6.5. Fundamentalgleichung.

Sei K ein Zahlkörper vom Grad n , sei $\mathcal{O}_K$ der Ring der ganzen Zahlen in K .

Ist P ein maximales Ideal von $\mathcal{O}_K$, so gibt es eine (und nur eine) Primzahl $p \in \mathbb{Z}$, die zu P gehört. Der Restklassenring $\mathcal{O}_K/P$ ist ein endlicher Körper der Charakteristik p , also ein Vektorraum über $\mathbb{Z}/p$. Man nennt $e(P) = \dim_{\mathbb{Z}/p} \mathcal{O}_K/P$ den *Trägheitsgrad* von P , natürlich ist $N(P) = p^{e(P)}$.

Schreiben wir das von p erzeugte Hauptideal $\langle p \rangle$ in $\mathcal{O}_K$ als Produkt von Primideale, etwa

$$\langle p \rangle = P_1^{f_1} \cdots P_t^{f_t},$$

mit paarweise verschiedenen Primidealen $P_1, \dots, P_t$ und natürlichen Zahlen $f_i \geq 1$, so nennt man f_i den *Verzweigungs-Index* des Primideals P_i . Wir setzen $e_i = e(P_i)$. Die Multiplikativität der Norm liefert

$$p^n = N(\langle p \rangle) = N(P_1)^{f_1} \cdots N(P_t)^{f_t} = p^{e_1 f_1} \cdots p^{e_t f_t},$$

also

$$n = e_1 f_1 + \cdots + e_t f_t,$$

dies wird die **Fundamentalgleichung** für das Zerlegungsverhalten der Primzahl p genannt. Gilt $f_i \geq 2$, so sagt man, dass P_i eine *Verzweigung* liefert. Die Primzahl p heißt *verzweigt*, falls es einen Index i mit $f_i \geq 2$ gibt, sonst *unverzweigt*.

Beispiel. Ist K ein quadratischer Zahlkörper, also $n = 2$, so gibt es drei verschiedene Arten des Zerlegungsverhaltens:

Fall 1	$t = 2$	$e_1 = 1$	$f_1 = 1$	$e_2 = 1$	$f_2 = 1$
Fall 2	$t = 1$	$e_1 = 2$	$f_1 = 1$		
Fall 3	$t = 1$	$e_1 = 1$	$f_1 = 2$		

Nur im Fall 3 gibt es Primideale, die verzweigt sind. Wir können das verschiedenartige Zerlegungsverhaltens auch folgendermaßen formulieren:

Fall 1	$\mathcal{O}_K/p$ ist Produkt zweier Körper.
Fall 2	$\mathcal{O}_K/p$ ist Körper.
Fall 3	$\mathcal{O}_K/p$ ist lokaler Ring der Länge 2.

Ist etwa $K = \mathbb{Q}[\sqrt{-1}]$, so erhalten wir in Abhängigkeit von p

Fall 1	für $p \equiv 1 \pmod{4}$
Fall 2	für $p \equiv 3 \pmod{4}$
Fall 3	für $p = 2$

6.6. Die Diskriminante zeigt, welche Primzahlen verzweigt sind.

Satz (Dedekind). Sei $\mathcal{O}_K$ Zahlkörper, sei p Primzahl. Genau dann gibt es über $\langle p \rangle$ ein verzweigtes Primideal, wenn p die Diskriminante Δ_K teilt. Insbesondere gibt es nur endlich viele verzweigte Primideale!

Beweis: Als erstes notieren wir:

(a) Genau dann gibt es über $\langle p \rangle$ ein verzweigtes Primideal, wenn $\mathcal{O}_K/\langle p \rangle$ von Null verschiedene nilpotente Elemente besitzt.

