7.3. Zerlegungsgruppe und Trägheitsgruppe. Sei $\mathcal{O}_K$ ein Dedekind-Ring mit Quotientenkörper K. Sei $L\colon K$ eine Körpererweiterung vom Grad n. Sei $\mathcal{O}_L$ der ganze Abschluss von $\mathcal{O}_K$ in L. Wir setzen wieder voraus, dass $L\colon K$ galois'sch ist.

Sei Q ein maximales Primideal von $\mathcal{O}_L$ und $P = Q \cap \mathcal{O}_K$. Wir definieren zwei Untergruppen wie folgt: erstens die *Zerlegungsgruppe*

$$\mathcal{Z} = \mathcal{Z}_Q = \{\sigma \in G \mid \sigma(Q) = Q\}$$

und zweitens die *Trägheitsgruppe*

$$\mathcal{T} = \mathcal{T}_Q = \{\sigma \in Z \mid \sigma(x) \equiv x \mod Q^2, \text{ für alle } x \in Q\}$$

Dies sind offensichtlich Untergruppen von $G = \mathrm{Gal}(L\colon K)$ und zwar gilt:

$$\mathcal{T} \subseteq \mathcal{Z} \subseteq G.$$

Wir setzen

$$Z = \mathrm{Fix}(\mathcal{Z}), \qquad \text{und} \qquad T = \mathrm{Fix}(\mathcal{T}),$$

also können wir den Körperturm

$$K \subseteq Z \subseteq T \subseteq L$$

betrachten, dabei heißt Z der *Zerlegungskörper* von Q über K, entsprechend heißt T der *Trägheitskörper* von Q über K. Wir verfolgen nun, was mit dem Primideal Q geschieht, wenn wir es mit T oder mit Z schneiden.

(1) Die Erweiterung $Z\colon K$**.** *Es ist* $[Z\colon K] = g$. Und es gilt: *Sind* Q, Q' *maximale Ideale von* L *von* $Q \cap \mathcal{O}_Z = Q' \cap \mathcal{O}_Z$*, so ist* $Q = Q'$ (das Primideal $Q \cap \mathcal{O}_Z$ wird in L nicht zerlegt).

Beweis: Sei $G = \mathrm{Gal}(L\colon K)$. Es gibt die Formel: Bahnenlänge $\times$ Stabilisatorordnung = Gruppenordnung. Die Bahnenlänge ist g, der Stabilisator ist $\mathcal{Z}$. Also ist $|\mathcal{Z}| = |G|/g$. Andererseits liefert die Galois-Theorie $[L\colon Z] = |\mathcal{Z}|$ und $[L : K] = |G|$. Demnach ist $[Z\colon K] = [L\colon K]/[L\colon Z] = |G|/(|G|/g) = g$.

Die Primideale Q' von $\mathcal{O}_L$, die über $Q \cap \mathcal{O}_Z$ liegen, liegen über $Q \cap \mathcal{O}_K$, es sind also dies einige unserer Primideale $Q = Q_1, \ldots, Q_g$. Nach 9.1, angewandt auf die Galois-Erweiterung $L\colon Z$ gilt: die Gruppe $\mathcal{Z} = \mathrm{Gal}(L\colon Z)$ operiert transitiv auf diesen Primidealen. Aber nach Definition von $\mathcal{Z}$ gilt: $\sigma(Q) = Q$ für alle $\sigma \in \mathcal{Z}$, demnach ist Q das einzige Primideal von $\mathcal{O}_L$, das über $Q \cap \mathcal{O}_Z$ liegt.

Warnung. Im Allgemeinen wird $Z\colon K$ nicht galois'sch sein. Genau dann ist $Z\colon K$ galois'sch, wenn $\mathcal{Z}$ ein Normalteiler von G ist. Die Zerlegungsgruppe zum Primideal $\sigma(Q)$ ist die zu $\mathcal{Z}$ konjugierte Untergruppe $\sigma\mathcal{Z}\sigma^{-1}$. Ist also $\mathcal{Z}$ ein Normalteiler, so haben alle Primideale Q_i die gleiche Zerlegungsgruppe und demnach den gleichen Zerlegungskörper und die Primideale $Q_i \cap \mathcal{O}_Z$ sind dann paarweise verschieden: wir sehen: Zumindest in diesem Fall ist das Primideal $P = Q \cap \mathcal{O}_K$ in $\mathcal{O}_Z$ voll zerlegt.

