x(1-z)} \end{aligned}$$

Es gilt:

$$\sum_{x=1}^{p-1}\zeta_p^{ax} = \begin{cases} p-1 & a \equiv 0 \pmod p \\ -1 & a \not\equiv 0 \pmod p \end{cases}$$

$$|G|^2 = (\frac{1}{p})(p-1) + \sum_{z \neq 1,0} (\frac{z}{p})(-1) = p - 1 - \sum_{z \neq 1,0} (\frac{z}{p}) = p$$

$\Rightarrow |G|^2 = p$

Andererseits:

$$\begin{aligned} \overline{G} &= \sum_{x=1}^{p-1} (\frac{x}{p}) \zeta_p^{-x} && (y = -x) \\ &= \sum_{y=1}^{p-1} (\frac{-y}{p}) \zeta_p^y = (\frac{-1}{p}) \sum (\frac{y}{p}) \zeta_p^y \\ \Rightarrow \overline{G} &= (\frac{-1}{p}) \cdot G \\ \Rightarrow G^2 &= (\frac{-1}{p}) p \end{aligned}$$

Also

$$G = \begin{cases} \pm\sqrt{p} & p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & p \equiv 3 \pmod 4 \end{cases}$$

Nun Schurs Beweis für das Vorzeichen:

$$M := (\zeta_p^{xy})_{0 \leq x,y \leq p-1} \zeta_p = e^{\frac{2\pi i}{p}}$$

$$\operatorname{Tr} M = \sum_{x=0}^{p-1} \zeta_p^{x^2}$$

Durchläuft a die Quadrate in $\mathbb{F}_p^*$ und b die Nichtquadrate in $\mathbb{F}_p^*$, so ist

$$1 + \sum_a \zeta_p^a + \sum_b \zeta_p^b = 0$$

Andererseits ist

$$G = \sum_a \zeta_p^a - \sum_b \zeta_p^b = 1 + 2 \sum_a \zeta_p^a = \sum_{x=0}^{p-1} \zeta_p^{x^2}$$

$\Rightarrow \operatorname{Tr} M = G$.

M^2 hat folgende Einträge

$$\sum_{i=0}^{p-1} \zeta_p^{xi} \zeta_p^{iy} = \sum_{i=0}^{p-1} \zeta_p^{i(x+y)}$$

Also

$$M^2 = \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & & & p \\ \vdots & & \ddots & \\ 0 & p & & \end{pmatrix}$$

Seien $\lambda_1, \dots, \lambda_p$ die Eigenwerte von M, dann sind $\lambda_1^2, \dots, \lambda_p^2$ die Eigenwerte von M^2.

Das charakteristische Polynom von M^2 ist

$$\det \begin{pmatrix} x-p & \dots & & \\ & x & & -p \\ & & \ddots & \\ & -p & & x \end{pmatrix} = (x-p) \det \begin{pmatrix} x & & -p \\ & \ddots & \\ -p & & x \end{pmatrix}$$

$= (x-p)((x+p)(x-p))^{\frac{p-1}{2}} = (x-p)^{\frac{p-1}{2}}(x+p)^{\frac{p-1}{2}}$. Übungsaufgabe.

Also sind undern den λ_i^2 $\frac{p+1}{2}$ viele gleich p, $\frac{p-1}{2}$ viele $= -p$. Die Eigenwerte λ_i sind $\pm\sqrt{p}, \pm i\sqrt{p}$.

Seien a, b, c, d die Anzahlen der λ_i gleich

$$\sqrt{p}, -\sqrt{p}, i\sqrt{p}, -i\sqrt{p}$$

Es gilt $a + b = \frac{p+1}{2}$ und $c + d = \frac{p-1}{2}$

$$G = (a - b + (c - d)i)\sqrt{p} \qquad (G = \sum \lambda_i)$$

(Da $\operatorname{Tr} M$ auch die Summe der Eigenwerte ist.)

Es folgt

$$a - b = \pm 1, c = d \qquad \text{für } p \equiv 1 \pmod 4$$
$$a - b = 0, c - d = \pm 1 \text{für } p \equiv 3 \pmod 4$$

$$(\det M)^2 = \det \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & 0 & \dots & p \\ \vdots & & & p \\ 0 & p & & 0 \end{pmatrix} = (-1)^{\frac{p(p-1)}{2}} p^p$$

$$\det M = \pm i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}$$

M ist eine Vandermondsche Matrix, also kann man die Determinante auch mit der Formel

$$\det M = \prod_{0\le s<r\le p-1} \zeta_p^r - \zeta_p^s$$

$\eta = e^{\frac{\pi i}{p}} = \zeta_{2p} = \cos\frac{\pi}{p} + i\sin\frac{\pi}{p}$