Sei $\langle p \rangle = P_1^{f_1} \cdots P_n^{f_n}$ mit paarweise verschiedenen maximalen Idealen P_i und natürlichen Zahlen $f_i \geq 1$. Ist nun etwa $f_1 \geq 2$, so setze $I = P_1 P_2^{f_2} \cdots P_t^{f_t}$. Es ist

$$\langle p \rangle = P_1^{f_1} \cdots P_n^{f_n} \subset P_1 P_2^{f_2} \cdots P_n^{f_n} = I$$

(echte Inklusion), also ist $I/\langle p \rangle \neq 0$. Offensichtlich ist aber $I^{f_1} \subseteq \langle p \rangle$ und demnach sind alle Elemente in $I/\langle p \rangle$ nilpotent.

Ist dagegen $f_i = 1$ für alle i , so ist also $\langle p \rangle = P_1 \cdots P_n$ und demnach zeigt der chinesische Restsatz

$$\mathcal{O}_K/\langle p \rangle = \mathcal{O}_K/P_1 \times \cdots \times \mathcal{O}_K/P_t,$$

dass $\mathcal{O}_K/\langle p \rangle$ ein Produkt von t Körpern ist. Ein Produkt von Körpern besitzt aber keine von Null verschiedenen nilpotenten Elemente.

Der weitere Beweis beruht darauf, einen allgemeineren Diskriminanten-Begriff einzuführen, der nicht nur für Zahlkörper sinnvoll ist. Zur Vorbereitung zeigen wir, dass sich die Diskriminante eines Zahlkörpers ganz anders berechnen lässt! Allgemeiner betrachten wir eine separable Körper-Erweiterung $K : K'$ vom Grad n . Die Separabilität besagt, dass es n paarweise verschiedene Ring-Homomorphismen $K \rightarrow \overline{K'}$ (den algebraischen Abschluss von K') gibt. Ist $\alpha \in K$, so sei $\text{Tr}(\alpha)$ die Spur der Multiplikationsabbildung $(\alpha \cdot)$ (wir fassen K als n -dimensionalen K' -Vektorraum auf).

Lemma. Sei $K : K'$ eine separable Körpererweiterung, sei $\omega_1, \dots, \omega_n$ eine K' -Basis von K und es seien $\sigma_1, \dots, \sigma_n : K \rightarrow \overline{K'}$ paarweise verschiedene K' -lineare Ring-Homomorphismen. Dann gilt:

$$\det((\sigma_i(\omega_j))_{ij})^2 = \det(\text{Tr}(\omega_i \omega_j)_{ij}).$$

Beachte: Ist K ein Zahlkörper und setzen wir $K' = \mathbb{Q}$, so haben wir die linke Determinante als Diskriminante $\Delta(\omega_1, \dots, \omega_n)$ bezeichnet. Wir sehen also, dass wir diese Diskriminante auch durch die Determinante rechts beschreiben können. Die Matrix $(\sigma_i(\omega_j))_{ij}$ hat komplexen Koeffizienten, die üblicherweise nicht rational sein werden. Dagegen sind die Koeffizienten $\text{Tr}(\omega_i \omega_j)$, die rechts verwendet werden, rationale Zahlen! Besser noch: arbeitet man mit einer Basis $\omega_1, \dots, \omega_n$ mit ganz-algebraischen Zahlen, so sind auch die Werte $\text{Tr}(\omega_i \omega_j)$ ganz-algebraisch, also ganze rationale Zahlen.

Beweis: Die Multiplikationsabbildung $(\alpha \cdot)$ hat die Eigenwerte $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ (mit den richtigen Vielfachheiten). Es ist also $\text{Tr}(\alpha) = \sum_i \sigma_i(\alpha)$; denn die Spur ähnlicher Matrizen ist gleich, jede darstellende Matrix für (α) ist aber über $\overline{K'}$ ähnlich zur Diagonalmatrix mit den Diagonalkoeffizienten $\sigma_i(\alpha)$.