(2) Die Erweiterung $T\colon Z$.

Setze $\overline{L} = \mathcal{O}_L/Q$ und $\overline{K} = \mathcal{O}_K/P$; wir können $\overline{K}$ als einen Unterkörper von $\overline{L}$ auffassen. Ist $\sigma \in \mathcal{Z}$, so ist also $\sigma(Q) = Q$, demnach induziert σ einen Automorphismus $\overline{\sigma}$ von $\overline{L}$. Natürlich bleiben die Elemente aus $\overline{K}$ unter $\overline{\sigma}$ invariant, also ist $\overline{\sigma}$ ein Element von $\mathrm{Gal}(\overline{L}\colon \overline{K})$.

Satz. *Sei $\overline{L}\colon \overline{K}$ separabel. Dann gilt: Die kanonische Abbildung $\mathcal{Z} \to \mathrm{Gal}(\overline{L}\colon \overline{K})$ ist surjektiv,* der Kern ist $\mathcal{T}$, wir erhalten also einen Gruppen-Isomorphismus

$$\boxed{\mathcal{Z} \to \mathrm{Gal}(\overline{L}\colon \overline{K})}$$

Beweis: Sei $\overline{\theta} \in \overline{L}$ ein primitives Element, mit $\theta \in L$. Sei $f = \prod_{\sigma\in G}(X - \sigma\theta)$ das charakteristische Polynom von θ; dies ist also ein Polynom in $\overline{K}[X]$ und wir können $\overline{f} \in \overline{K}[X]$ betrachten. Das Minimalpolynom Polynom von $\overline{\theta}$ ist ein Teiler von $\overline{f}$, zerfällt also über $\overline{L}$ in Linearfaktoren, die Nullstellen sind von der Form $\overline{\sigma(\theta)} = \overline{\sigma}(\overline{\theta})$.

Ist also $\overline{L}\colon \overline{K}$ separabel, so ist $T\colon Z$ eine Körpererweiterung vom Grad f und $Q \cap Z$ ist träge, insbesondere unverzweigt.

(3) Die Erweiterung $L\colon T$. *Das Primideal $Q \cap \mathcal{O}_T$ ist in L vollständig verzweigt.*

Zusammenfassung. Die Fundamentalgleichung

$$\boxed{n = efg}$$

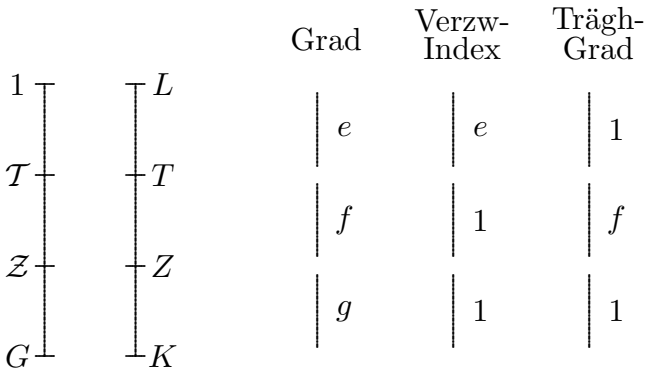
die wir zu einer galois'schen Körpererweiterung $L\colon K$ vom Grad n und jedem maximalen Ideal P von $\mathcal{O}_K$ erhalten, drückt sich also nach Wahl eines Primideals Q von $\mathcal{O}_L$ mit $Q \cap \mathcal{O}_K = P$ folgendermaßen aus: Es gibt einen Körperturm

$$L \supseteq T \supseteq Z \supseteq K$$

mit

$$[L\colon T] = e,\ [T\colon Z] = f,\ [Z\colon K] = g;$$

und diese Körpererweiterungen haben bezüglich des jeweiligen Primideals $Q \cap \mathcal{O}_T$, bzw. $Q \cap \mathcal{O}_Z$, bzw. $Q \cap \mathcal{O}_K = P$ das folgende Verhalten:



Für die Körperweiterungen $L\colon T$ und $T\colon Z$ ist rechts jeweils der gemeinsame Verzweigungsindex und Trägheitsgrad der Primideale über $Q \cap \mathcal{O}_T$ bzw. $Q \cap \mathcal{O}_Z$ notiert; für die nicht-notwendig galois'sche Erweiterung $Z\colon K$ handelt es sich um den Verzweiungsindex und Trägheitsgrad des Primideals $Q \cap \mathcal{O}_Z$ über $Q \cap \mathcal{O}_K = P$.

