7. Die Hilbert'sche Verzweigungstheorie.

Sei $L\colon K$ eine Körpererweiterung vom Grad n, die galois'sch ist. Dann vereinfacht sich die Fundamentalgleichung ganz entschieden.

Sei $G = \mathrm{Gal}(L\colon K)$ die Galois-Gruppe der Körper-Erweiterung. Jedes $\sigma \in G$ bildet $\mathcal{O}_L$ in sich (sogar auf sich) ab. Die Einschränkung von σ auf $\mathcal{O}_L$ liefert also einen Ring-Automorphismus von $\mathcal{O}_L$, und unter diesem Ring-Automorphismus (der wieder mit σ bezeichnet wird) bleiben die Elemente aus $\mathcal{O}_L$ (und nur diese!) invariant.

7.1. Transitivität der Operation der Galois-Gruppe auf Mengen von Primidealen von $\mathcal{O}_L$. Ist Q ein Primideal von $\mathcal{O}_L$, so ist $\sigma(Q)$ ein Primideal von $\mathcal{O}_L$, wir sehen also: G operiert auf der Menge der maximalen Ideale von $\mathcal{O}_K$. Wir wissen: Ist Q maximales Ideal von $\mathcal{O}_L$, so ist $Q \cap \mathcal{O}_K$ ein maximales Ideal von $\mathcal{O}_K$, und für $\sigma \in G$ gilt:

$$\sigma(Q) \cap \mathcal{O}_K = Q \cap \mathcal{O}_K$$

(denn ist $\alpha \in Q \cap \mathcal{O}_K$, so ist $\alpha \in K$, also $\sigma(\alpha) = \alpha$, also $\alpha \in \sigma(\alpha) \cap \mathcal{O}_K$; die umgekehrte Inklusion erhält man entsprechend: Ist $\beta \in Q$ mit $\sigma(\beta) \in \mathcal{O}_K$, so wende σ^{-1} an: es ist $\beta = \sigma^{-1}\sigma(\beta) \in Q \cap \mathcal{O}_K$).

Wir sehen: G operiert auf der Menge der Primideale von $\mathcal{O}_L$, die über einem gegebenen maximalen Ideal P von $\mathcal{O}_K$ liegen.

Satz. *Sei P maximales Ideal von $\mathcal{O}_K$. Die Galois-Gruppe $G = \mathrm{Gal}(L\colon K)$ operiert transitiv auf der Menge der Primideale von $\mathcal{O}_L$, die über P liegen.*

Beweis. Zur Erinnerung: Sind $Q_1, \ldots, Q_g$ die Primideale von $\mathcal{O}_L$ (paarweise verschieden), die über P liegen. Betrachten wir einen festen Index i, so liefert der chinesische Restsatz ein Element $\alpha \in Q_i$ mit $\alpha \notin Q_j$ für $j \neq i$.

Bilde das Produkt

$$\beta = \prod\nolimits_{\sigma \in G} \sigma^{-1}(\alpha)$$

(wir könnten auch $\beta = \prod_{\sigma \in G} \sigma^{-1}(\alpha)$ schreiben, denn die Menge der Elemente $\{\sigma^{-1} | \sigma \in G\}$ ist nichts anderes als die Menge der Elemente von G, nur eben in einer anderen Reihenfolge durchlaufen).

Einer der Faktoren ist $\alpha \in Q_i$ (nämlich für $\sigma = 1 \in G$), alle anderen gehören zumindest zu $\mathcal{O}_L$, also ist $\beta \in Q_i$. Es ist $\tau(\beta) = \beta$ für jedes $\tau \in G$ (denn unter der Anwendung von τ gehen die Faktoren $\sigma^{-1}(\alpha)$ in $\tau\sigma^{-1}(\alpha)$ über — jeweils wird die ganze Gruppe durchlaufen). Daraus folgt aber $\beta \in K$, also $\beta \in \mathcal{O}_L \cap K = \mathcal{O}_K$, und daraus folgt

$$\beta \in Q_i \cap \mathcal{O}_K = P \subseteq Q_1.$$

Da Q_1 ein Primideal in $\mathcal{O}_L$ ist und die Faktoren $\sigma^{-1}(\alpha)$ zu $\mathcal{O}_L$ gehören, muss mindestens einer der Faktoren zu Q_1 gehören: Aus $\sigma^{-1}(\alpha) \in Q_1$ folgt $\alpha \in \sigma(Q_1)$.

