

Seminar über komplexe Multiplikation

---

Bielefeld 1979

Rudolf Scharlau

Vortrag 3

## Der "Erste Hauptsatz" : Ringklassenkörper

---

Im folgenden wird in Anlehnung an Deurings Artikel

[D] M. Deuring, Die Klassenkörper der komplexen Multiplikation, 1958,  
in: Enzyklopädie der mathematischen Wissenschaften,

der "Erste Hauptsatz" der komplexen Multiplikation bewiesen. Er besagt, daß die Ringklassenkörper zu einem imaginärquadratischen Körper  $k$  durch gewisse Zahlen  $j(\tau)$ ,  $\tau \in k$  über  $k$  erzeugt werden. Eine weitere klassische Referenz hierfür ist die Arbeit

[H] H. Hasse, Neue Begründung der komplexen Multiplikation.  
I. Einordnung in die allgemeine Klassenkörpertheorie.  
J. Reine Angew. Math. 157 (1927), 115-139.

Weitere Literatur:

[L-E] S. Lang, Elliptic Functions, 1973,

[B] Borel u.a., Seminar On Complex Multiplication,  
Springer Lecture Notes Nr. 21 .

In den Beweisen von Deuring und auch schon von Hasse scheint mir eine gewisse Unkorrektheit vorzuliegen. Ich sehe nicht, wie aus ihren Argumenten ohne weiteres folgt, daß der Ringklassenkörper schon von einem einzigen  $j(\tau)$  erzeugt wird. Siehe meinen Kommentar unten vor Satz 0.

Erster Hauptsatz. Es sei  $k$  imaginärquadratischer Zahlkörper,  $f$  eine positive ganze Zahl und  $\mathfrak{o}$  die Ordnung vom Index  $f$  in  $\mathfrak{o}_k$ , weiter  $\mathfrak{f} = f\mathfrak{o}_k$  der Führer von  $\mathfrak{o}$  und  $M$  ein zu  $\mathfrak{f}$  teilerfremdes (gebrochenes) Ideal von  $\mathfrak{o}$ , z.B.  $M = \mathfrak{o}$ . Es ist  $K := k(j(M))$  der Ringklassenkörper von  $\mathfrak{o}$  (oder  $\mathfrak{f}$ ). Das heißt: Sei

$$P_{\mathbb{Q}}(\mathfrak{f}) = \left\{ \frac{\alpha}{\beta} \mathfrak{o}_k \mid \begin{array}{l} \alpha, \beta \in \mathfrak{o}_k, \text{ ex. } a, b \in \mathbb{Z} \text{ mit} \\ \alpha \equiv a(\mathfrak{f}), \beta \equiv b(\mathfrak{f}), \\ (a, f) = (b, f) = 1 \end{array} \right\} .$$

$K$  ist der Klassenkörper zu der mod  $\mathfrak{f}$  erklärten Kongruenz-Idealgruppe  $P_{\mathbb{Q}}(\mathfrak{f})$  von  $k$ .

Erinnerung. i) Wenn  $\mathfrak{f}$  ein ganzes Ideal, allgemeiner ein Divisor eines Zahlkörpers  $k$  ist, so besteht der Strahl  $\text{mod } \mathfrak{f}$  aus denjenigen Hauptidealen von  $k$ , die von Elementen  $\equiv 1 \pmod{\mathfrak{f}}$  erzeugt werden. Eine  $\text{mod } \mathfrak{f}$  erklärte Kongruenz-Idealgruppe ist eine Untergruppe der Gruppe  $I(\mathfrak{f})$  der zu  $\mathfrak{f}$  teilerfremden Ideale, die  $P_{\mathfrak{f}}$  enthält.

ii) Seien  $I_0(\mathfrak{f}) \supseteq P_0(\mathfrak{f})$  die Gruppen der zu  $\mathfrak{f}$  teilerfremden  $\mathcal{O}$ -Moduln in  $k$  bzw. der von einem Element erzeugten zu  $\mathfrak{f}$  teilerfremden  $\mathcal{O}$ -Moduln. Vermöge  $M \mapsto \mathcal{O}_k M$  wird  $I_0(\mathfrak{f})$  isomorph auf  $I(\mathfrak{f})$  abgebildet, dabei wird  $P_0(\mathfrak{f})$  auf  $P_{\mathbb{Q}}(\mathfrak{f})$  abgebildet.  $I_0(\mathfrak{f})/P_0(\mathfrak{f}) \simeq I(\mathfrak{f})/P_{\mathbb{Q}}(\mathfrak{f})$  ist isomorph zu  $I_0/P_0$ , wobei  $I_0$  die Gruppe aller invertierbaren  $\mathcal{O}$ -Moduln ist und  $P_0 = \{\delta\mathcal{O} \mid \delta \in k^*\}$ .