$$\begin{aligned}
&= \prod_{0\le s<r\le p-1} \eta^{r+s}(\eta^{r-s} - \eta^{s-r}) \\
&= \prod_{0\le s<r\le p-1} \eta^{r+s}(2i\sin\frac{(r-s)\pi}{p}) \\
&= \prod_{0\le s<r\le p-1} \eta^{r+s} \prod_{0\le s<r\le p-1} 2i\sin\frac{(r-s)\pi}{p} \\
\sum_{0\le s<r\le p-1} r+s &= \sum_{r=1}^{p-1}\sum_{s=0}^{r-1} r+s = \sum_{r=1}^{p-1} r^2 + \frac{r(r-1)}{2} \\
&= \frac{3}{2}\frac{1}{6}p(p-1)(2p-1) - \frac{1}{2}\frac{p(p-1)}{2} \\
&= 2p\Big(\frac{p-1}{2}\Big)^2 \equiv 0 \pmod{2p} \\
\Rightarrow \prod_{0\le s<r\le p-1} \eta^{r+s} &= 1 \\
\det M &= \prod_{0\le s<r\le p-1} 2i\sin\frac{\pi(r-s)}{p} \\
&= 2^{\frac{p(p-1)}{2}} i^{\frac{p(p-1)}{2}} \underbrace{\prod_{0\le s<r\le p-1} \sin\frac{\pi(r-s)}{p}}_{>0} \\
\Rightarrow \det M &= +i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}} \\
\det M &= \prod \lambda_i = (-1)^b i^c (-i)^d p^{\frac{p}{2}} \\
&= i^{2b+c-d} p^{\frac{p}{2}} \\
\Rightarrow 2b + c - d &\equiv \frac{p(p-1)}{2} \pmod 4
\end{aligned}$$

Sei $p \equiv 1 \pmod 4 \Rightarrow$

$$a - b \equiv \frac{p+1}{2} - 2b \equiv \frac{p+1}{2} - p\frac{p-1}{2} \equiv 1 \pmod 4$$

$\Rightarrow a - b = +1$.

Sei $p \equiv 3 \pmod 4 \Rightarrow$

$$c - d \equiv \frac{p(p-1)}{2} - 2b \equiv -\frac{p-1}{2} - 2b \equiv -\frac{p-1}{2} - a - b \equiv -\frac{p-1}{2} - \frac{p+1}{2} \equiv -p \equiv 1 \pmod 4$$

$\Rightarrow c - d = +1$.

Zurück und einsetzen in die Formel $G = (a - b + (c - d)i)\sqrt{p}$

$$G = \begin{cases} \sqrt{p} & p \equiv 1 \pmod 4 \\ i\sqrt{p} & p\sqrt{3} \pmod 4 \end{cases}$$

■

Beispiel 4.2

1. $p = 3$, $\zeta_3 = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$

$$G(1, \left(\frac{\cdot}{3}\right) = (\frac{0}{3})\zeta_3^0 + (\frac{1}{3})\zeta_3^1 + (\frac{2}{3})\zeta_3^2 = \zeta_3 - \zeta_3^2 = \zeta_3 - \overline{\zeta_3} = i\sqrt{3}$$

2. $p = 5$

$$G(1, \left(\frac{\cdot}{5}\right) = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$

Beweis:

$$G = \sum (\frac{x}{p})\zeta_p^x, \zeta_p = e^{\frac{2\pi i}{p}}$$

4.4 2007 – Interessante Ergebnisse zur Jahreszahl

todo: hier fehlt der Anfang

$2007 = 9 \cdot 223$, $223 \equiv 3 \pmod 4$, $K = \mathbb{Q}(\sqrt{-2007}) = \mathbb{Q}(\sqrt{-223})$

Ganzheitsbasis: $1, \frac{1+\sqrt{-223}}{2} = \omega$

$$\begin{aligned} N(a + b\omega) &= \left(a + \frac{b}{2}\right)^2 + \frac{b^2}{4} \cdot 223 \\ &= a^2 + ab + 56b^2 \qquad\qquad d_k = -223 \end{aligned}$$

$$\mathbb{N}\mathfrak{p} \leq \frac{2}{\pi}\sqrt{223} \leq 20$$

2 ist zerlegt, $d_K \equiv 1 \pmod 8$

$$\begin{aligned} (\frac{-223}{3}) = (\frac{-1}{3}) &= -1 && \Rightarrow 3 \text{ träge} \\ (\frac{-223}{5}) = (\frac{2}{5}) &= -1 && \Rightarrow 5 \text{ träge} \\ (\frac{-223}{7}) = (\frac{-13}{7}) = (\frac{1}{7}) &= 1 && \Rightarrow 7\text{zerlegt} \end{aligned}$$

