Protokoll der Vorlesung über Quadratische Zahlkörper, SS 2001

Diese Vorlesung verstand sich als kurze Einführung zu einem Seminar (im Juni/Juli 2001) über Zagiers Buch *Zetafunktionen und quadratische Zahlkörper*, Springer Hochschultext (1981) [Stellnummer in der UBA : SK 180 Z 18]. Vorausgesetzt wurden gute Kenntnisse in Linearer Algebra, keine aus der Algebra.

Protokoll der 1. Sitzung

Ein quadratischer Zahlkörper K ist ein den Körper $\mathbb{Q}$ der rationalen Zahlen enthaltender Körper, der, aufgefaßt als Vektorraum über $\mathbb{Q}$, die Dimension 2 hat.

Ist $\alpha \in K \setminus \mathbb{Q}$, so sind $1, \alpha$ linear unabhängig, $1, \alpha, \alpha^2$ jedoch linear abhängig. Es resultiert die Existenz eines eindeutig bestimmten, normierten, quadratischen Polynoms

$$f_\alpha(x) = x^2 + ax + b\,,\ a, b \in \mathbb{Q}$$

mit Nullstelle α. Aus Dimensionsgründen folgt unmittelbar, daß $K = \mathbb{Q}(\alpha) \stackrel{\text{def}}{=} \{s + t\alpha : s, t \in \mathbb{Q}\}$, und weiter, daß $K = \mathbb{Q}(\sqrt{d'})$ mit $d' = a^2 - 4b$, der Diskriminante von f_α, gilt. Schreibt man die rationale Zahl $d' = \frac{z}{n}$ als Bruch ganzer Zahlen und erweitert mit n, so ergibt sich

SATZ. *Die quadratischen Zahlkörper sind genau die Körper $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ ohne quadratische Teiler. Diese Parametrisierung ist eindeutig.*

Insbesondere können alle K als Teilkörper des komplexen Zahlkörpers $\mathbb{C}$ aufgefaßt werden.

DEFINITION. $G = G(K/\mathbb{Q}) = \mathrm{Aut}(K)$ *ist die Gruppe aller Körperautomorphismen von K.*

Ist $\tau \in G$, so gilt $\tau(s) = s$ für $s \in \mathbb{Q}$ und, für $\alpha \in K \setminus \mathbb{Q}$, $\tau(\alpha) = \alpha$ oder $= \alpha'$, je nachdem ob $\tau = 1$ oder $\neq 1$ ist; α' ist die zweite Wurzel von $f_\alpha(x)$. Insbesondere ist G die Gruppe der Ordnung 2; wir bezeichnen fortan mit σ ihr nichttriviales Element, also, wenn $K = \mathbb{Q}(\sqrt{d})$, $\sigma(s + t\sqrt{d}) = \sigma(s - t\sqrt{d})$. Wenn also $\alpha \in K \setminus \mathbb{Q}$, so sind α und $\sigma(\alpha)$ die beiden Wurzeln von $f_\alpha(x)$. Wir setzen, in obiger Notation,

$$\mathrm{tr}\,(\alpha) \stackrel{\text{def}}{=} \alpha + \sigma(\alpha) = -b\ ,\ \mathrm{norm}(\alpha) \stackrel{\text{def}}{=} \alpha \cdot \sigma(\alpha) = c\,.$$

$\mathrm{tr}\,(\alpha)$ und $\mathrm{norm}(\alpha)$ heißen die Spur beziehungsweise Norm von α. In diesen Definitionen darf α auch rational sein – es gibt dann allerdings weder b noch c: $\mathrm{tr}\,(\alpha) = 2\alpha$, $\mathrm{norm}(\alpha) = \alpha^2$.

LEMMA. tr *ist eine $\mathbb{Q}$-Linearform;* norm *ist multipilkativ und "*$\mathrm{norm}(\alpha) = 0 \iff \alpha = 0$*".*

Im Falle, daß $\alpha \in \mathbb{Q}$, setzen wir einfach $f_\alpha(x) = x - \alpha$.