Nun ist

$$\begin{aligned} \det(\sigma_i(\omega_j)_{ij})^2 &= \det((\sigma_i(\omega_j))_{ij}) \det((\sigma_s(\omega_t))_{st}) \\ &= \det((\sigma_s(\omega_r))_{rs}) \det((\sigma_s(\omega_t))_{st}) \\ &= \det\left(\left(\sum_s \sigma_s(\omega_r)\sigma_s(\omega_t)\right)_{st}\right) \\ &= \det((\text{Tr}(\omega_r\omega_t))_{rt}). \end{aligned}$$

Dabei haben wir zweimal die Multiplikativität der Determinante und dazwischen das Übereinstimmen der Determinante einer Matrix mit der der Transponierten verwendet.

Der allgemeine Rahmen. Seien $R \subseteq S$ kommutative Ringe, sei S ein freier R -Modul endlichen Rangs, etwa mit Basis $\omega_1, \dots, \omega_n$. Setze

$$\Delta_{S|R}(\omega_1, \dots, \omega_n) = \det(\text{Tr}(\omega_i\omega_j)).$$

Hier betrachten wir also die Determinante zu einer Matrix, die zu der symmetrischen Bilinearform

$$S \times S \longrightarrow R, \quad \text{mit } (\alpha, \beta) \mapsto \text{Tr}(\alpha\beta) \quad \text{für } \alpha, \beta \in S$$

gehört; man nennt diese Bilinearform die *Spurform* zur Ring-Erweiterung $R \subseteq S$. Um eine darstellende Matrix für eine derartige Bilinearform zu finden, braucht man eine R -Basis von S , wir haben diese Basis mit $\omega_1, \dots, \omega_n$ bezeichnet. Bei einem Basiswechsel mit Basiswechselmatrix C ändert sich die Determinante der darstellenden Matrix mit dem Faktor $(\det C)^2$. Folgende Definition macht daher Sinn: man nennt eine derartige Bilinearform *ausgeartet*, wenn die Determinante der darstellenden Matrix bezüglich einer Basiswahl (und damit bezüglich jeder Basiswahl) gleich Null ist.

Ist $R = \mathbb{Z}$ und $S = \mathcal{O}_K$, so ist die Determinante einer jeden darstellenden Matrix der Spurform gleich Δ_K , also ist hier die Spurform nicht ausgeartet (in diesem Fall haben alle darstellenden Matrizen die gleiche Determinante, da $(\det C)^2$ für jede invertierbare Matrix C mit Koeffizienten in $\mathbb{Z}$ gilt).

Als nächstes betrachten wir nun den Fall $R = \mathbb{Z}/p$ und $S = \mathcal{O}_K/\langle p \rangle$.

(b) *Genau dann ist p ein Teiler von Δ_K , wenn die Spurform des Rings $\mathcal{O}_K/\langle p \rangle$ ausgeartet ist.*

Beweis: Bezüglich der $\mathbb{Z}/p$ -Basis $\bar{\omega}_1, \dots, \bar{\omega}_n$ ist die Determinante der darstellenden Matrix der Spurform gerade $\bar{\Delta}_K$ (alle Restklassenbildungen sind modulo p). Denn ist $\alpha \in \mathcal{O}_K$ und $\alpha\omega_i = \sum_j c_{ij}\omega_j$, so ist $\text{Tr}(\alpha) = \sum_i c_{ii}$. In $\mathcal{O}_K/\langle p \rangle$ gilt dann entsprechend $\bar{\alpha}\bar{\omega}_i = \sum_j \bar{c}_{ij}\bar{\omega}_j$, also ist

$$\text{Tr}(\bar{\alpha}) = \sum_i \bar{c}_{ii} = \overline{\text{Tr}(\alpha)}.$$

Also ist

$$\begin{aligned} \Delta_{\mathcal{O}_K/\langle p \rangle|\mathbb{Z}/p}(\bar{\omega}_1, \dots, \bar{\omega}_n) &= \det(\text{Tr}(\bar{\omega}_i\bar{\omega}_j)) \\ &= \det(\text{Tr}(\overline{\omega_i\omega_j})) \\ &= \det(\overline{\text{Tr}(\omega_i\omega_j)}) = \bar{\Delta}_K. \end{aligned}$$

