Nachtrag zur Vorlesung über Verzweigung im Galoisfall

Diese Notiz soll einen ausführlichen Beweis der folgenden Behauptung geben:

> Sei $L|K$ eine Galoiserweiterung von Zahlkörpern. Sei $\mathfrak{P} \subseteq \mathcal{O}_L$ ein Primideal über $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ mit $\mathfrak{P} \neq (0)$. Dann ist die Erweiterung $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ galoissch und der kanonische Gruppenhomomorphismus
>
> $$\begin{array}{rcl} G_{\mathfrak{P}} & \longrightarrow & \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) \\ \sigma & \longmapsto & \overline{\sigma} \end{array}$$
>
> ist surjektiv.

Dabei ist $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$, $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ und $G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L|K) \,|\, \sigma[\mathfrak{P}] = \mathfrak{P}\}$; und $\overline{\sigma}$ schickt $[x]$ auf $[\sigma(x)]$.

Reduktionsschritt

Zunächst beobachtet man, dass man ohne Einschränkung der Allgemeinheit voraussetzen kann, dass die Zerlegungsgruppe $G_{\mathfrak{P}}$ schon gleich der gesamten Galoisgruppe $\mathrm{Gal}(L|K)$ ist. Denn das ist im Fall, dass man nicht die Erweiterung $L|K$, sondern die Erweiterung $L|Z_{\mathfrak{P}}$ betrachtet, der Fall (Teilaussage (0) des vorhergehenden Satzes); und beim Übergang von $L|K$ zu $L|Z_{\mathfrak{P}}$ ändert sich die Behauptung nicht, denn $G_{\mathfrak{P}|\mathfrak{p}} = G_{\mathfrak{P}|\mathfrak{q}}$ und $\mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{q}))$. (Die letzte Gleichheit folgt aus $f(\mathfrak{q}|\mathfrak{p}) = 1$, denn somit gilt $\kappa(\mathfrak{p}) = \kappa(\mathfrak{q})$.)

Die so geschenkte Zusatzvoraussetzung $G_{\mathfrak{P}} = \mathrm{Gal}(L|K)$ wird erst im letzten Teilschritt des Beweises eingehen.

Nachweis der Normalität

Sei $\overline{g} \in \kappa(\mathfrak{p})[X]$ ein normiertes irreduzibles Polynom, das in $\kappa(\mathfrak{P})$ eine Nullstelle $\overline{\theta}$ besitzt. Es gibt dann ein $\theta \in \mathcal{O}_L$ mit $\overline{\theta} = [\theta] \in \kappa(\mathfrak{P})$. Wir möchten zeigen, dass $\overline{g}$ über $\kappa(\mathfrak{P})$ in Linearfaktoren zerfällt.

Sei $f \in K[X]$ das Minimalpolynom von θ über K. Da θ ganz ist, sind auch alle Koeffizienten von f ganz, also liegt f schon in $\mathcal{O}_K[X]$. Wir schreiben „$\overline{f}$“ für dasjenige Polynom in $\kappa(\mathfrak{p})[X]$, das aus f entsteht, indem man alle Koeffizienten längs $\mathcal{O}_K \to \kappa(\mathfrak{p})$ reduziert.

Nun gilt $\overline{f}(\overline{\theta}) = [f(\theta)] = [0] = 0 \in \kappa(\mathfrak{P})$, also ist $\overline{f}$ ein Vielfaches des Minimalpolynoms von $\overline{\theta}$. Somit $\overline{g} \mid \overline{f}$ über $\kappa(\mathfrak{p})$.

Da $L|K$ normal ist und f in L eine Nullstelle besitzt (nämlich θ), zerfällt f über L schon in Linearfaktoren. Die einzelnen Nullstellen sind wie θ jeweils ganz, also zerfällt L sogar schon über $\mathcal{O}_L$ in Linearfaktoren.

Somit zerfällt auch $\overline{f}$ über $\kappa(\mathfrak{P})$ in Linearfaktoren. Und $\overline{g}$ als Teiler von $\overline{f}$ damit ebenfalls.

