Von Minkowski zur Endlichkeit der Idealklassengruppe

Sei K ein Zahlkörper vom Grad n mit s Pärchen komplexer Einbettungen. Wir wollen verstehen, wieso die Idealklassengruppe Cl_K endlich ist. Genauer: wieso es endlich viele Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_m \subseteq \mathcal{O}_K$ mit

$$\mathrm{Cl}_K = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_m]\}$$

gibt – und wie man diese Ideale bestimmen kann. Grundlegend dazu ist folgendes Resultat:

Zu jedem Element $g \in \mathrm{Cl}_K$ gibt es ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ mit $g = [\mathfrak{a}]$ und

$$N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|} =: \mathrm{Min}_K.$$

Denn nach Definition gilt ja zunächst nur

$$\mathrm{Cl}_K = \{[\mathfrak{a}] \mid \mathfrak{a} \subseteq K \text{ gebrochenes Ideal}\}.$$

Wegen Minkowskis Resultat kann man aber auch

$$\mathrm{Cl}_K = \{[\mathfrak{a}] \mid \mathfrak{a} \subseteq \mathcal{O}_K \text{ Ideal mit } \mathfrak{a} \neq (0) \text{ und } N(\mathfrak{a}) \leq \mathrm{Min}_K\}$$

schreiben. Das ist eine starke Einschränkung, denn – wie wir gleich sehen werden – gibt es von diesen Idealen nur endlich viele; und mehr noch: Man kann sie finden und explizit angeben.

Dazu betrachten wir für den Moment ein beliebiges Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ mit $\mathfrak{a} \neq (0)$ und $N(\mathfrak{a}) \leq \mathrm{Min}_K$. Welche Primideale können in der Primidealzerlegung von $\mathfrak{a}$ nur vorkommen? Wenn wir $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_k^{\nu_k}$ schreiben, so gilt

$$N(\mathfrak{p}_i) \leq N(\mathfrak{p}_i)^{\nu_i} = N(\mathfrak{p}_i^{\nu_i}) \leq N(\mathfrak{p}_1^{\nu_1}) \cdots N(\mathfrak{p}_k^{\nu_k}) = N(\mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_k^{\nu_k}) = N(\mathfrak{a}) \leq \mathrm{Min}_K.$$

Ferner erkennen wir: Das Primideal $\mathfrak{p}_i$ ist nicht irgendein Primideal. Vielmehr ist es eines der Faktoren in der Primidealzerlegung von $(p) \subseteq \mathcal{O}_K$, wobei $p \in \mathbb{Z}$ die Primzahl mit $(p) = \mathfrak{p}_i \cap \mathbb{Z} \subseteq \mathbb{Z}$ ist.[1] Diese Primzahl ist nicht beliebig groß, denn es gilt

$$p \leq p^{f_i} = N(\mathfrak{p}_i) \leq \mathrm{Min}_K,$$

wenn man mit „f_i“ die endliche Dimension des $\mathbb{F}_p$-Vektorraums $\mathcal{O}_K/\mathfrak{p}_i$ bezeichnet.

Das Fazit dieser Überlegung lautet:

Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ die endlich vielen Primideale, die in den Primidealzerlegungen der endlich vielen Primideale $(p) \subseteq \mathcal{O}_K$, wobei $p \in \mathbb{Z}$ über alle Primzahlen mit $p \leq \mathrm{Min}_K$ läuft, vorkommen. Dann gilt

$$\mathrm{Cl}_K = \{[\mathfrak{a}] \mid \mathfrak{a} \subseteq \mathcal{O}_K \text{ ist ein Produkt der } \mathfrak{p}_1, \ldots, \mathfrak{p}_\ell \text{ mit } N(\mathfrak{a}) \leq \mathrm{Min}_K\}.$$

Die $\mathfrak{p}_i$ dürfen in diesen Produkten durchaus mit Vielfachheit Null oder auch mit Vielfachheit größer als Eins auftreten.