(c) *Gibt es in $S = \mathcal{O}_K/\langle p \rangle$ von Null verschiedene nilpotente Elemente, so ist die Spurform von S über $\mathbb{Z}/p$ ausgeartet.*

Beweis: Sei $0 \neq x_1 \in S$ nilpotent. Betrachte eine $\mathbb{Z}/p$ -Basis $x_1, \dots, x_n$ von S , deren erstes Element also nilpotent ist. Mit x_1 sind auch die Elemente $x_1 x_j$ für alle j nilpotent (in jedem kommutativen Ring ist mit einem Element r auch jedes Vielfache rr' nilpotent). Ist aber $\alpha \in S$ nilpotent, so ist die Multiplikationsabbildung $(\alpha \cdot): S \rightarrow S$ nilpotent. Die Spur eines nilpotenten Endomorphismus ist Null. Also sehen wir: $\text{Tr}(x_1 x_j) = 0$ für alle j . Die darstellende Matrix der Spurform bezüglich der Basis $x_1, \dots, x_n$ hat also in der ersten Zeile nur Nullen, demnach ist ihre Determinante gleich Null.

(d) *Gibt es in $S = \mathcal{O}_K/\langle p \rangle$ keine von Null verschiedene nilpotente Elemente, so ist die Spurform von S über $\mathbb{Z}/p$ nicht ausgeartet.*

Beweis: Nach Voraussetzung ist $S = \mathcal{O}_K/\langle p \rangle = F_1 \times \dots \times F_t$ mit endlichen Körpern F_i der Charakteristik p (hier ist $F_i = \mathcal{O}_K/P_i$, wobei $\langle p \rangle = P_1 \cdots P_t$ mit maximalen Idealen P_i). Als erstes zeigen wir:

$$\Delta_{S|\mathbb{Z}/p} = (\Delta_{F_1|\mathbb{Z}/p}) \cdots (\Delta_{F_t|\mathbb{Z}/p}).$$

Wähle dazu eine Basis $x_1, \dots, x_n$ von S , wobei die ersten Basiselemente zu F_1 , die nächsten zu F_2 , usw.; die letzten zu F_t gehören. Bezüglich dieser Basis ist die darstellende Matrix der Spurform geblockt, von Null verschiedene Blöcke gibt es nur entlang der Hauptdiagonalen, und der s -te derartige Block ist gerade die darstellende Matrix der Spurform auf F_s bezüglich derjenigen Basisvektoren x_i , die zu F_s gehören.

Es bleibt also zu zeigen: *Ist F ein endlicher Körper der Charakteristik p so ist die Spurform von F bezüglich $\mathbb{Z}/p$ nicht ausgeartet.* Dies liegt an der Separabilität der Körper-Erweiterung $F : \mathbb{Z}/p$.

Ganz allgemein gilt nämlich : *Die Spurform einer separablen Körpererweiterung $K : K'$ ist nicht ausgeartet.*

Beweis: Sei $n = [K : K']$ und $K : K'$ separabel. Es gibt n paarweise verschiedene K' -lineare Ring-Homomorphismen $\sigma_i : K \rightarrow \overline{K'}$. Wählt man eine K' -Basis $x_1, \dots, x_n$ von K , so besagt das Lemma:

$$\Delta_{K:K'}(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2.$$

Es bleibt zu zeigen: *die Matrix $(\sigma_i(\omega_j))_{ij}$ ist invertierbar.* Beweis. Angenommen, die Matrix ist nicht invertierbar. Dann gibt es einen von Null verschiedenen Zeilenvektor $[c_1, \dots, c_n]$ mit $[c_1, \dots, c_n](\sigma_i(\omega_j))_{ij} = 0$, also

$$\sum_i c_i \sigma_i(\omega_j) = 0 \quad \text{für alle } 1 \leq j \leq n.$$

Dies impliziert, dass die linearen Abbildungen $\sigma_i : K \rightarrow \overline{K'}$ linear abhängig sind. Dies ist ein Widerspruch zum Dedekind-Lemma (mit $H = (K, \cdot)$ und $\Omega = \overline{K'}$).