DEFINITION. *Ein $\alpha \in K$ heiße ganz, falls $f_\alpha(x)$ ganzzahlige Koeffizienten hat. Die Menge aller in K ganzen Elemente wird mit $\mathfrak{o}$ bezeichnet.*

$\alpha \in \mathbb{Q}$ ist also ganz, falls $\alpha \in \mathbb{Z}$, d.h. $\mathfrak{o} \cap \mathbb{Q} = \mathbb{Z}$; $\alpha \in K \setminus \mathbb{Q}$ ist ganz, falls $b, c \in \mathbb{Z}$.

SATZ. *Sei* $K = \mathbb{Q}(\sqrt{d})$. *Ist* $d \equiv 2, 3 \bmod 4$, *so gilt* $\mathfrak{o} = \mathbb{Z}[\sqrt{d}] \stackrel{\text{def}}{=} \{s + t\sqrt{d} : s, t \in \mathbb{Z}\}$; *ist* $d \equiv 1 \bmod 4$, *so ist* $\mathfrak{o} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. *Insbesondere ist* $\mathfrak{o}$ *ein Ring.*

Beachte, daß $\mathfrak{o}$ als $\mathbb{Z}$-Modul frei mit einer zweielementigen Basis ist; beachte auch, daß $\mathfrak{o}$ stabil unter G ist. Beachte schließlich, daß tr und norm den Ring $\mathfrak{o}$ nach $\mathbb{Z}$ abbilden.

Protokoll der 2. Sitzung

DEFINITION. *Ein Ideal* $\mathfrak{a}$ *in* $\mathfrak{o}$ *ist der Kern eines nicht-injektiven Ringhomomorphismus* $\varphi : \mathfrak{o} \to R$, R *ein Ring.*

Also $\mathfrak{a} = \ker \varphi = \{\alpha \in \mathfrak{o} : \varphi(\alpha) = 0\}$. Es folgt, daß $\mathfrak{a}$ abgeschlossen unter $\pm$ ist und daß darüber hinaus "$\gamma \in \mathfrak{o}$, $\alpha \in \mathfrak{a} \Longrightarrow \gamma\alpha \in \mathfrak{o}$" gilt. Umgekehrt ist jede Teilmene $\{0\} \neq \mathfrak{a} \subset \mathfrak{o}$, die diese Eigenschaften hat, ein Ideal: Definiere dazu auf $\mathfrak{o}$ eine neue Gleichheit durch

$$\gamma_1 \equiv \gamma_2 \iff \gamma_1 - \gamma_2 \in \mathfrak{a}$$

und rechne nach, daß diese reflexiv, symmetrisch, transitiv und verträglich mit $+$ und $\cdot$ ist. Die neuen Gleichheitsklassen $\overline{\gamma}$ bilden deshalb einen Ring $R = \mathfrak{o}/\mathfrak{a}$ und $\varphi : \mathfrak{o} \to \mathfrak{o}/\mathfrak{a}$, $\gamma \mapsto \overline{\gamma}$ ist ein Homomorphismus mit Kern $\mathfrak{a}$.

LEMMA. $\mathfrak{a} \cap \mathbb{Z} = \mathbb{Z} \cdot a$ *mit einem* $0 \neq a \in \mathbb{N}$; $\quad \mathfrak{a} \neq \mathfrak{o} \Longrightarrow a \neq 1$.

Denn $\mathrm{norm}(\alpha) \in \mathfrak{a} \cap \mathbb{Z}$, falls $\alpha \in \mathfrak{a}$.

LEMMA. $\mathfrak{o}/\mathfrak{a}$ *ist endlich. Insbesondere ist* $\mathfrak{a}$ *ein freier* $\mathbb{Z}$*-Modul mit einer zweielementigen Basis.*

Ersteres resultiert aus der Endlichkeit von $\mathbb{Z}/a$. Für die zweite Behauptung projiziere $\mathfrak{o} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ auf die erste Komponente und erhalte einen additiven Homomorphismus von $\mathfrak{a}$ nach $\mathbb{Z}\omega_1$ mit Kern $\mathfrak{a} \cap \mathbb{Z}\omega_2 \simeq \mathbb{Z}$ und Bild $\simeq \mathbb{Z}$.