[1] Weiter vorne im Satz ist mit „(p)“ das von p erzeugte Ideal von $\mathcal{O}_K$ gemeint; weiter hinten das von p erzeugte Ideal in $\mathbb{Z}$. Die Behauptung kann man in drei Schritten einsehen:

1. Dass es überhaupt eine Primzahl $p \in \mathbb{Z}$ gibt, für die $(p) = \mathfrak{p}_i \cap \mathbb{Z}$ ist, liegt daran, dass aus ganz allgemeinen ringtheoretischen Gründen das Ideal $\mathfrak{p}_i \cap \mathbb{Z}$ ein Primideal von $\mathbb{Z}$ ist und dass dieses Primideal nicht das Nullideal ist (das liegt an der Ganzheit von $\mathcal{O}_K$ über $\mathbb{Z}$).
2. Aus allgemeinen ringtheoretischen Gründen folgt $(p) \subseteq \mathfrak{p}_i$. („Idealerweiterung ist linksadjungiert zu Idealkontraktion.“)
3. Sei $(p) = \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathcal{O}_K$ die Primidealzerlegung von (p). Da $\mathfrak{p}_i$ ein Primideal ist, folgt aus $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{p}_i$ schon, dass es einen Index j mit $\mathfrak{q}_j \subseteq \mathfrak{p}_i$ gibt. Da $\mathfrak{q}_j$ wie jedes nichttriviale Primideal in einem Dedekindring maximal ist, folgt $\mathfrak{q}_j = \mathfrak{p}_i$.

Ein Beispiel: Die Klassengruppe von $\mathbb{Q}(\sqrt{-5})$

Sei $K = \mathbb{Q}(\sqrt{-5})$. Da $-5 \equiv 3$ modulo 4, ist die Diskriminante von K gleich $4 \cdot (-5)$ und die Minkowskischranke daher

$$\mathrm{Min}_K = \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2} \cdot \sqrt{20} \approx 2{,}85.$$

Somit müssen wir nur die Primzahl $p = 2$ untersuchen, um alle Elemente der Klassengruppe auflisten zu können.

Der Führer $\mathfrak{F}_{\sqrt{-5}}$ ist das Einsideal, denn $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Daher genügt es, um die Primidealzerlegung von $(2) \subseteq \mathcal{O}_K$ zu bestimmen, die Zerlegung des Minimalpolynoms $X^2 + 5$ über $\mathbb{F}_2$ zu bestimmen. Diese lautet $X^2 + 5 = (X+1)^2 \in \mathbb{F}_2[X]$. Daher zerlegt sich das Ideal (2) als

$$(2) = \mathfrak{p}^2 \text{ mit } \mathfrak{p} = (2, \sqrt{-5} + 1).$$

Somit folgt $\mathrm{Cl}_K = \{[\mathfrak{p}^\nu] \mid \nu \geq 0 \text{ mit } N(\mathfrak{p}^\nu) \leq \mathrm{Min}_K\}$. Das können wir noch aufdröseln: Es gilt $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathbb{F}_2| = 2$, also $N(\mathfrak{p}^\nu) = 2^\nu$. Für ν sind daher nur die Werte 0 und 1 möglich. Somit besteht die Klassengruppe aus höchstens zwei Elementen:

$$\mathrm{Cl}_K = \{[(1)], [\mathfrak{p}]\}.$$

Ferner ist $\mathfrak{p}$ kein Hauptideal, denn eine Nebenrechnung zeigt, dass die Norm eines Hauptideals stets von der Form $a^2 + 5b^2$ mit $a, b \in \mathbb{Z}$ ist. Daher ist $[\mathfrak{p}] \neq [(1)]$; die Klassengruppe besteht aus genau zwei Elementen.

Eine Warnung

Man könnte denken, dass die Abschätzung $h_K \leq \mathrm{Min}_K$ gilt. Das ist jedoch falsch. Im Fall $K = \mathbb{Q}(\sqrt{-71})$ ist $h_K = 7$ und $\mathrm{Min}_K = 2\sqrt{71}/\pi \approx 5{,}36$.