Cl_K erzeugt von $\mathfrak{p}_2$ und $\mathfrak{p}_7$. Beide keine Hauptideale: $\alpha = a+b\omega, b = 1$

a	$N(a+b\omega) = a^2+ab+56b^2$
1	$58 = 2 \cdot 29$
2	$62 = 2 \cdot 31$
3	$68 = 2 \cdot 2 \cdot 17$
4	$76 = 2 \cdot 2 \cdot 19$
5	$86 = 2 \cdot 43$
6	$98 = 2 \cdot 49$
7	$112 = 2^4 \cdot 7$
8	$128 = 2^7$

$\mathfrak{p}_2\mathfrak{p}_7^2 \sim 1, \mathfrak{p}_2^4\mathfrak{p}_7 \sim 1 \Rightarrow \mathfrak{p}_2$ erzeugt Cl_k, $\mathfrak{p}_2^7 \sim 2 \Rightarrow Cl_K$ zyklisch der Ordnung 7

$L = \mathbb{Q}(\sqrt{2007}) = \mathbb{Q}(\sqrt{223})$, $d_K = 4 \cdot 223 = 892$,

$1, \omega = \sqrt{223}$ Ganzheitsbasis

4.4.1 Kettenbruchzerlegung von $\sqrt{223}$

$$\begin{aligned}
\sqrt{223} &= 14 + (\omega - 14) \\
\frac{1}{\omega - 14} &= \frac{\omega + 14}{27} = 1 + \frac{\omega - 13}{27} \\
\frac{27}{\omega - 13} &= \frac{27(\omega + 13)}{58} = 13 + \frac{\omega - 13}{2} \\
\frac{2}{\omega - 13} &= \frac{2(\omega + 13)}{13} = 1 + \frac{\omega - 14}{27} \\
\frac{27}{\omega - 14} &= \frac{27(\omega + 14)}{27} = \omega + 14 = 28 + (\omega - 14)
\end{aligned}$$

$\sqrt{223} = [14; \overline{1,13,1,28}]$

n	0	1	2	3	4	5
a_n		14	1	13	1	28
p_n	1	14	15	209	224	
q_n	0	1	1	14	15	
$p_n^2 - 223q_n^2$		-27	2	73	1	

$\varepsilon_K = 224 + 15\sqrt{223}$

Cl_K: $\mathbb{N}\mathfrak{p} \leq \frac{1}{2}\sqrt{4 \cdot 223} = \sqrt{223} < 15$.

2 verzweigt:

$$
\begin{aligned}
(\frac{223}{3}) = (\frac{1}{3}) = 1 && \text{3 zerlegt}\\
(\frac{223}{5}) = (\frac{3}{5}) = -1 && \text{5 träge}\\
(\frac{223}{7}) = (\frac{13}{7}) = (\frac{-1}{7}) = -1 && \text{7 träge}\\
(\frac{223}{11}) = (\frac{3}{11}) = (-1)^{15}(\frac{11}{3}) = -(\frac{2}{3}) = 1 && \text{11 zerlegt}\\
(\frac{223}{13}) = (\frac{-37}{13}) = (\frac{2}{3}) = -1 && \text{13 träge}
\end{aligned}
$$

Cl_K erzeugt durch $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_{11}$.

$N(a + b\omega) = a^2 - 223b^2$

	a	$a^2 - 223$	
$b = 1$	15	2	$\Rightarrow \mathfrak{p}_2 = (12 + \omega) \sim 1$
	16	33	$\Rightarrow \mathfrak{p}_3\mathfrak{p}_{11} \sim 1$
	14	-27	$\Rightarrow \mathfrak{p}_3^3 \sim 1$
	17	66	$\Rightarrow \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_{11} \sim 1$
	13	$-54 = -2 \cdot 3^3$	$\Rightarrow \mathfrak{p}_3^3 \sim 1$

Cl_K erzeugt von $\mathfrak{p}_3$, $h_K = 1{,}3$

Ist $\mathfrak{p}_3$ ein Hauptideal?

$$
\begin{gathered}
\mathfrak{p}_3 = (\alpha), |N\alpha| = 3, \alpha = a + b\sqrt{223}, a, b \in \mathbb{Z}\\
a^2 - 223b^2 = \pm 3 \Rightarrow = -3\\
a^2 - 223b^2 = 3 \Rightarrow (\frac{3}{223}) = 1, (\frac{3}{223}) = -(\frac{223}{3}) = -(\frac{1}{3}) = -1
\end{gathered}
$$

$N(\alpha) = -3 \Rightarrow N(\varepsilon_K^m \alpha) = -3$ Also existieren Lösungen, so auch solche mit $1 < \alpha < \varepsilon_K < 450$. $\alpha\alpha' = -3 \Rightarrow \alpha' = -\frac{3}{\alpha}$

$$
\begin{gathered}
1 < a + b\sqrt{223} < 450\\
\Rightarrow \frac{1}{450} < \frac{1}{\alpha} < 1\\
\Rightarrow -3 < -\frac{3}{\alpha} < -\frac{3}{450}\\
-3 < a - b\sqrt{223} < -\frac{3}{450}\\
\Rightarrow -2 < 2a < 450 - \frac{3}{450} \Rightarrow a > 0 \Rightarrow b > 0
\end{gathered}
$$

Also $0 < b < \frac{450}{\sqrt{223}} < 30{,}2$. Also: Man mustere die 30 Zahlen $223b^2 - 3$ $b = 1{,}2, \ldots, 30$ durch, ob ein Quadrat vorkommt. – Es kommt kein Quadrat vor $\Rightarrow Cl_K$ ist zyklisch der Ordnung 3.