Nun ist aber Q_i das einzige der Primideale $Q_1, \ldots, Q_g$ mit $\alpha \in Q_i$. Da $\sigma(Q_1)$ eines dieser Primideale ist und $\alpha \in \sigma(Q_1)$ gilt, sehen wir $\sigma(Q_1) = Q_i$.

7.2. Die Fundamental-Gleichung.

Zur Erinnerung: Sei Q maximales Ideal von $\mathcal{O}_L$ und $P = Q \cap \mathcal{O}_K$. Der *Verzweigungsindex* von Q über K ist die kleinste natürliche Zahl e mit $Q^e \subseteq \mathcal{O}_K P$ (mit $P = Q \cap \mathcal{O}_K$). Da $\mathcal{O}_L$ ein Dedekind-Ring ist, kann der Verzweigungsindex e auch folgendermäsen definiert werden: Es ist $\mathcal{O}_K P = Q^e J$, wobei J ein Ideal von $\mathcal{O}_L$ mit $J \not\subseteq Q$ ist. Der *Trägheitsgrad* von Q über K ist der Grad der Körpererweiterung $\mathcal{O}_L/Q \colon \mathcal{O}_K/P$.

Lemma. *Sei Q maximales Ideal von $\mathcal{O}_L$ und $\sigma \in G$. Dann gilt für jede natürliche Zahl e:*

$$\sigma(Q^e) = \sigma(Q)^e$$

und σ induziert einen Isomorphismus

$$\overline{\sigma} \colon \mathcal{O}_K/Q^e \longrightarrow \mathcal{O}_K/\sigma(Q)^e.$$

Insbesondere gilt: *Trägheitsgrad und Verzweigungsindex von Q und $\sigma(Q)$ sind gleich.*

Beweis: Sei P ein maximales Ideal von $\mathcal{O}_K$. Seien $Q_1, \ldots, Q_g$ die Primideale von $\mathcal{O}_L$ (paarweise verschieden), die über P liegen. Die Primidealzerlegung von $\mathcal{O}_L P$ hat dann die Form

$$\mathcal{O}_L P = Q_1^{e_1} \cdots Q_g^{e_g}$$

mit natürlichen Zahlen $e_i \geq 1$. Sei f_i der Trägheitsindex von Q_i (über K). Wie wir gerade gesehen haben, gilt

$$e := e_1 = \cdots = e_g,$$
$$f := f_1 = \cdots = f_g.$$

Die Fundamentalgleichung hat demnach die einfache Form:

$$\boxed{n = efg}$$

Hier ist also n der Grad der (galois'schen) Körpererweiterung $L \colon K$, ein maximales Ideal P von $\mathcal{O}_K$ ist vorgegeben, g ist die *Zerlegungszahl*: die Anzahl der Primideale Q_i von $\mathcal{O}_L$, die über P liegen, f ist der Trägheitsgrad und e der Verzweigungsgrad eines jeden Q_i.

Bemerkung. Jede quadratische Körpererweiterung $L \colon K$ ist galois'sch. Sei P ein maximales Ideal von $\mathcal{O}_K$. Die Gleichung $2 = efg$ hat drei mögliche Lösungen:
- $e = 1,\ f = 1,\ g = 2$. Das Ideal P ist in $\mathcal{O}_L$ voll zerlegt.
- $e = 1,\ f = 2,\ g = 1$. Trägheit: $\mathcal{O}_L P$ ist Primideal in $\mathcal{O}_L$.
- $e = 2,\ f = 1,\ g = 1$. Das Ideal P ist in $\mathcal{O}_L$ total verzeigt.

Entsprechendes gilt für jede galois'sche Erweiterung $L \colon K$ mit Primzahlgrad p: Genau eine der drei Zahlen e, f, g ist gleich p, die beiden anderen sind gleich 1.