7.4. Die Verzweigungsgruppen. Sei $L\colon K$ endliche Galois-Erweiterung, sei Q ein maximales Ideal von $\mathcal{O}_L$. Für $i \geq 0$ setze

$$\mathcal{V}_i = \{\sigma \in \mathcal{Z} \mid \sigma(x) \equiv x \mod Q^{i+1} \text{ für alle } x \in \mathcal{O}_L\}.$$

Dies ist der Kern des kanonischen Gruppen-Homomorphismus $\mathcal{Z} \to \mathrm{Aut}(\mathcal{O}/Q^{i-1})$, also ein Normalteiler von $\mathcal{Z}$, man nennt $\mathcal{V}_i$ die *i-te Verzweigungsrguppe.* Es gilt:

$$\mathcal{T} = \mathcal{V}_0 \supseteq \mathcal{V}_1 \supseteq \cdots \supseteq \mathcal{V}_r = \{1\}$$

für ein geeignetes r. (Die Inklusionen sind offensichtlich; die Existenz von r sieht man folgendermaßen: Es ist $\bigcap_i \mathcal{V}_i = \{1\}$, denn ist $\sigma \in \mathcal{V}_i$ für alle i, so ist $\sigma(x) - x \in Q^{i+1}$ für alle i, aber $\bigcap_i Q^i = 0$, also $\sigma(x) = x$, also $\sigma = 1$. Da $\mathcal{T}$ eine endliche Gruppe ist, muss es ein r mit $\mathcal{V}_r = \{1\}$ geben.)

Satz. Sei $p \in Q$.

(a) *Die Gruppen-Ordnung $|\mathcal{V}_0/\mathcal{V}_1|$ ist ein Teiler von $|\overline{L}| - 1$.*

(b) *Die Gruppe $\mathcal{V}_1$ ist eine p-Gruppe.*

(c) *Sei $K = \mathbb{Q}$. Ist $\mathcal{Z}$ abelsch, so ist $|\mathcal{V}_0/\mathcal{V}_1|$ ein Teiler von $p - 1$.*

Beweis: Sei $\pi \in Q \setminus Q^2$. Es ist also Q^i/Q^{i+1} ein eindimensionaler $\overline{L}$-Vektorraum mit Basiselement die Restklasse $\overline{\pi^i}$ von π^i modulo Q^{i+1}.

Zum Beweis von (a) und (c) definiere einen Gruppen-Homomorphismus

$$\theta_0\colon \mathcal{V}_0 \longrightarrow (\overline{L}^*, \cdot)$$

mit Kern $\mathcal{V}_1$. Dann ist die Faktorgruppe $\mathcal{V}_0/\mathcal{V}_1$ zu einer Untergruppe der multiplikativen Gruppe $(\overline{L}^*, \cdot)$ isomorph, und demnach ist die Ordnung $|\mathcal{V}_0/\mathcal{V}_1|$ ein Teiler der Ordnung $|(\overline{L}^*, \cdot)| = |\overline{L}| - 1$.

Ist $\sigma \in \mathcal{V}_0$, so sei

$$\sigma(\pi) \equiv c_\sigma \pi \mod Q^2 \qquad \text{mit} \qquad c_\sigma \in \mathcal{O}_L.$$

Da $\pi \notin Q^2$, ist auch $\sigma(\pi) \notin Q^2$, also $c_\sigma \notin Q$, demnach ist die Restklasse $\overline{c}_\sigma \in \overline{L}$ von Null verschieden. Setze

$$\theta_0(\sigma) = \overline{c}_\sigma.$$

wir erhalten auf diese Weise eine Abbildung $\mathcal{V}_0 \to \overline{L}^*$, und dies ist ein *Gruppen-Homomorphismus mit Kern $\mathcal{V}_1$* (wie man leicht nachrechnet). Damit ist (a) bewiesen.