4.4.2 Alle Darstellung von 223 als Summe von vier Quadraten

.

Die Formel von Jaccobi besagt, dass für ungerades n die Anzahl der Quadrupel

$$r_4(n) = 8 \sum_{d|n} d$$

$r_4(223) = 8 \cdot 224 = 2^8 \cdot 7$, $r_4(223) = \text{card}\{m \in \mathbb{Z}^4 \colon \|m\|^2 = 223\}$

Wir wollen keinen Brute-force-Angriff machen. Ansatz für systematisches Suche:

$$\begin{gathered} 223 = a^2 + b^2 + c^2 + d^2 \\ 223 = 7 \pmod 8 \Rightarrow \text{keine Darstellung durch 3} \\ x^2 \equiv 0{,}1{,}4 \pmod 8 \\ \Rightarrow x^2 + y^2 + z^2 \equiv 7 \pmod 8 \end{gathered}$$

Wir nennen eine Lösung (a, b, c, d) generisch $:\Leftrightarrow 0 < a < b < c < d$. Sonst ausgeartet.

1. $223 = a^2 + b^2 + 2c^2$
2. $223 = a^2 + 3b^2$

Generische Lösung liefert $16 \cdot 24 = 2^7 \cdot 3$ Vektoren:

1. liefert $16 \cdot 12 = 2^6 \cdot 3$ Vektoren
2. liefert $16 \cdot 4 = 2^6$ Vektoren

Mit r bezeichnen wir die Anzahl der generischen Lösungen. Mit s unt t bezeichnen wir die Anzahl der Lösungen, die nach Typ (1) bzw. (2) (Auszählung oben) ausgeartet sind.

$2^8 \cdot 7 = 2^7 \cdot 3r + 2^6 \cdot 3s + 2^6 t$
$28 = 2^2 \cdot 7 = 6r + 3s + t$

b	$223 - 3b^2$
1	220
2	209
3	$196 = 14^2$
4	175
5	148
6	115
7	76
8	31

einzige Lösung $t = 1 \Rightarrow$ (14,3,3,3).

1	$221 = 13 \cdot 17 = 10^2 + 11^2 = 5^2 + 14^2$
2	$215 = 5 \cdot 43$
3	$205 = 5 \cdot 41 = 13^2 + 6^2 = 14^2 + 3^2$
5	$173 \equiv 1 \pmod 4 \Rightarrow 13^2 + 2^2$
7	$125 = 5^3 = 10^2 + 5^2 = 11^2 + 2^2$
9	$61 \equiv 1 \pmod 4 \Rightarrow 6^2 + 5^2$

gefunden 6 Lösungen dieses Typs: (11,10,1,1), (14,5,1,1), (13,6,3,3), (14,3,3,3), (13,5,5,2), (10,7,7,5), (11,7,7,2), (9,9,6,5

$28 = 6r + 21 + 1 \Rightarrow r = 1$

Raten: erster Versuch $223 - 14^2 = 27$ lässt sich nicht als Summe von 3 Quadraten darstellen. Nächster Versuch: $223 - 13^2 = 54 = 49 + 4 + 1$

Also einzige generische Lösung: $223 = 13^2 + 7^2 + 2^2 + 1^2$

4.4.3 Alle Gruppen der Ordnung 2007

abelsche: $c_3 \times c_3 \times c_{223}, c_1 \times c_{223}$.

SYLOW: $N_P = \text{card}\, P\text{-SYLOW-Gruppen}, N_P \equiv 1 \pmod p, N_P \mid (G : 1)$

$N_3 \equiv 1 \pmod 3, N_3 \mid 2007$: 1,3,9,223,3 · 223, 2007
$N_3 = 1$ oder $N_3 = 223$
$N_{223} \equiv 1 \pmod{223} \Rightarrow N_{223} = 1 \Rightarrow G_{223}$ ist nicht trivial.

G_{223} und G_3 sind „disjunkt“: $G_{223} \cap G_3 = \{1\}$.

$\Rightarrow G$ ist semidirektes Produkt.

G_3 operiert dich Konjunktion auf C_{223}. $G_3 \to Aut(C_{223}) = (\mathbb{Z}/223\mathbb{Z})^*$ ist eine zyklische Gruppe der Ordnung 222, $222 = 2 \cdot 3 \cdot 37$. (*Aut* ist Automorphismus)

$\Rightarrow$ insgesamt noch zwei Isotypen nicht abelscher Gruppen.

