Teil II. Die Diskriminante.

Sei K ein Zahlkörper vom Grad n (also $[K:\mathbb{Q}]=n$). Es gibt genau n Körper-Homomorphismen $\sigma_i\colon K\to\mathbb{C}$ (siehe Merkzettel Separabilität). Stellen wir uns K als einen Unterkörper von $\mathbb{C}$ vor, so werden wir als σ_1 die gegebene Einbettung wählen. Die Elemente $\sigma_i(\alpha)$ heißen die zu α *konjugierten* Elemente.

6.1. Die Diskriminante einer $\mathbb{Q}$-Basis eines Zahlkörpers.

Sei K ein Zahlkörper, sei $\omega_1,\dots,\omega_n$ eine $\mathbb{Q}$-Basis von K. Man nennt

$$\Delta(\omega_1,\dots,\omega_n)=\det(\sigma_i(\omega_j))^2$$

die *Diskriminante* der Basis.

(a) Basiswechsel-Formel. *Ist $C=(c_{ij})_{ij}\in M(n\times n,\mathbb{Q})$ invertierbar, und ist $\omega'_j=\sum\omega_s c_{sj}$, also auch $\sigma_i(\omega'_j)=\sum\sigma(\omega_s)c_{sj}$, so gilt*

$$\Delta(\omega'_1,\dots,\omega'_n)=\Delta(\omega_1,\dots,\omega_n)(\det C)^2.$$

Beweis. Hier sind die entsprechenden Matrizen:

$$\begin{bmatrix}\sigma_1(\omega_1) & \dots & \sigma_1(\omega_n)\\ \vdots & & \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_n)\end{bmatrix}\cdot\begin{bmatrix}c_{11} & \dots & c_{1n}\\ \vdots & & \\ c_{n1} & \dots & c_{nn}\end{bmatrix}=\begin{bmatrix}\sum\sigma_1(\omega_s)c_{s1} & \dots & \sum\sigma_1(\omega_s)c_{sn}\\ \vdots & & \\ \sum\sigma_n(\omega_s)c_{s1} & \dots & \sum\sigma_n(\omega_s)c_{sn}\end{bmatrix}$$
$$=\begin{bmatrix}\sigma_1(\sum\omega_s c_{s1}) & \dots & \sigma_1(\sum\omega_s c_{sn})\\ \vdots & & \\ \sigma_n(\sum\omega_s c_{s1}) & \dots & \sigma_n(\sum\omega_s c_{sn})\end{bmatrix}$$
$$=\begin{bmatrix}\sigma_1(\omega'_1) & \dots & \sigma_1(\omega'_n)\\ \vdots & & \\ \sigma_n(\omega'_1) & \dots & \sigma_n(\omega'_n)\end{bmatrix}.$$

Man bilde die Determinante und quadriere. Dies liefert die Formel.

(b) Satz: *Die Diskriminante einer jeden $\mathbb{Q}$-Basis von K ist eine rationale Zahl ungleich Null.*

Beweis. Wir betrachten zuerst einen Spezialfall: die Basis sei von der Form

$$1,\alpha,\alpha^2,\dots,\alpha^{n-1}\quad\text{mit }\ \alpha\in K.$$

Wir bezeichnen mit $\alpha_1=\alpha,\alpha_2,\dots,\alpha_n$ die Konjugierten von α. Die Diskriminante ist in diesem Fall das Quadrat der Determinante der folgenden Matrix:

$$\begin{bmatrix}1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1}\\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_n^{n-1}\\ \vdots & & & & \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1}\end{bmatrix}.$$

Wir erhalten als Diskriminante das Quadrat der Vandermond'sche Determinante, also

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Insbesondere sehen wir: Die Diskriminante ist nicht Null. Und dies ist ein Element in $\mathbb{Q}$, da es sich um die Auswertung eines symmetrischen Polynoms in den Konjugierten handelt.

Da $K : \mathbb{Q}$ eine separable, also eine primitive Körper-Erweiterung ist, gibt es immer ein $\alpha \in K$ mit $K = \mathbb{Q}[\alpha]$, dies bedeutet aber, dass $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ eine $\mathbb{Q}$-Basis von K ist.

Ist nun $\alpha_1, \ldots, \alpha_n$ eine beliebige $\mathbb{Q}$-Basis von K, so ist die Übergangsmatrix von der Basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ zur Basis $\alpha_1, \ldots, \alpha_n$ eine invertierbare Matrix mit Koeffizienten in $\mathbb{Q}$. Die Basiswechsel-Formel zeigt, dass die Behauptung auch für die Basis $\alpha_1, \ldots, \alpha_n$ richtig ist.