Beachte die Folgerung: Jedes Ideal hat höchstens zwei Erzeugende, d.h. $\exists\, \alpha_1, \alpha_2 \in \mathfrak{a} : \mathfrak{a} = \mathfrak{o}\alpha_1 + \mathfrak{o}\alpha_2$.

DEFINITION. $\mathrm{norm}(\mathfrak{a}) = |\mathfrak{o}/\mathfrak{a}|$.

Das Ideal $\mathfrak{a}$ heißt Primideal, falls $\mathfrak{o}/\mathfrak{a}$ nullteilerfrei ist. Maximale Ideale, also solche $\mathfrak{a}$ mit "$\mathfrak{o}/\mathfrak{a}$ ist ein Körper", sind Primideale.

SATZ. *Jedes Primideal ist maximal. Jedes Ideal ist eindeutig als (endliches) Produkt von Primidealen darstellbar.*

Dieser Satz ist eine Art Analogon zum Satz von der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$.

In seinen Beweis geht folgende Definition ein

$$\mathfrak{a}^{-1} \stackrel{\text{def}}{=} \{\kappa \in K : \kappa\mathfrak{a} \subset \mathfrak{o}\},$$

und die Hauptbeoachtung ist die, daß

$$\mathfrak{p}^{-1} \supsetneq \mathfrak{o}, \quad \mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{o}$$

für Primideale $\mathfrak{p}$ gilt. Deren Beweis fließt im wesentlichen aus dem

LEMMA. *Ist $\mathfrak{a}$ ein Ideal und $\kappa \in K$ so, daß $\kappa \cdot \mathfrak{a} \subset \mathfrak{a}$, dann ist κ ganz, also $\in \mathfrak{o}$.*

Es ist nämlich κ Eigenwert des $\mathbb{Q}$-Endomorphismus $\gamma \mapsto \kappa\gamma$ von K, den man bezüglich einer $\mathbb{Z}$-Basis von $\mathfrak{a}$ betrachtet. Die charakteristische Gleichung hat Koeffizienten aus $\mathbb{Z}$ und ist $= f_\kappa(x)$ (für $\kappa \notin \mathbb{Q}$).

Protokoll der 3. Sitzung

Wir beobachten, daß die *gebrochenen Ideale von K*, also die $\mathfrak{a}\cdot\mathfrak{b}^{-1}$, genau die endlich erzeugten $\mathfrak{o}$-Teilmoduln $\neq 0$ von K sind. Diese alle zusammen bilden eine freie abelsche Gruppe, I_K, mit den Primidealen in $\mathfrak{o}$ als freien Erzeugenden (das Einselement wird von $\mathfrak{o}$ selbst repräsentiert).

DEFINITION. *Die Idealklassengruppe $\mathrm{cl} = \mathrm{cl}_K$ von K ist der Quotient I_K/P_K, wobei P_K die Untergruppe der gebrochenen Haupideale von K bezeichnet:* $P_K = \langle \mathfrak{o} \cdot \kappa : 0 \neq \kappa \in K \rangle$.

SATZ. cl *ist endlich. Die Ordnung* $|\mathrm{cl}|$ *heißt die Klassenzahl $h = h_K$ von K.*

Der Satz resultiert aus Eigenschaften der Idealnorm (siehe das Lemma weiter unten) und aus der Beobachtung, daß es eine nur von K abhängige Schranke $c \in \mathbb{N}$ gibt, so daß in jeder Klasse $\overline{\mathfrak{a}} \in \mathrm{cl}$ ein $\mathfrak{a}' \subset \mathfrak{o}$ mit $\mathrm{norm}(\mathfrak{a}') \leq c$ existiert. Über die tatsächliche Größe von h sagt er wenig. Tatsächlich bestehen nach wie vor Kenntnislücken über die Klassenzahlen und, mehr noch, über die Gruppenstruktur und G-Struktur von cl: beachte, daß cl eine G-stabile Gruppe ist. So ist z.B. nicht bekannt, ob es unendlich viele positive d mit $h_{\mathbb{Q}(\sqrt{d})} = 1$ gibt; vergleiche dazu auch den letzten SATZ in diesem Kapitel [1].