Weiter im eigentlichen Vorlesungsstoff!

Fakt 4.7

$$\begin{aligned} G(\varepsilon_{-4}) &= 2i \\ G(\varepsilon_8) &= \sqrt{8} \\ G(\varepsilon_{-8}) &= i\sqrt{8} \end{aligned}$$

Beweis:

$$\begin{array}{r|cccc} \varepsilon_8 & 1 & -1 & -1 & 1 \\ \varepsilon_{-8} & 1 & 1 & -1 & -1 \end{array}$$

$$\begin{aligned} G(\varepsilon_{-4}) &= \varepsilon_{-4}(1)\zeta_4 + \varepsilon_{-4}(3)\zeta_4^3 = i - i^3 = 2i \\ G(\varepsilon_8) &= \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 \\ &= 2\cos\frac{2\pi}{8} - 2\cos\frac{6\pi}{8} = 2\cos\frac{\pi}{4} - 2\cos\frac{3\pi}{4} = \sqrt{2} + \sqrt{2} = 2\sqrt{2} \\ G(\varepsilon_{-8}) &= \zeta_8 + \zeta_8^3 - \zeta_8^5 - \zeta_8^7 = 2i\sin\frac{\pi}{4} - 2i\sin\frac{3\pi}{4} = 2i\sqrt{2} \end{aligned}$$

■

Fakt 4.8
$G(a, \chi_K) = \chi_K(a)G(\chi_K)$

Beweis:

$$G(a, \chi_K) = \sum_{x \mod^* |d_K|} \chi_K(x)\zeta_p^{ax}$$

Mit x durchläuft auch ax die primen Restklassen $\mod |d_K|$, falls nur a prime Restklasse ist. $\Rightarrow$

$$G(a, \chi_K) = \sum_{y \mod^* |d_K|} \chi_K(a^{-1}y)\zeta_p^y = \chi_K(a^{-1})G(\chi_K)$$

$\chi_K^2 \equiv 1 \Rightarrow \chi_K(a) = \chi_K(a^{-1})$.

Übungsuafgabe: Ist $(a, d_K) > 1$, so ist $G(a, \chi_K) = 0$. ■

Fakt 4.9

$$G(\chi_K) = \begin{cases} \sqrt{|d_K|} & d_K > 0 \\ i\sqrt{|d_K|} & d_K < 0 \end{cases}$$

Beweis:
Fall 1: $d_K \equiv 1 \pmod 4$

$$d_K = (-1)^{\varepsilon} p_1 \cdots p_r$$

$p_j > 2$ und verschieden.

$\varepsilon = 0{,}1$, $\varepsilon \equiv$ (Anzahl der $p_i \equiv 3 \pmod 4$) $\pmod 2$

$\chi_K = \left(\frac{\cdot}{p_1}\right) \cdots \left(\frac{\cdot}{p_r}\right)$

$$G(\chi_K) = G(\left(\frac{\cdot}{p_1}\right)) \cdots G(\left(\frac{\cdot}{p_r}\right)) \cdot \prod_{i \neq j} \left(\frac{p_i}{p_j}\right)$$

Sei $\alpha =$ Anzahl der $p_j \equiv 3 \pmod 4$

$$\left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right) = \begin{cases} -1 & p_i \equiv p_j \equiv 3 \pmod 4 \\ 1 & \text{sonst} \end{cases}$$

$$G(\chi_K) = i^{\alpha}\sqrt{p_1 \cdots p_r}(-1)^{\frac{\alpha(\alpha-1)}{2}} = i^{\alpha^2}\sqrt{p_1 \cdots p_r}$$

Ist $d_K > 0$, so ist $\varepsilon = 0$, also α gerade, $\alpha^2 + G$ durch 4, $\Rightarrow$

$$G(\chi_K) = \sqrt{p_1 \cdots p_r} = \sqrt{d_K}$$

Ist $d_K < 0$, so ist $\varepsilon = 1$, α ungerade, $\alpha^2 \equiv 1 \pmod 4 \Rightarrow G(\chi_K) = i\sqrt{|d_K|}$

Fall 2: $d_K \equiv 0 \pmod 4 \Rightarrow$ so ähnlich. ∎

4.5 Die Klassenzahlformeln

Zur Erinnerung. Satz 10 todo: link finden:

$$L(1, \chi_K) = \frac{2\pi}{w\sqrt{|d_K|}} h_K \qquad d_K < 0$$

$$L(1, \chi_K) = \frac{2 \log \varepsilon_K}{\sqrt{|d_K|}} h_K \qquad d_K > 0$$

$$L(1, \chi_K) = \frac{1}{m} \sum_{a=1}^{m-1} G(a, \chi_K)(-\log)(2 \sin \frac{\pi a}{m}) - i(\frac{\pi}{2} - \frac{\pi a}{m})$$