(c) Zusatz. *Besteht die Basis $\omega_1, \ldots, \omega_n$ von K aus ganzen Elementen, so ist $\Delta(\omega_1, \ldots, \omega_n) \in \mathbb{Z}$.*

Denn $\Delta(\omega_1, \ldots, \omega_n)$ liegt in dem von $\omega_1, \ldots, \omega_n$ erzeugten Unterring, ist also ganz. Die ganzen Elemente in $\mathbb{Q}$ sind aber Elemente von $\mathbb{Z}$.

6.2. Ganzheitsbasen. Die Diskriminante von K.

Wir haben gesehen, dass die Diskriminante $\Delta(\omega_1, \ldots, \omega_n)$ für jede $\mathbb{Q}$-Basis von K, die aus ganzen Elementen besteht, eine von Null verschiedene ganze Zahl ist (und solche Basen gibt es immer: ist $\alpha_1, \ldots, \alpha_n$ eine beliebige $\mathbb{Q}$-Basis von K, so gibt es zu α_i ein $c_i \in \mathbb{N}_1$ sodass $c_i\alpha_i$ ganz ist; die Elemente $c_1\alpha_1, \ldots, c_n\alpha_n$ bilden dann eine $\mathbb{Q}$-Basis von K, die aus ganzen Elementen besteht).

Für alle diese $\mathbb{Q}$-Basen aus ganzen Elementen betrachten wir nun diejenigen Basen $\omega_1, \ldots, \omega_n$, für die $|\Delta(\omega_1, \ldots, \omega_n)|$ minimal ist.

Satz. *Sei $\omega_1, \ldots, \omega_n$ eine $\mathbb{Q}$-Basis von K, die in $\mathcal{O}_K$ enthalten ist. Setzen wir voraus, dass $|\Delta(\omega_1, \ldots, \omega_n)|$ minimal ist, so ist*

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Das heißt: $\omega_1, \ldots, \omega_n$ ist ein Erzeugendensystem für die abelsche Gruppe $(\mathcal{O}_K, +)$, und natürlich sogar eine Basis (denn die Elemente $\omega_1, \ldots, \omega_n$ sind linear unabhängig im $\mathbb{Q}$-Vektorraum K). Wir sehen also: *Die additive Gruppe $(\mathcal{O}_K, +)$ ist eine freie abelsche Gruppe vom Rang n.* Man nennt eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ eine *Ganzheitsbasis* von K. Es gilt also: *Jeder Zahlkörper besitzt eine Ganzheitsbasis.*

Die Existenz einer Ganzheitsbasis impliziert sofort, dass $\mathcal{O}_K$ noethersch ist. Denn als endlich erzeugte abelsche Gruppe erfüllt $(\mathcal{O}_K, +)$ die aufsteigende Kettenbedingung für Untergruppen, also auch für Ideale (denn Ideale von $\mathcal{O}_K$ sind Untergruppen von $(\mathcal{O}_K, +)$). Wir sehen also: Um zu zeigen, dass die Ringe $\mathcal{O}_K$ noethersch sind, braucht

man den Satz von Krull-Akizuki nicht. Der neue Beweis liefert sogar eine schärfere Aussage: $\mathcal{O}_K$ ist sogar noethersch als abelsche Gruppe!

Beweis des Satzes. Sei $\omega_1, \ldots, \omega_n$ eine Ganzheitsbasis von K. Sei $\alpha \in \mathcal{O}_K$. Da $\omega_1, \ldots, \omega_n$ eine $\mathbb{Q}$-Basis von K ist, können wir α in der Form

$$\alpha = a_1\omega_1 + \cdots + a_n\omega_n \quad \text{mit} \quad a_i \in \mathbb{Q}$$

schreiben. Wir wollen zeigen, dass alle diese Koeffizienten a_i zu $\mathbb{Z}$ gehören. Angenommen, einer dieser Koeffizienten a_i ist nicht ganzzahlig. Wir können annehmen, dass dies der Koeffizient mit Index 1 ist. Sei also $a_1 = c + r$ mit $c \in \mathbb{Z}$ und $0 < r < 1$. Wir definieren eine neue $\mathbb{Q}$-Basis von K, nämlich

$$\begin{aligned}
\omega_1' &= \alpha - c\omega = r\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n \\
\omega_2' &= \omega_2 \\
&\vdots \\
\omega_n' &= \omega_n,
\end{aligned}$$

auch diese Basis liegt in $\mathcal{O}_K$.

