

## 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

$$\begin{array}{ccc} G_{\mathfrak{p}} & \longrightarrow & \text{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) \\ \sigma & \longmapsto & \bar{\sigma} \end{array}$$

ist surjektiv.

Dabei ist  $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ ,  $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$  und  $G_{\mathfrak{p}} = \{\sigma \in \text{Gal}(L|K) \mid \sigma[\mathfrak{P}] = \mathfrak{P}\}$ ; und  $\bar{\sigma}$  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  $\text{Gal}(L|K)$  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  $\text{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = \text{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{q}))$ . (Die letzte Gleichheit folgt aus  $f(\mathfrak{q}|\mathfrak{p}) = 1$ , denn somit gilt  $\kappa(\mathfrak{p}) = \kappa(\mathfrak{q})$ .)

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

### Nachweis der Normalität

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

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

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

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

Somit zerfällt auch  $\bar{f}$  über  $\kappa(\mathfrak{P})$  in Linearfaktoren. Und  $\bar{g}$  als Teiler von  $\bar{f}$  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  $\tau \in \text{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$  gegeben; wir suchen ein Urbild in  $G_{\mathfrak{p}}$ .

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

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

Der Automorphismus  $\tau$  ist durch die Angabe seines Bilds  $\bar{\theta}' := \tau(\bar{\theta})$  schon eindeutig festgelegt. Da wir einen Lift von  $\tau$  auf  $L$  finden möchten, sollten wir dieses Bild genauer studieren. Zumindest ist klar, dass es eine der Nullstellen von  $\bar{g}$  ist. (Wie immer:  $\bar{g}(\bar{\theta}') = \bar{g}(\tau(\bar{\theta})) = \tau(\bar{g}(\bar{\theta})) = \tau(0) = 0$ , da  $\tau$  die Koeffizienten von  $\bar{g}$  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  $\bar{f}$  über  $\kappa(\mathfrak{P})$  in Linearfaktoren, nämlich in die  $\prod_i (X - [\theta_i])$ . Da  $\bar{g}$  ein Teiler von  $\bar{f}$  ist, ist  $\bar{\theta}'$  eine der Nullstellen von  $\bar{f}$ . Also gibt es einen Index  $i$  mit  $\bar{\theta}' = [\theta_i]$ .

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

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

---

<sup>1</sup>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  $L = K$ .