$m = |d_K|$ sowie

$$G(a, \chi_K) = \chi_K(a) G(\chi_K), G(\chi_K) = \begin{cases} \sqrt{|d_K|} \\ i\sqrt{|d_K|} \end{cases}$$

Sei $d_K > 0$

$$L(1, \chi_K) = \frac{1}{d_K} \sqrt{d_K} \sum_{(a, d_K)=1} \chi_K(a)(-\log 2\pi \frac{a}{d_K})$$

wegen $L(1, \chi_K) \in \mathbb{R}$

$\Rightarrow$

$$h_K = -\frac{1}{2 \log \varepsilon_K} \sum_{(a, d_K)=1} \chi_K(a) \frac{2\pi a}{d_K}$$

Da $\sum_a \chi_K(a) = 0$, kann man die 2 weglassen.

$\chi_K(-a) = \chi_K(-1)\chi_K(a)$, $\chi_K(-1) = 1$ für K reellquadratisch

$$\log(\sin \frac{\pi(d_K - a)}{d_K}) = \log(\sin \frac{\pi a}{d_K})$$

Satz 4.3 (Klassenzahlformel für reellquadratische Zahlkörper)

$$h_K = -\frac{1}{\log \varepsilon_K} \sum_{0<a<\frac{d_K}{2}} \chi_K(a) \log \sin \frac{\pi a}{d_K}$$

Folgerung 4.12
Für $a, b \in (0, \frac{1}{2} d_K)$ mit $\chi_K(a) = +1, \chi_K(b) = -1$ sei

$$\eta = \frac{\prod_b \sin \frac{\pi b}{d_K}}{\prod_a \sin \frac{\pi a}{d_K}}$$

Dann folgt $\varepsilon_K^{h_K} = \eta =$ Einheit im O_K, $\eta > 1$.

Sei nun $d_K < 0$

$$\frac{2\pi}{w\sqrt{|d_K|}} h_K = \frac{\sqrt{d_K}}{|d_K|} \sum_{a \mod |d_K|} \chi_K(a)\Big(\frac{\pi}{2} - \frac{\pi a}{|d_K|}\Big)$$

$$\Rightarrow h_K = -\frac{w}{2|d_K|} \sum_{a \mod |d_K|} \chi_K(a) \cdot a$$

Sei $d_K \leftarrow 4 \Rightarrow$

$$h_K = -\frac{1}{|d_K|} \sum_{a \mod |d_K|} \chi_K(a) \cdot a$$

Satz 4.4 (Klassenzahlformel für imaginärquadratische Zahlkörper)
Sei K imaginärquadratisch, $d_K < -4$

$$h_K = \frac{1}{2 - \chi_K(2)} \sum_{0<a<\frac{|d_K|}{2}} \chi_K(a)$$

Beispiel 4.3
Sei $d_K = -43$, dann ist $\chi_K = \left(\frac{\cdot}{43}\right)$. Da $-43 \equiv 5 \pmod 8$ folgt $\chi_K(2) = -1$. Also $h_K = \frac{1}{3}(R - N)$ wobei R die Anzahl der Quadrate in [1,21] und N die Anzahl der Nichtquadrate in [1,21] ist.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$(\frac{x}{43})$	1	−1	−1	1	−1	1	−1	−1	1	1	1	−1	1	1	1	1	1	−1	−1	−1	1

damit ergibt sich $R = 12$ und $N = 9$ also ist $h_K = \frac{12-9}{3} = 1$.

todo: Hier fehlt der Anfang

Sei nun d_K gerade. Zuerst zeigen wir $\chi(a + \frac{m}{2}) = -\chi(a)$.

$(a+\frac{m}{2})(b+\frac{m}{2}) = ab+(a+b)\frac{m}{2}+\frac{m^2}{4}$, a, b ungerade $\Rightarrow a+b$ gerade $\Rightarrow (a+\frac{m}{2})(b+\frac{m}{2}) \equiv ab \pmod m$, man beachte noch, dass d_K durch 4 teilbar ist.

$\Rightarrow \chi(a + \frac{m}{2})\chi(b + \frac{m}{2}) = \chi(a)\chi(b) \Rightarrow \chi(a)\chi(a + \frac{m}{2}) = \chi(b)\chi(b + \frac{m}{2})$. Das gilt für alle $a, b \mod {}^*m$, also prim zu m, d. h. $\chi(a + \frac{m}{2}) = c\chi(a)$ mit $c = \pm 1$ unabhängig von a.

Nachgereicht wird: χ_K nicht periodisch modulo $\frac{m}{2}$.