iii) Definition. Sei  $k$  Zahlkörper,  $\mathfrak{f}$  Divisor,  $J$  Idealgruppe mit  $I(\mathfrak{f}) \supseteq J \supseteq P_{\mathfrak{f}}$  und  $K/k$  eine endliche Erweiterung.  $K$  heißt Klassenkörper zu  $J$  (und  $\mathfrak{f}$ ), wenn gilt:

- a)  $K/k$  ist galois'sch.
- b) Für jedes zu  $\mathfrak{f}$  teilerfremde Primideal  $\mathfrak{p}$  ersten Grades von  $k$  gilt:  $\mathfrak{p}$  zerfällt voll in  $K$  genau dann, wenn  $\mathfrak{p}$  in  $J$  liegt.

iv) Der Klassenkörper zu  $J$  existiert, ist eindeutig, seine Galoisgruppe über  $k$  isomorph zu  $I(\mathfrak{f})/J$ , insbesondere abelsch. Für die Situation des Ersten Hauptsatzes ist  $\text{Gal}(K/k)$  nach ii) also isomorph zur Modulklassengruppe  $I_0/P_0$ .

Wir werden zunächst beweisen, daß man den Ringklassenkörper durch Adjunktion sämtlicher Klasseninvarianten  $j(M)$  erhält. Hierzu benötigen wir aus der Klassenkörpertheorie lediglich den folgenden Satz 1, der ein Kriterium dafür ist, wann eine nicht als normal vorausgesetzte Erweiterung Klassenkörper ist. Über die Modulfunktion  $j$  werden nur die nicht sehr schwierigen unten zitierten Sätze 2 und 3 verwendet. Als nichttriviales zahlentheoretisches Hilfsmittel wird der Satz über die Existenz von Primidealen in "arithmetischen Progressionen", d.h. Nebenklassen von Kongruenz-Idealgruppen, verwendet.

Seien also  $M_1, \dots, M_h$  zu  $\mathfrak{f}$  teilerfremde Vertreter für die Klassen invertierbarer  $\mathcal{O}$ -Moduln und

$$L := k(j(M_1), \dots, j(M_h)) .$$

Wenn wir schon gezeigt haben, daß  $L$  Klassenkörper über  $k$  ist, so kann

man unter Verwendung von allgemeinen Ergebnissen der Klassenkörpertheorie sowie etwas mehr Information über die Zahlen  $j(M)$  schnell einsehen, daß  $L$  sogar von einem beliebigen einzelnen  $j(M)$  erzeugt wird, und hat dann den ersten Hauptsatz bewiesen.

Weil  $L/k$  abelsch ist, reicht es zu zeigen, daß alle  $j(M_\nu)$  konjugiert über  $k$  sind. Das erhält man sehr leicht mittels Satz 4, der es gestattet, den Isomorphismus

$$I_0(\mathfrak{f})/P_0(\mathfrak{f}) \longrightarrow \text{Gal}(L/k)$$

der Klassenkörpertheorie explizit anzugeben. Dabei wird übrigens wieder der Satz über Primideale in Progressionen verwendet.

Der unten gegebene Beweis dafür, daß  $L$  der Ringklassenkörper zu  $\mathfrak{o}$  ist, steht in Abschnitt 10 von [D]. Deuring gibt dort vor, zu zeigen, daß schon  $K$  der Ringklassenkörper ist (und dann natürlich gleich  $L$ ). Der letzte Absatz des Beweises auf S. 25 scheint mir aber nicht stichhaltig zu sein. Zunächst einmal sollte man von dem  $\mathfrak{p}$  dort lediglich voraussetzen, daß es wenigstens einen Faktor  $\mathfrak{P}$  ersten Grades in  $K$  enthält, mehr wird allerdings auch nicht verlangt. Die letzte Kongruenz bei Deuring macht zunächst nur Sinn im Körper  $L$ , wobei dann  $\mathfrak{P}$  durch ein darüberliegendes  $\mathfrak{P}'$  in  $L$  zu ersetzen ist. Solange aber noch nicht  $L$  wenigstens als normal über  $k$  erkannt ist, weiß man nicht, ob ein solches  $\mathfrak{P}'$  existiert, das auch vom Grad 1 ist.

Ich zitiere nun die beiden im folgenden benötigten allgemeinen zahlentheoretischen Sätze, zunächst den über die Primideale in "arithmetischen Progressionen".