Wir wollen für jetzt nur das folgende Ergebnis zitieren (in dem p eine ganzrationale Primzahl ist); sehr viel schärfere werden bei der Lektüre des Zagierschen Buches ersichtlich.

SATZ. $h = 1 \iff [\forall\, p \in \mathbb{Z} :$ *entweder p ist prim in $\mathfrak{o}$ oder p oder $-p$ ist Norm aus $\mathfrak{o}$*$]$.

Der Beweis benutzt das Kriterium

$$h = 1 \iff [\,\text{unzerlegbar} = \text{prim}\,] .$$

Dabei heißt $\gamma \in \mathfrak{o}$ unzerlegbar, beziehungsweise prim, wenn $\gamma \nmid 1$ und γ kein echtes Produkt $\gamma = \gamma_1\gamma_2\,, \gamma_j \nmid 1$ ist, beziehungsweise $[\,\gamma|\gamma_1\gamma_2 \Longrightarrow \gamma|\gamma_1$ oder $\gamma|\gamma_2\,]$ erfüllt $(\gamma_1, \gamma_2 \in \mathfrak{o})$.

Mit h ist ein erstes (endliches) Hindernis zum gewohnten Rechnen in $\mathbb{Z}$ enstanden; ein zweites folgt aus der Größe der Einheitengruppe $\mathfrak{o}^\times$, die immer dann unendlich ist, wenn $d > 0$. Dazu kommen wir später. Hier folgt zunächst das oben angekündigte

LEMMA. $\mathrm{norm}(\mathfrak{ab}) = \mathrm{norm}(\mathfrak{a})\mathrm{norm}(\mathfrak{b})\,; \quad \mathrm{norm}(\mathfrak{o}\alpha) = |\mathrm{norm}(\alpha)|$.

Die erste Behauptung kann man zufolge des

CHINESISCHEN RESTSATZES: *sind $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremde Ideale von $\mathfrak{o}$ und α_1, α_2 beliebige Elemente in $\mathfrak{o}$, so existiert ein $\gamma \in \mathfrak{o}$ mit* $\gamma \equiv \alpha_1 \bmod \mathfrak{a}_1\,,\ \gamma \equiv \alpha_2 \bmod \mathfrak{a}_2$

auf Potenzen $\mathfrak{a}$ und $\mathfrak{b}$ eines Primideales $\mathfrak{p}$ zurückführen. Ist $\mathfrak{p} = \mathfrak{o}\pi$ ein Hauptideal, so liefert die Multiplikation mit π Isomorphismen $\mathfrak{o}/\mathfrak{p}^j \simeq \mathfrak{p}^i/\mathfrak{p}^{i+j}$ $(i, j \in \mathbb{N})$ woraus die Behauptung

[1] SATZ (Stark). *Ist $d < 0$, so ist $h_{\mathbb{Q}(\sqrt{d})} = 1$ genau für $-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.*

unmittelbar resultiert. Den allgemeinen Fall führt man darauf durch Ersetzung von $\mathfrak{o}$ durch $\mathfrak{o}_{(\mathfrak{p})} \stackrel{\text{def}}{=} \{\gamma_1/\gamma_2 : \gamma_1 \in \mathfrak{o},\, \gamma_2 \in \mathfrak{o} \setminus \mathfrak{p}\} \subset K$ zurück, indem man $\mathfrak{o}/\mathfrak{p}^j \simeq \mathfrak{o}_{(\mathfrak{p})}/\mathfrak{p}^j\mathfrak{o}_{(\mathfrak{p})}$ beweist. – Die zweite Behauptung sieht man so. $|\mathfrak{o}/\mathfrak{o}\alpha|$ ist die Größe des Kokerns $\operatorname{coker} m_\alpha \stackrel{\text{def}}{=} \mathfrak{o}/\operatorname{im}(m_\alpha)$ der Abbildung $m_\alpha : \mathfrak{o} \to \mathfrak{o}$, $\gamma \mapsto \gamma\alpha$, die wir uns als $\mathbb{Z}$-lineare Abbildung des freien $\mathbb{Z}$-Moduls $\mathfrak{o}$ vom Rang 2 in sich vorstellen. Die adjungierte Abbildung $\tilde{m}_\alpha$ besitzt eine Matrix, die durch Vertauschungen, Transponieren und Multiplikationen mit $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ und $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ aus der von m_α hervorgeht. Da $\mathfrak{o}\alpha$ wieder frei vom Rang 2 ist, folgt $|\mathfrak{o}/\mathfrak{o}\alpha| = |\mathfrak{o}\mathfrak{a}/\tilde{m}_\alpha(\mathfrak{o}\alpha)|$ und daraus $|\mathfrak{o}/\mathfrak{o}\alpha| = |\det m_\alpha|$. Andererseits ist $1, \alpha$ eine Basis von $K/\mathbb{Q}$ (vorausgesetzt, daß $\alpha \notin \mathbb{Q}$), also gehört zu m_α die Matrix $\begin{pmatrix} 0 & -\operatorname{norm}(\alpha) \\ 1 & \operatorname{tr}\alpha \end{pmatrix}$ mit Determinante $\operatorname{norm}(\alpha)$.