Also ist $c = -1$ und $\chi(a + \frac{m}{2}) = -\chi(a)$.

$$\begin{aligned} hm &= -\sum_{0<a<\frac{m}{2}} \chi(a)a - \sum_{0<a<\frac{m}{2}} \chi(a + \frac{m}{2})(a + \frac{m}{2}) \\ &= -\sum_{0<a<\frac{m}{2}} \chi(a)a + \sum_{0<a<\frac{m}{2}} \chi(a)a + \frac{m}{2} \sum_{0<a<\frac{m}{2}} \chi(a) \\ \Rightarrow h &= \frac{1}{2} \sum_{0<a<\frac{m}{2}} \chi(a) \end{aligned}$$

d_K gerade $\Rightarrow \chi_K(2) = 0$

Beispiel 4.4
$D = -23$, $K = \mathbb{Q}(\sqrt{-23}), d_K = -23$, $\chi_K(2) = 1$, da d_K ungerade

$$\begin{aligned} h_K &= \frac{1}{2 - \chi_K(2)} \sum_{0<a<12} \left(\frac{a}{23}\right) \\ &= 1 + 1 + 1 + 1 - 1 + 1 - 1 + 1 + 1 - 1 - 1 = 7 - 4 = 3 \end{aligned}$$

Die Klassenzahl von $\mathbb{Q}(\sqrt{-23})$ ist 3.

4.5.1 Nachtrag 1: Gebrochene Ideale

K/Q quardatisch, $\lambda \in K^*$, dann ist $(\lambda) = \lambda O_K$ fast ein Ideal: additive Untergruppe und Multiplikation aus O_K führen nicht aus O_K heraus. Außerdem existiert $\mu \in K^*$, sogar aus $O_K \supset 0$, so dass $\mu(\lambda) \subset O_K$.

Definition 4.3
Eine additive Untergruppe $\mathfrak{p} \subset K$ heißt **gebrochenes Ideal** :$\Leftrightarrow$

1. $\mathfrak{p}$ ist O_K-Modul: $O_K \cdot \mathfrak{p} \subset \mathfrak{p}$ und
2. $\exists \mu \in K^* \colon \mu(\mathfrak{p}) \subset O_K$

Beispiel 4.5
1. Ideale
2. gebrochene Hauptideale $(\lambda) = \lambda O_K$, $\lambda \in K^*$
3. Ist $\mathfrak{p} \subset O_K$ Ideal, so ist $\lambda\mathfrak{p}$, $\mathfrak{p} \in K^*$ gebrochenes Ideal
4. K^* ist kein gebrochenes Ideal

Definition 4.4
$\mathfrak{a}, \mathfrak{b}$ gebrochene Ideale

$$\mathfrak{a} \cdot \mathfrak{b} = \{a_1 b_1 + \cdots + a_r b_r \colon a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Bemerkung 4.8
Das ist wieder ein gebrochenes Ideal: $\lambda\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$ für $\lambda \in O_K$ ist klar.

$\alpha\mathfrak{a} \subset O_K$ und $\beta\mathfrak{b} \subset O_K \Rightarrow \alpha\beta(\mathfrak{a} \cdot \mathfrak{b}) \subset O_K$

Übungsaufgabe:

1. $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$
2. $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$

Definition 4.5
Sei $\mathfrak{a} \subset O_K$ ein Ideal, dann sei

$$\mathfrak{a}^{-1} := \{\alpha \in K \colon \alpha\mathfrak{a} \subset O_K\}$$

Fakt 4.10
1. $\mathfrak{a}^{-1}$ ist gebrochenes Ideal
2. $O_K \subset \mathfrak{a}^{-1}$, $(\mathfrak{a}^{-1} \colon O_K)$ todo: hier fehlt was

Beweis:
1. folgt aus (3)

2. $O_K \subset \mathfrak{a}^{-1}$ ist klar,

$$\begin{aligned}(\mathfrak{a}^{-1} : O_K) &= (\frac{1}{\mathbb{N}\mathfrak{a}}\mathfrak{a}' : O_K) \\ &= (\mathfrak{a}' : \mathbb{N}\mathfrak{a} \cdot O_K) \\ &= (O_K : \mathbb{N}\mathfrak{a}O_K)/(O_K : \mathfrak{a}') \\ &= (\mathbb{N}\mathfrak{a})^2/\mathbb{N}\mathfrak{a} = \mathbb{N}\mathfrak{a}\end{aligned}$$

3. Sei $\alpha \in \mathfrak{a}^{-1} \Rightarrow \alpha\mathfrak{a} \subset O_K \Rightarrow \alpha\mathfrak{a}\mathfrak{a}' \subset \mathfrak{a}' \subset O_K$.