Satz 0. Es sei  $k$  ein Zahlkörper,  $J$  eine Kongruenz-Idealgruppe von  $k$  und  $\mathfrak{a}J$  eine beliebige Nebenklasse von  $J$ . In  $\mathfrak{a}J$  liegen unendlich viele Primideale ersten Grades.

Jetzt das angekündigte Kriterium für Klassenkörper.

Satz 1. Es seien  $K/k$  Zahlkörper und  $J$  eine Kongruenz-Idealgruppe von  $k$ . Für fast alle zu einem Erklärungsmodul von  $J$  teilerfremden Primideale  $\mathfrak{p}$  ersten Grades von  $k$  gelte folgendes:

- a)  $p \in J \Rightarrow p$  zerfällt voll in  $K$ .  
 b)  $p$  hat in  $K$  einen Faktor ersten Grades  $\Rightarrow p \in J$ .

Dann ist  $K$  der Klassenkörper zu  $J$ .

Beweisskizze: Zu zeigen ist, daß  $K$  normal über  $k$  ist. Es werden die Standardtechniken für Dirichlet'sche Reihen verwendet, die dem Beweis des Dirichlet'schen Satzes über Primideale in einer Idealklasse (Satz 0) und der "zweiten Ungleichung" der Klassenkörpertheorie zugrundeliegen.

Sei für eine Erweiterung  $K/k$  von Zahlkörpern

$$\Omega_K = \left\{ P \mid \begin{array}{l} P \text{ unverzweigtes Primideal} \\ \text{ersten Grades von } K \end{array} \right\}$$

$$\Omega_{K/k} = \left\{ p \in \Omega_k \mid \begin{array}{l} p \text{ ist unverzweigt und} \\ \text{zerfällt voll in } K \end{array} \right\} .$$

Wir werden das folgende elementare Lemma verwenden.

Lemma 1. Für die normale Hülle  $\tilde{K}$  von  $K$  gilt  $\Omega_{\tilde{K}/k} = \Omega_{K/k}$ .

Für die  $\zeta$ -Funktion eines Zahlkörpers gilt für  $s > 1$

$$\log \zeta_k(s) \sim \sum_{p,m} m(Np^m)^{-s} \sim \sum_{p \in \Omega_k} Np^{-s} ,$$

wobei  $g \sim h$  bedeutet, daß  $\lim_{s \rightarrow 1+} (g(s) - h(s))$  existiert und endlich ist. Es konvergiert nämlich die Summe

$$\sum_{\substack{m \geq 2 \\ p}} mp^{-ms}$$

für  $s > \frac{1}{2}$ .

Seien nun  $J$  und  $K/k$  wie in Satz 1. Für fast alle unverzweigten  $P$  bzw.  $p$  gilt folgendes:

Wenn  $P \subseteq K$  vom Grad 1 ist, so ist  $p := P \cap k$  vom Grad 1, liegt also in  $J$  nach a). Nach b) zerfällt  $p$  in  $K$  in  $[K:k]$  verschiedene  $P = P_1, P_2, \dots \in \Omega_K$ . Umgekehrt führt ein vorgegebenes  $p \in \Omega_k \cap J$  zu  $[K:k]$  verschiedenen  $P \in \Omega_K$ . Also gilt

$$\log \zeta_K(s) \sim \sum_{P \in \Omega_K} NP^{-s} \sim [K:k] \sum_{p \in \Omega_k \cap J} Np^{-s}$$

Mittels des Lemmas 1 zeigt man das gleiche für  $\tilde{K}$ . Es folgt

$$\frac{1}{[K:k]} \zeta_K(s) \sim \frac{1}{[\tilde{K}:k]} \zeta_{\tilde{K}}(s).$$

Es ist aber  $\zeta_E(s) \sim -\log(s-1)$  für jeden Zahlkörper  $E$ , also notwendig  $[K:k] = [\tilde{K}:k]$ .

Es sei  $s$  eine positive ganze Zahl und  $S_1, \dots, S_d$  ein Vertretersystem für die ganzzahligen primitiven Matrizen der Determinante  $s$  bezüglich der Operation der  $SL_2 \mathbb{Z}$  durch Linksmultiplikation. Definiere

$$J_s(X, j) := \prod_{v=1}^d (X - j \circ S_v).$$

Die beiden folgenden Sätze findet man in [D], Seite 10, oder [L-E], Seite 55 bzw. 57.

Satz 2.  $J_s$  hat ganzrationale Koeffizienten.