Beachte: *Der Gruppenhomomorphismus θ_0 hängt nicht von der Auswahl von π ab.* Ist nämlich $\pi' \in Q \setminus Q^2$, so ist $\pi' \equiv \alpha\pi \mod Q^2$ mit $\alpha \in \mathcal{O}_L \setminus Q$. Es ist

$$\sigma(\pi') \equiv \sigma(\alpha\pi) = \sigma(\alpha)\sigma(\pi) \equiv \alpha\sigma(\pi) \equiv \alpha c_\sigma \pi \equiv c_\sigma \pi' \mod Q^2$$

(wegen $\sigma \in \mathcal{V}_0$ ist $\sigma(\alpha) \equiv \alpha \mod Q$, also $\sigma(\alpha)\sigma(\pi) \equiv \alpha\sigma(\pi) \mod Q^2$).

Da die Faktorgruppe $\mathcal{V}_0/\mathcal{V}_1$ zu einer Untergruppe der multiplikativen Gruppe $\overline{L}^*$ isomorph ist, ist $|\mathcal{V}_0/\mathcal{V}_1|$ ein Teiler von $|\overline{L}| - 1$.

Zum Beweis von (c) zeigen wir, dass das Bild von θ_0 in $(\mathbb{Z}/p)^*$ enthalten ist (falls $K = \mathbb{Q}$ und $\mathcal{Z}$ abelsch). Wir wissen, dass die kanonische Abbildung

$$\mathcal{Z} \to \mathrm{Gal}(\overline{L}, \mathbb{Z}/p)$$

surjektiv ist. Nun gibt es in $\mathrm{Gal}(\overline{L}, \mathbb{Z}/p)$ den Frobenius-Automorphismus $x \mapsto x^p$, also gibt es $\phi \in \mathcal{Z}$, sodass $\overline{\phi}$ dieser Frobenius-Automorphismus ist. Es ist also

$$\phi(\alpha) \equiv \alpha^p \qquad \text{für alle} \qquad \alpha \in \mathcal{O}_L.$$

Natürlich ist $\phi(\pi) \in Q \setminus Q^2$, also gilt für $\sigma \in \mathcal{V}_0$

$$c_\sigma \phi(\pi) \equiv \sigma\phi(\pi) = \phi\sigma(\pi) = \phi(c_\sigma \pi) = \phi(c_\sigma)\phi(\pi) \equiv c_\sigma^p \phi(\pi) \mod Q^2,$$

also $c_\sigma \equiv c_\sigma^p \mod Q$. Dies bedeutet aber, dass $\overline{c}_\sigma$ zum Primkörper $\mathbb{Z}/p$ gehört.

Wir beweisen nun (b). Sei also $i \geq 1$. Auch zum Beweis von (b) konstruieren wir einen Gruppen-Homomorphismus der auf $\mathcal{V}_i$ definiert ist (mit Kern $\mathcal{V}_{i+1}$), diesmal aber mit Werten in der **additiven** Gruppe $(\overline{L}, +)$. Ist $\sigma \in \mathcal{V}_i$, so ist $\sigma(\pi) \equiv \pi \mod Q^{i+1}$, also $\sigma(\pi) - \pi \in Q^{i+1}$. Es gibt daher $c_\sigma \in \mathcal{O}_L$ mit

$$\sigma(\pi) - \pi \equiv c_\sigma \pi^{i+1} \mod Q^{i+2},$$

also $\sigma(\pi) \equiv \pi + c_\sigma \pi^{i+1}$. Setze

$$\theta_i \colon \mathcal{V}_i \to (\overline{L}, +) \text{ mit } \theta_i(\sigma) = \overline{c}_\sigma.$$

Auch hier kann man unmittelbar nachrechnen, dass θ_i ein Gruppen-Homomorphismus und dass der Kern gerade $\mathcal{V}_{i+1}$ ist. Wir sehen also, dass $\mathcal{V}_i/\mathcal{V}_{i+1}$ isomorph zu einer Untergruppe der additiven Gruppe $(\overline{L}, +)$ ist.

Da $|\overline{L}|$ eine p-Potenz ist (denn $\overline{L}$ ist ein $\mathbb{Z}/p$-Vektorraum), ist die Gruppe $\mathcal{V}_i/\mathcal{V}_{i+1}$ für jedes $i \geq 1$ eine p-Gruppe. Nun ist $\mathcal{V}_1$ eine Erweiterung der Gruppen $\mathcal{V}_i/\mathcal{V}_{i+1}$ mit $i \geq 1$, also ebenfalls eine p-Gruppe. Damit ist auch (b) bewiesen.