Nachweis der Surjektivität

Dieser Teil des Beweises geht an vielen Stellen genau wie der vorherige Teilbeweis vor, jedoch ist die Zielsetzung eine andere. Sei $\tau \in \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$ gegeben; wir suchen ein Urbild in $G_{\mathfrak{P}}$.

Da die Voraussetzungen des Satzes über das primitive Element erfüllt sind, gibt es ein $\overline{\theta} \in \kappa(\mathfrak{P})$ mit $\kappa(\mathfrak{P}) = \kappa(\mathfrak{p})(\overline{\theta})$. Es gibt dann ein $\theta \in \mathcal{O}_L$ mit $\overline{\theta} = [\theta]$.[1]

Sei $\overline{g} \in \kappa(\mathfrak{p})[X]$ das Minimalpolynom von $[\theta]$ über $\kappa(\mathfrak{p})$ und seien f und $\overline{f}$ wie im vorherigen Abschnitt definiert, sei also $f \in \mathcal{O}_K[X]$ das Minimalpolynom von θ über K und $\overline{f}$ seine Reduktion modulo $\mathfrak{p}$.

Der Automorphismus τ ist durch die Angabe seines Bilds $\overline{\theta}' := \tau(\overline{\theta})$ schon eindeutig festgelegt. Da wir einen Lift von τ auf L finden möchten, sollten wir dieses Bild genauer studieren. Zumindest ist klar, dass es eine der Nullstellen von $\overline{g}$ ist. (Wie immer: $\overline{g}(\overline{\theta}') = \overline{g}(\tau(\overline{\theta})) = \tau(\overline{g}(\overline{\theta})) = \tau(0) = 0$, da τ die Koeffizienten von $\overline{g}$ invariant lässt, da sie in $\kappa(\mathfrak{p})$ liegen.)

Wie oben zerfällt f über $\mathcal{O}_L$ in Linearfaktoren: $f = \prod_i (X - \theta_i)$ mit Nullstellen $\theta_i \in \mathcal{O}_L$. Somit zerfällt auch $\overline{f}$ über $\kappa(\mathfrak{P})$ in Linearfaktoren, nämlich in die $\prod_i (X - [\theta_i])$. Da $\overline{g}$ ein Teiler von $\overline{f}$ ist, ist $\overline{\theta}'$ eine der Nullstellen von $\overline{f}$. Also gibt es einen Index i mit $\overline{\theta}' = [\theta_i]$.

Wir können nun einen Automorphismus $\sigma : L \to L$ über K durch die Forderung $\sigma(\theta) = \theta_i$ konstruieren. Das machen wir, indem wir zunächst eine Körpereinbettung $K(\theta) \to L$ durch $\theta \mapsto \theta_i$ definieren (dazu müssen wir bekanntlich nur beachten, dass das Bildelement θ_i Nullstelle des Minimalpolynoms des Erzeugers θ ist) und diese dann beliebig zu einem Automorphismus $L \to L$ fortsetzen.

Wegen der Zusatzvoraussetzung ist σ nicht nur ein Element von $\mathrm{Gal}(L|K)$, sondern sogar von $G_{\mathfrak{P}}$. Dieses Element ist das gesuchte Urbild, denn $\overline{\sigma}$ und τ stimmen auf dem Erzeuger $\overline{\theta}$ überein: $\overline{\sigma}(\overline{\theta}) = \overline{\sigma}([\theta]) = [\sigma(\theta)] = [\theta_i] = \overline{\theta}' = \tau(\overline{\theta})$, und stimmen somit schon auf ganz $\kappa(\mathfrak{P})$ überein.

[1] Man kann sich fragen, ob auch $L = K(\theta)$ ist. Das ist allerdings nicht zu erwarten – man denke an den Fall, dass $f(\mathfrak{P}|\mathfrak{p}) = 1$ ist. In diesem Fall ist $\kappa(\mathfrak{P}) = \kappa(\mathfrak{p})$, also ist $\theta = 1$ möglich. Aber in diesem Fall ist ja noch nicht unbedingt $L = K$.