   $\mathfrak{a}\mathfrak{a}' = (\mathbb{N}\mathfrak{a}) = \mathbb{N}\mathfrak{a}O_K$. Somit $\alpha \cdot \mathbb{N}\mathfrak{a} \in O_K$, $\alpha \in \frac{1}{\mathbb{N}\mathfrak{a}}\mathfrak{a}'$

   Sei $\alpha = \frac{1}{\mathbb{N}\mathfrak{a}}\beta$, $\beta \in \mathfrak{a}' \Rightarrow \alpha\mathfrak{a} = \frac{1}{\mathbb{N}\mathfrak{a}}\beta\mathfrak{a}$, $\beta\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a} = \mathbb{N}\mathfrak{a} \cdot O_K \Rightarrow \alpha\mathfrak{a} \subset O_K$

4. $\mathfrak{a} \cdot \mathfrak{a}' = \frac{1}{\mathbb{N}\mathfrak{a}}\mathfrak{a} \cdot \mathfrak{a}' = \frac{1}{\mathbb{N}\mathfrak{a}}(\mathbb{N}\mathfrak{a}) = O_K$ ∎

Fakt 4.11
Jedes gebrochene Ideal besitzt eine eindeutige Darstellung als Produkt von ganzahligen Potenzen von Primidealen. Mit anderen Worten: Die Gruppe der gebrochenen Ideal ist eine freie abelsche Gruppe über der Menge der Primideale.

Beweis:
Sei $\mathfrak{a}$ gebrochen, $\lambda \in O_K, \lambda \neq 0$, so dass $\lambda\mathfrak{a} \subset O_K \Rightarrow (\lambda)\mathfrak{a} = \mathfrak{b}$ ist übliches Ideal. Dann folgt für $\mathfrak{c} = (\lambda) \cdot \mathfrak{b}^{-1}$, dass $\mathfrak{a}\mathfrak{c} = \mathfrak{a} \cdot (\lambda) \cdot \mathfrak{b}^{-1} = \mathfrak{b} \cdot \mathfrak{b}^{-1} = O_K$. Daraus folgt, dass $\mathfrak{a}$ eine Inverses besitzt und damit bilden Id_K eine abelsche Gruppe.

$(\lambda)\mathfrak{a} = \mathfrak{b}$ wie oben. (λ) und $\mathfrak{b}$ haben eine Zerlegung in Primideal $\Rightarrow \mathfrak{a} = (\lambda)^{-1}\mathfrak{b}$ ebenfalls.

Zeigen wir die Eindeutigkeit:

$$\begin{gathered}\mathfrak{a} = \prod \mathfrak{p}_i^{m_i} = \prod \mathfrak{q}_j^{n_j}, m_i, n_j \in \mathbb{Z} \\ \Rightarrow \prod_{m_j>0} \mathfrak{p}_i^{m_i} \cdot \prod_{n_j<0} \mathfrak{q}_j^{-n_j} = \prod_{m_j<0} \mathfrak{p}_i^{-m_i} \cdot \prod_{n_j>0} \mathfrak{q}_j^{n_j}\end{gathered}$$

$\Rightarrow \mathfrak{p}_i = \mathfrak{q}_j, m_i = n_j$. ∎

Fakt 4.12
Der kannonische Homomorphismus $K^* \to Id_K : \lambda \mapsto (\lambda)$ besitzt als Kern die Einheitengruppe O_K^* und als Cokern Cl_K. Mit anderen Worten: $Cl_K = {}^{Id_K}/_{\text{gebr. HI}}$

Beweis:
$(\lambda) = O_K \Rightarrow \lambda \in O_K, 1 \in O_K \Rightarrow 1 = \lambda\mu$ mit $\mu \in O_K \Rightarrow \lambda$ ist Einheit.

Für λ Einheit ist $(\lambda) = O_K$ klar.

Aus $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ folgt $\mathfrak{a} = (\beta/\alpha)\mathfrak{b} \Rightarrow$ liegen in derselben Klasse in ${}^{Id_K}/_{(HI)}$. Also $\mathfrak{a}, \mathfrak{b}$ in derselben Klasse in der alten $Cl_K \Rightarrow$ in derselben in der neuen

$Cl_K \to {}^{Id_K}/_{HI}$ durch $\mathfrak{a} \mapsto \mathfrak{a}$. Wir zeigen: Das ist ein Isomorphismus.

Sei $\mathfrak{a} \subset O_K$ Ideal und $\mathfrak{a} = (\lambda), \lambda \in K^*$. Dann ist $\lambda \in O_K$ also $\mathfrak{a} = (\lambda) \cdot O_K \Rightarrow \mathfrak{a} \sim O_K$ ind Cl_K.

Surjektivität: Für jedes gebrochene Ideal $\mathfrak{a}$ existiert $\lambda \in K^*$, so dass $(\lambda)\mathfrak{a} \subset O_K$, also $\lambda\mathfrak{a}$ übliches Ideal ist. Das folgt aus der Defeinition von gebrochenen Idealen. ∎

Bemerkung 4.9
Wir hatten Cl_K so konstruiert: $\mathfrak{a}, \mathfrak{b} \subset O_K, \mathfrak{a} \sim \mathfrak{b} := \exists \alpha, \beta \in O_K, \alpha \neq 0 \neq \beta$, so dass $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

Die Äquivalenzklassen bilden die Gruppe Cl_K.

Index