Die Übergangsmatrix ist

$$\begin{bmatrix} r & a_2 & \cdots & a_n \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix},$$

ihre Determinante ist gleich r, also ist

$$\Delta(\omega_1', \ldots, \omega_n') = r^2\Delta(\omega_1, \ldots, \omega_n) < \Delta(\omega_1, \ldots, \omega_n).$$

Wir erhalten einen Widerspruch zur Minimalitätsvoraussetzung.

Bemerkung. Sind $\omega_1, \ldots, \omega_n$ und $\omega_1', \ldots, \omega_n'$ Ganzheitsbasen von K, so ist die Übergangsmatrix von der Basis $\omega_1, \ldots, \omega_n$ zur Basis $\omega_1', \ldots, \omega_n'$ eine invertierbare $(n \times n)$-Matrix C mit Koeffizienten in $\mathbb{Z}$, es ist also $\det C = \pm 1$, und demnach $(\det C)^2 = 1$.

Man setzt

$$\Delta_K = \Delta(\omega_1, \ldots, \omega_n)$$

wobei $\omega_1, \ldots, \omega_n$ eine Ganzheitsbasis von K ist, und nennt dies die *Diskriminante* von K; dies ist unabhängig von der Wahl der Ganzheitsbasis $\omega_1, \ldots, \omega_n$.

6.3. Die Norm eines Ideals.

Sei K ein Zahlkörper.

Sei $0 \neq I \subseteq \mathcal{O}_K$ ein Ideal. Es ist $I \cap \mathbb{Z} \neq 0$, also ein von Null verschiedenes Ideal von $\mathbb{Z}$, also $I \cap Z = m\mathbb{Z}$ für eine natürliche Zahl m. Da $m \in I$, ist $\mathcal{O}_K/I$ ein Faktorring von $\mathcal{O}_K/\langle m\rangle$. Ist $\omega_1, \ldots, \omega_n$ Ganzheitsbasis von $\mathcal{O}_K$, so ist also $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$, also $\langle m\rangle = m\mathbb{Z}\omega_1 \oplus \cdots \oplus m\mathbb{Z}\omega_n$, also ist $\mathcal{O}_K/\langle m\rangle \simeq \mathbb{Z}/m \oplus \cdots \oplus \mathbb{Z}/m$ and hat demnach die Ordnung m^n. Die Ordnung von $\mathcal{O}_K/I$ ist ein Teiler von m^n, insbesondere sieht man: *Der Faktorring $\mathcal{O}_K/I$ ist endlich.* Schreibe $N(I) = |\mathcal{O}_K/I|$, man nennt dies die *Norm* des Ideals I. Da $N(I)$ die Kardinalität einer nicht-leeren Menge ist, ist $N(I) \in \mathbb{N}_1$.

Diese Überlegungen zeigen auch: *Jedes von Null verschiedene Ideal I von $\mathcal{O}_K$ ist als abelsche Gruppe frei vom Rang n.* Denn liegt $m \in \mathbb{N}_1$ in I, so hat man die Inklusionskette

$$m\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$$

und mit $\mathcal{O}_K$ ist auch $m\mathcal{O}_K$ eine freie abelsche Gruppe vom Rang n.

(0) *Ist $I \neq 0$ ein Ideal von $\mathcal{O}_K$, so ist $N(I) \in I$.*

Beweis: Betrachte $\mathcal{O}_K/I$ als additive Gruppe. Diese Gruppe hat die Ordnung $t = N(I)$. In jeder additiven Gruppe G der Ordnung t gilt $tg = 0$ für alle $g \in G$. Also sehen wir: $tx \in \mathcal{O}_K/I$ für alle $x \in \mathcal{O}_K/I$, insbesondere gilt dies für die Restklasse der 1. Aus $0 = t\overline{1} = \overline{t}$ folgt $t \in I$.