Bemerkung. Für jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}$ kann man eine *Bewertung* $w_\mathfrak{p}$ auf K so definieren: $w_\mathfrak{p}(\alpha) = z \in \mathbb{Z} \cup \{\infty\} \iff \alpha \in \mathfrak{p}^z \setminus \mathfrak{p}^{z+1}$. Setzt man noch $|\alpha|_\mathfrak{p} \stackrel{\text{def}}{=} p^{-w_\mathfrak{p}(\alpha)}$, für die Primzahl $p \in \mathfrak{p}$, so erhält man eine Betragsfunktion, die alle gewohnten Gesetze des komplexen Betrages erfüllt. Insbesondere kann man K bezüglich dieser komplettieren (d.h. die Grenzwerte der [neuen] Cauchyfolgen zu K hinzunehmen) und erhält ähnliche vollständige Körper $K_\mathfrak{p}$ (also mit schönen Konvergenzeigenschaften) wie $\mathbb{R}$ oder $\mathbb{C}$. Diese erlauben ein *lokales* Studium von K *an der Stelle* $\mathfrak{p}$ und sind wichtig für das Studium der Arithmetik von K. Wir wollen hier nicht weiter darauf eingehen, weisen aber wenigstens auf eine erstaunliche Topologieeigenschaft dieser Körper $K_\mathfrak{p}$ hin: eine Reihe $\sum_n \alpha_n$ konvergiert schon dann, wenn $\alpha_n \to 0$.

Protokoll der 4. Sitzung

Wir interessieren uns im weiteren zuerst für die Verzweigungstheorie in K, d.h. für die Produktzerlegung der Ideale $p\mathfrak{o}$, p Primzahl in $\mathbb{Z}$.

Satz. *Sei* $\mathfrak{o} = \mathbb{Z}[\omega]$ *(mit* $\omega = \sqrt{d}$ *oder* $= \frac{1+\sqrt{d}}{2}$*) und* $f_\omega(x)$ *die irreduzible quadratische Gleichung mit Wurzel* ω*. Ist* p *eine ganzrationale Primzahl, so bezeichnen wir mit* $f_\omega \bmod p$ *die aus* $f_\omega(x)$ *resultierende Gleichung, wenn man ihre Koeffizienten* $\bmod p$ *liest. Dann gilt:*

$p\mathfrak{o} = \mathfrak{p} \iff f_\omega \bmod p$ *ist irreduzibel über* $\mathbb{F}_p \stackrel{\text{def}}{=} \mathbb{Z}/p$*,*

$p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$ *mit* $\mathfrak{p}_1 \neq \mathfrak{p}_2 \iff f_\omega \bmod p$ *hat zwei verschiedene Wurzeln in* $\mathbb{F}_p$*,*

$p\mathfrak{o} = \mathfrak{p}^2 \iff f_\omega \bmod p$ *hat eine doppelte Wurzel in* $\mathbb{F}_p$*.*

Im ersten Fall heißt p *träge*, im zweiten Fall *zerlegt* (es gilt dann $\mathfrak{p}_2 = \sigma(\mathfrak{p}_1)$), im dritten Fall *verzweigt*.