Satz 3. Für Primzahlen  $p$  gilt

$$J_p(X, j) \equiv (X^p - j) (X - j^p) \pmod{p}.$$

Noch ein elementares Lemma über algebraische Zahlen.

Lemma 2. Seien  $k$  und  $L = k(\beta_1, \dots, \beta_h)$  Zahlkörper,  $P$  ein Primideal von  $L$  und  $p = P \cap k$ . Alle  $\beta_i$  seien ganz bei  $P$  und ihre Diskriminanten teilerfremd zu  $p$ . Dann wird  $\mathfrak{o}_L/P$  über  $\mathfrak{o}_k/p$  von den Bildern der  $\beta_i$  erzeugt.

Beweis: Es seien  $\mathfrak{o}_p$  die Lokalisierung von  $\mathfrak{o}_k$  bei  $p$  und  $\mathfrak{O}_P$  die von  $\mathfrak{o}_L$  bei  $P$ . Die Diskriminanten der  $\mathfrak{o}_p[\beta_i]$  über  $\mathfrak{o}_p$  sind die von den Diskriminanten der  $\beta_i$  über  $k$  erzeugten Ideale, also gleich (1), dementsprechend auch die Diskriminante von  $\mathfrak{o}_p[\beta_1, \dots, \beta_h]$  gleich (1). Also gilt  $\mathfrak{O}_P = \mathfrak{o}_p[\beta_1, \dots, \beta_h]$ , woraus die Behauptung folgt.

Beweis des Ersten Hauptsatzes: Zunächst überlegen wir uns, daß  $L$  der Ringklassenkörper ist. Wir prüfen die Bedingungen von Satz 1 nach und

betrachten dabei nur solche  $p$ , die den folgenden Bedingungen genügen.

- 1)  $p \neq 6$ .
- 2) alle  $j(M_\nu)$  sind ganz bei  $p$ , das heißt, bei den Primidealen, die in  $L$  über  $p$  liegen.
- 3)  $p$  ist teilerfremd zu den Diskriminanten der  $j(M_\nu)$ .
- 4)  $p$  ist teilerfremd zu allen Differenzen  $j(M_\nu) - j(M_\mu) \neq 0$ .

Bemerkung: In Wirklichkeit sind die  $j(M_\nu)$  ganz und über  $k$  konjugiert, also 2) immer erfüllt und 3) äquivalent zu 4).

Sei nun  $M = M_\nu$  fest,  $p$  vom Grad 1 und  $Np = p$ , weiter  $p_0 = p \cap o$ . Sei  $(\alpha_1, \alpha_2)$  Basis von  $M$  und  $(\beta_1, \beta_2)$  Basis von  $Mp_0$ . Es ist

$$\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = S \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \quad S \in M_2 \mathbf{Z}, \quad \det(S) = p,$$

$$\text{weiter } j(M) = j \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \quad j(Mp_0) = j \circ S \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}.$$

Es gilt  $J_p(j \circ S, j) = 0$ , also

$$(*) \quad J_p(j(Mp_0), j(M)) = 0.$$

Wähle nach Satz 0 speziell  $p$  so, daß  $p_0$  in der Hauptklasse liegt. Es folgt  $J_p(j(M), j(M)) = 0$ . Nach Satz 2 ist  $J_p(X, X)$  nicht das Nullpolynom, also  $j(M)$  algebraisch. Wenn  $\mathcal{O}_p$  den Ring bezeichnet, der aus  $\mathcal{O}_L$  durch Invertieren aller zu  $p$  teilerfremden Primideale entsteht, so gilt nach (\*) und Satz 3

$$(**) \quad (j(Mp_0)^P - j(M)) (j(Mp_0) - j(M)^P) \equiv 0 \pmod{p \mathcal{O}_p}.$$

Sei nun  $p$  in  $J_{\mathcal{O}}(\mathfrak{f})$ , also  $p_0$  Hauptideal. Dann gilt nach (\*\*) für alle Primteiler  $P$  von  $p$  in  $L$

$$j(M)^P - j(M) \equiv 0 \pmod{\mathcal{O}_p P}.$$

Mittels Lemma 2 folgt  $\alpha^P \equiv \alpha \pmod{P}$  für alle  $\alpha \in \mathcal{O}_L$ , also hat  $P$  den Grad 1, und a) aus Satz 1 ist bewiesen.

Habe nun  $p$  in  $L$  einen Faktor  $P$  ersten Grades. Nach (\*\*) gilt dann

$j(M\rho_0) - j(M) \in P_0$ . Wegen Voraussetzung 4) über  $\rho$  folgt hieraus  $j(M\rho_0) = j(M)$ , also  $M\rho_0 = \lambda M$  für ein  $\lambda \in k^*$ , also  $\rho \in J_{\mathbb{Q}}(\mathfrak{f})$ . Somit ist b) aus Satz 1 bewiesen.