(1) *Zu jeder natürlichen Zahl t gibt es nur endliche viele Ideale I in $\mathcal{O}_K$ mit $N(I) = t$.*

Beweis. Wir haben gesehen: aus $N(I) = t$ folgt $t \in I$, also $\langle t\rangle \subseteq I$. Es gibt aber nur endliche viele Ideale I, die ein vorgegebenes von Null verschiedenes Ideal J (hier das Ideal $\langle t\rangle$) enthalten: schreiben wir $J = \prod_i P_i^{e_i}$ mit paarweise verschiedenen maximalen Idealen P_i und $e_i \in \mathbb{N}_1$, so ist I genau dann ein Ideal mit $J \subseteq I$, wenn gilt $I = \prod_i P_i^{e_i'}$ mit $0 \leq e_i' \leq e_i$. Also ist die Anzahl der Ideale I mit $|\mathcal{O}_K/I| = t$ endlich.

(2) *Sind I, J von Null verschiedene Ideale, so ist $N(IJ) = N(I)N(J)$.*

Beweis. Wir zeigen: Sind $P_1, \ldots, P_t$ paarweise verschiedene maximale Ideale von $R = \mathcal{O}_K$ und $e_1 \ldots, e_t$ natürliche Zahlen, so ist

$$N(\prod\nolimits_i P_1^{e_i}) = \prod\nolimits_i N(P_i)^{e_i}.$$

Wegen des chinesischen Restsatzes brauchen wir nur den Fall $t = 1$ zu betrachten. Zu zeigen ist also: Ist P maximales Ideal, so ist $N(P^e) = N(P^{e-1})N(P)$, für $e \geq 2$. Die Eindeutigkeit der Primidealdarstellung liefert $P^e \subset P^{e-1}$ (echte Inklusion). Auch folgt aus der Invertierbarkeit des Ideals P^{e-1}, dass das einzige Ideal I mit $P^e \subset I \subseteq P^{e-1}$

das Ideal $I = P^{e-1}$ ist. Denn multiplizieren wir die Inklusionskette $P^e \subset I \subseteq P^{e-1}$ mit $J = (P^{e-1})^{-1} = P^{1-e}$, so erhalten wir

$$P = P^e J \subset IJ \subseteq P^{e-1}J = \mathcal{O}_K;$$

da P maximales Ideal ist, folgt $IJ = \mathcal{O}_K$, also $I = J^{-1} = P^{e-1}$.

Da $P^e \subset P^{e-1}$ eine echte Inklusion ist, können wir $\alpha \in P^{e-1} \setminus P^e$ wählen. Wir erhalten durch $r \mapsto \overline{r\alpha}$ einen Homomorphismus $R \to P^{e-1}/P^e$ von R-Moduln mit Kern P (denn offensichtlich ist P im Kern enthalten, wäre P echt im Kern enthalten, so wäre die Abbildung die Null-Abbildung). Diese Abbildung ist auch surjektiv ist, denn das Ideal $I = P^e + \langle\alpha\rangle$ erfüllt offensichtlich die Bedingungen $P^e \subset I \subseteq P^{e-1}$ und demnach ist $I = P^{e-1}$. Wir erhalten einen Modul-Isomorphismus $R/P \simeq P^{e-1}/P^e$, insbesondere ist also $|R/P| = |P^{e-1}/P^e|$.

Ist G eine endliche Gruppe, so gilt für jeden surjektiven Gruppen-Homomorphismus $\phi\colon G \to H$ mit Kern U die Gleichung

$$|G| = |H| \cdot |U|.$$

Wenden wir dies auf die kanonische Abbildung $R/P^e \to R/P^{e-1}$ mit Kern P^{e-1}/P^e an, so erhalten wir die gewünschte Gleichheit:

$$N(P^e) = |R/P^e| = |R/P^{e-1}| \cdot |P^{e-1}/P^e| = |R/P^{e-1}| \cdot |R/P| = N(P^{e-1})N(P).$$

Damit ist die Multiplikativität von $N(-)$ gezeigt.

Beachte: Die Multiplikativität der Idealnorm gilt für Ideale in beliebigen Ringen im allgemeinen nicht. Betrachte $R = k[X^2, X^3]$ wobei k ein endlicher Körper ist, sagen wir $k = \mathbb{Z}/2$. Betrachte die Ideale $I = J = \langle X^2, X^3\rangle$, mit Basis $X^2, X^3, X^4, X^5, \ldots$. Es ist $I^2 = \langle X^4, X^5\rangle$, hat also $X_4, X_5, X_6, \ldots$ als Basis. Wir sehen: $\dim R/I = 1$, aber $\dim R/I^2 = 3$. Demnach ist $|R/I| = 2$, aber $|R/I^2| = 2^3$.