Obiges Kriterium betrifft in Wiklichkeit die Diskriminante D von f_ω; beachte daß $D = 4d$ oder $D = d$, je nachdem ob $\omega = \sqrt{d}$ oder $= \frac{1+\sqrt{d}}{2}$ gilt. Das *Gaußsche quadratische Reziprozitätsgesetz*, das wir erst in der letzten Maiwoche (Kalenderwoche 22) beweisen wollen, liefert die Antwort für alle p auf einmal:

Satz. *Sei* $p \neq 2$*. Definiere für ein* $p \nmid z \in \mathbb{Z}$, $\left(\frac{z}{p}\right) = \begin{cases} 1 & z \bmod p \text{ ist Quadrat in } \mathbb{F}_p \\ -1 & \text{sonst} \quad . \end{cases}$

Dann gilt

$$\left(\frac{z_1 z_2}{p}\right) = \left(\frac{z_1}{p}\right)\left(\frac{z_2}{p}\right)$$

und

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

falls $q \neq p$ eine ungerade Primzahl ist.

BEMERKUNG. D wird auch die Diskriminante von $K = \mathbb{Q}(\sqrt{d})$ genannt. Offenbar gilt: *p verzweigt* $\iff$ $p \mid D$. Insbesondere ist die Anzahl der verzweigten p endlich. Mit dem Reziprozitätsgesetz können wir zwischen *träge* und *zerlegt* unterscheiden.

Eine (von fast unzählig vielen) Konsequenzen des Gaußschen quadratischen Reziprozitätsgesetzes ist der folgende schon füher angekündigte

SATZ. *Im Falle $d > 0$ liegt Klassenzahl 1 höchstens dann vor, wenn d prim oder von der Form $d = pq$ mit Primzahlen $p, q \not\equiv 1 \bmod 4$ ist.*

Unter einer (globalen) Einheit in K versteht man ein in $\mathfrak{o}$ invertierbares Element $\varepsilon \in \mathfrak{o}$. Offenbar sind dies genau die $\gamma \in \mathfrak{o}$ mit $\mathrm{norm}(\gamma) = \pm 1$. Deren Gesamtheit wird mit $E = E_K$ bezeichnet; E ist eine abelsche Gruppe. Eine Einheit ζ von endlicher Ordnung, also $\zeta^n = 1$ (für ein $n \geq 1$), wird als Einheitswurzel bezeichnet – und zwar als eine primitive n-te Einheitswurzel, falls obiges n minimal mit $\zeta^n = 1$ ist.

LEMMA. *Ist $d < 0$ so besteht E nur aus Einheitswuzeln. Diese sind, sofern $\neq 1$, primitiv für ein $n \leq 6$. Des weiteren ist E zyklisch und es gilt $\sigma(\zeta) = \zeta^{-1}$ außer für $\zeta = \pm 1$.*

Beachte, daß die Einheiten $\varepsilon = \frac{s+t\sqrt{D}}{2}$ genau den ganzzahligen Lösungen s, t der Pellschen Gleichung

$$s^2 - Dt^2 = \pm 4$$

entsprechen. (Die Koeffizientenbedingung für ε, nämlich $s \equiv t \bmod 2$ für $D = d$ und $2|s$ für $D = 4d$, ist bei jeder Lösung automatisch erfüllt.)

LEMMA. *Ist $d > 0$, so gibt es eine sogenannte Fundamental- oder Grundeinheit $\varepsilon_1 > 1$, so daß $E = \{\pm\varepsilon^z : z \in \mathbb{Z}\}$ gilt. Insbesondere ist $|E| = \infty$.*
Ist $\mathrm{norm}(\varepsilon_1) = 1$, so ist $\sigma(\varepsilon_1) = \varepsilon_1^{-1}$; ist $\mathrm{norm}(\varepsilon_1) = -1$, so ist $\sigma(\varepsilon_1) = -\varepsilon_1^{-1}$. Der letztere Fall erzwingt $[\, 2 \neq p \mid d \Longrightarrow p \equiv 1 \bmod 4\,]$.