Wie oben schon bemerkt, können wir den Beweis des Ersten Hauptsatzes vervollständigen, indem wir zeigen, daß alle Klasseninvarianten  $j(M_{\nu})$  zueinander konjugiert sind. Diese Tatsache wird im folgenden Satz präzisiert.

Satz 4. Es sei  $\sigma : I_0(\mathfrak{f})/P_0(\mathfrak{f}) \rightarrow \text{Gal}(L/k)$  der Artin-Isomorphismus. Für  $M, N \in I_0(\mathfrak{f})$  gilt

$$j(M)^{\sigma(N)} = j(MN^{-1}).$$

Zum Beweis wird der folgende Satz 5 benötigt. Der erste Teil wird auf Seite 27 von [D] bewiesen, der zweite ist eine Verschärfung von Satz 3 und wird im Abschnitt 14 von [D] bewiesen.

Satz 5. Es sei  $M$  ein zu  $\mathfrak{f}$  teilerfremder  $\sigma$ -Modul.

- i)  $j(M)$  ist ganz.
- ii) Sei  $\rho$  ein Primideal ersten Grades von  $k$ , das  $\mathfrak{f}$  nicht teilt. Es gilt

$$j(M(\rho \cap \sigma)^{-1}) \equiv j(M)^{N\rho} \pmod{\rho}.$$

Beweis von Satz 4: Es sei  $\rho$  ein Primideal ersten Grades in der Klasse  $(\sigma_k N) \cdot P_{\mathbb{Q}}(\mathfrak{f})$ , das zu  $\mathfrak{f}$  und allen Differenzen  $j(M_{\nu}) - j(M_{\mu})^{\sigma} \neq 0$ ,  $\sigma \in \text{Gal}(L/k)$ , teilerfremd ist. Es ist  $\sigma(N) = \sigma(\rho \cap \sigma)$  der Frobenius-Automorphismus zu  $\rho$ , also

$$j(M)^{\sigma(N)} \equiv j(M)^{N\rho} \pmod{\rho}.$$

Zusammen mit Satz 5 liefert das

$$j(MN^{-1}) \equiv j(M)^{\sigma(N)} \pmod{\rho},$$

woraus nach Voraussetzung über  $\rho$  die Behauptung folgt.

Zusatz (April 1980)

Herr Deuring hat mir inzwischen einen Entwurf für eine Neufassung des Abschnitts 10 des Enzyklopädie-Berichts geschickt. Daraus geht hervor, daß man die von mir oben auf S. 3, Mitte, erwähnte Schwierigkeit ("Solange aber noch nicht  $L$  wenigstens ... vom Grad 1 ist") leicht umgehen kann. Man kann in der Tat den Hauptsatz ohne Satz 4, nur mit Hilfe von Satz 1 beweisen. Hierzu ist Seite 5, unten, bis Seite 7 oben des Beweises in dieser Ausarbeitung wie folgt zu ändern:

Wir prüfen für  $K = k(j(M))$  die Bedingungen aus Satz 1 nach. Die Bedingungen 1) bis 4) an die  $\rho$  seien wie oben.

Sei  $\rho$  vom Grad 1 in  $k$  und  $N\rho = p$ . Wie oben gilt

$$(**) \quad (j(M\rho_0)^P - j(M)) (j(M\rho_0) - j(M)^P) \equiv 0 \pmod{p}$$

in  $K' := K(j(M\rho_0))$ .

Sei  $\rho_0$  Hauptideal. Es gilt dann  $K' = K$ , und für jeden Primteiler  $P$  von  $p$  in  $K$  folgt wie oben aus (\*\*), daß  $P$  vom Grad 1 ist.

Umgekehrt habe  $\rho$  einen Faktor  $P$  ersten Grades in  $K$ . Dann gilt

$$j(M)^P \equiv j(M) \pmod{P}.$$

Wir setzen das in (\*\*) zweimal ein und nehmen uns irgendeinen Primfaktor  $P'$  von  $P$  in  $K'$ :

$$(j(M\rho_0)^P - j(M)^P) (j(M\rho_0) - j(M)) \equiv 0 \pmod{P'}.$$

Hieraus folgt

$$j(M\rho_0) - j(M) \equiv 0 \pmod{P'}$$

und wie oben, daß  $\rho_0$  Hauptideal ist.