(3) *Ist I ein Ideal in $\mathcal{O}_K$ und ist $y_1, \ldots, y_n$ eine $\mathbb{Z}$-Basis von I, so ist*

$$\Delta(y_1, \ldots, y_n) = \Delta_K \cdot N(I)^2.$$

Beweis: Da $I \subseteq \mathcal{O}_K$ freie abelsche Gruppen vom Rang n sind, gibt es eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ und natürliche Zahlen $c_1, \ldots, c_n$, sodass $c_1x_1, \ldots, c_nx_n$ eine $\mathbb{Z}$-Basis von I ist. Die Faktorgruppe $\mathcal{O}_K/I$ ist zu $\mathbb{Z}/c_1 \times \cdots \times \mathbb{Z}/c_n$ isomorph, hat also die Ordnung $\prod_i c_i$. Also sehen wir: $N(I) = \prod_i c_i$.

Andererseits ist die Übergangsmatrix von der Basis $x_1, \ldots, x_n$ zu $c_1x_1, \ldots, c_nx_n$ die Diagonalmatrix mit Diagonalkoeffizienten $c_1, \ldots, c_n$. Demnach ist

$$\Delta(y_1, \ldots, y_n) = \Delta(c_1x_1, \ldots, c_nx_n) = (\prod\nolimits_i c_i)^2\Delta(x_1, \ldots, x_n) = (\prod\nolimits_i c_i)^2\Delta_K.$$

(4) *Sei $0 \neq \alpha \in \mathcal{O}_K$. Es ist $N(\langle\alpha\rangle) = |\prod_{i=1}^n \sigma_i(\alpha)|$.*

Dies ist eine ganz wichtige Formel! Man nennt die Zahl $\prod_{i=1}^{n} \sigma_i(\alpha)$ die *Norm des Elements* α (im Gegensatz zur (Ideal-)Norm $N(\langle\alpha\rangle)$ des Hauptideals $\langle\alpha\rangle$); die Bedeutung der Norm von Elementen in Zahlkörpern haben wir am Beispiel $K = \mathbb{Q}[\sqrt{-1}]$ gesehen; dort wurde ständig mit der Norm von Elementen argumentiert. Ähnlich geht man bei den anderen quadratischen Zahlkörpern vor, aber auch bei beliebigen Zahlkörpern! Die Formel (4) besagt, dass die (Ideal-)Norm des Haupideals $\langle\alpha\rangle$ gerade der Betrag der Norm des Elements α ist.

Wir können die Formel ohne Verwendung von $N(-)$ direkt in der Form

$$|\mathcal{O}_K/\langle\alpha\rangle| = |\prod_{i=1}^{n} \sigma_i(\alpha)|$$

schreiben. Die Betragsstriche links und rechts haben dabei aber ganz verschiedene Bedeutungen: links stehen sie für die Kardinalität der endlichen Menge $\mathcal{O}_K/\langle a\rangle$, rechts wird der Betrag einer rationalen Zahl genommen.

Beweis. Sei $\omega_1, \ldots, \omega_n$ Ganzheitsbasis von $\mathcal{O}_K$. Dann ist $\alpha\omega_1, \ldots, \alpha\omega_n$ eine $\mathbb{Z}$-Basis von $\langle\alpha\rangle$. Es ist also

$$\begin{aligned} N(\langle\alpha\rangle)^2\Delta_K &= \Delta(\alpha\omega_1, \ldots, \alpha\omega_n) = \det(\sigma_i(\alpha\omega_j))^2 \\ &= \det(\sigma_i(\alpha)\sigma_i(\omega_j))^2 = (\sigma_1(\alpha)\cdots\sigma_n(\alpha))^2\Delta_K, \end{aligned}$$

denn die Matrix $(\sigma_i(\alpha)\sigma_i(\omega_j))_{ij}$ entsteht aus der Matrix $(\sigma_i(\omega_j))_{ij}$ durch Multiplikation der i-ten Reihe mit $\sigma_i(\alpha)$, für $1 \leq i \leq n$.

Daraus folgt $N(\langle\alpha\rangle)^2 = (\sigma_1(\alpha)\cdots\sigma_n(\alpha))^2$. Beim Wurzelziehen ist zu beachten, dass $N(I)$ nach Definition positiv ist, für jedes Ideal I. Das Produkt $\sigma_1(\alpha)\cdots\sigma_n(\alpha)$ kann dagegen negativ sein.