Hier sind die wesentlichen Beweisschritte für den Fall, daß $\mathrm{norm}(\varepsilon) = -1$ unlösbar in E ist (der andere Fall wird in analoger Weise diskutiert).

1. Ist $\varepsilon \neq \pm 1$ eine Einheit, so ist von den vier Einheiten $\varepsilon, -\varepsilon, \overline{\varepsilon}, -\overline{\varepsilon}$ genau eine > 1. ($\overline{\varepsilon}$ ist kurz für $\sigma(\varepsilon)$.) Insbesondere folgt: $\varepsilon = x + y\sqrt{d} > 1 \iff x, y > 0$.

2. Es gibt ein $\varepsilon \neq \pm 1$. Das ist eine Konsequenz von Schubfachschlüssen. Zunächst gibt es zu jedem $\alpha \in \mathbb{R}_{>0}$ und jedem $1 < Q \in \mathbb{N}$ ganze Zahlen p, q mit $0 < q < Q$ und $|q\alpha - p| \leq \frac{1}{Q}$. Daraus folgt die Existenz unendlich vieler positiver ganzer Zahlen p, q mit $|p - q\sqrt{d}| \leq \frac{1}{q}$ und hieraus wiederum die Existenz unendlich vieler positiver ganzer Zahlen p, q mit

a. die $p - q\sqrt{d}$ haben alle gleiche Norm N

b. alle p sind untereinander kongruent modulo N, ebenso alle q.

Jeder Quotient aus solchen $p - q\sqrt{d}$ ist eine Einheit.

3. Die Grundeinheit ist nun $\min\{\varepsilon > 1 : \varepsilon \in E\}$.

Protokoll der 5. Sitzung

Hier folgt eine kurze Skizze vom Beweis des quadratischen Reziprozitätsgesetzes. Wohl erst in einer Algebravorlesung wird man verstehen, daß der Beweisansatz recht naheliegend ist, nämlich wenn man mit galoistheoretischem Werkzeug den quadratischen Teilkörper K in $\mathbb{Q}(\zeta_p)$ ausrechnet: $K = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$. Hier ist $p \geq 3$ eine Primzahl und ζ_p eine primitive p-te Einheitswurzel.

1. Es gibt ein $1 \leq w \leq p-1$ mit $\operatorname{ord}_p(w) = p-1$, i.e., $w^{p-1} \equiv 1 \bmod p$, $w^j \not\equiv 1 \bmod p$ für $1 \leq j \leq p-2$. Daraus resultiert insbesondere: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

2. Sind $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_i x^j$ zwei Polynome mit ganzrationalen Koeffizienten so, daß $\operatorname{ggT}(a_i : 0 \leq i \leq n) = 1 = \operatorname{ggT}(b_j : 0 \leq j \leq m)$, dann ist auch der größte gemeinsame Teiler der Koeffizienten des Produkts $f(x)g(x)$ gleich 1 (*Gaußsches Lemma*).

3. Das Polynom $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ ist irreduzibel über $\mathbb{Z}$ (*Eisenstein*).

4. Sei $\mathbb{Z}[\zeta_p] = \{\sum_{j=0}^{p-1} a_j \zeta_p^j : a_j \in \mathbb{Z}\} \subset \mathbb{C}$. Dies ist ein Ring mit $\mathbb{Z}$-Basis $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$. Insbesondere gilt: Sind $q, z \in \mathbb{Z}$ und gilt $q|z$ in $\mathbb{Z}[\zeta_p]$, so auch in $\mathbb{Z}$.

5. Setze $s = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right)\zeta_p^j \in \mathbb{Z}[\zeta_p]$. Dann gilt $s^2 = \left(\frac{-1}{p}\right)p$. Damit berechnet man für eine Primzahl $2 \neq q \neq p$

$$s^q \equiv \left(\frac{q}{p}\right) s \bmod q$$

und erhält das quadratische Reziprozitätsgesetz für ungerade Primzahlen.

6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ erhält man aus einem analogen Argument mittels $(1+i)^p$.