Aufgabe F20T3A4

Seien K ein Körper und $L|K$ eine endliche Galoiserweiterung.

(a) Wir betrachten Zwischenkörper M und M' von $L|K$ und ein Element σ in $\mathrm{Gal}(L|K)$. Zeigen Sie die Äquivalenz der folgenden beiden Aussagen.

  (i) $\sigma(M) = M'$

  (ii) $\sigma\mathrm{Gal}(L|M)\sigma^{-1} = \mathrm{Gal}(L|M')$

(b) Seien L der Zerfällungskörper eines irreduziblen Polynoms f in $K[x]$ und α und β Nullstellen von f in L. Zeigen Sie, dass die Galoisgruppen $\mathrm{Gal}(L|K(\alpha))$ und $\mathrm{Gal}(L|K(\beta))$ zueinander isomorph sind.

(c) Zeigen Sie, dass man in (b) die Voraussetzung, dass f irreduzibel ist, nicht weglassen kann.

Lösung:

zu (a) „$\Rightarrow$" Wir zeigen, dass M' der Fixkörper der Untergruppe $U = \sigma\mathrm{Gal}(L|M)\sigma^{-1}$ von $G = \mathrm{Gal}(L|K)$ ist; dann folgt Gleichung (ii) aus dem Hauptsatz der Galoistheorie. Sei $\alpha \in L$ vorgegeben. Weil $\sigma : L \to L$ bijektiv ist, existiert ein $\beta \in L$ mit $\sigma(\beta) = \alpha$. Es gilt nun die Äquivalenz

$$\alpha \in L^U \quad \Leftrightarrow \quad \forall\, \tau \in U : \tau(\alpha) = \alpha \quad \Leftrightarrow \quad \forall\, \tau \in \mathrm{Gal}(L|M) : (\sigma \circ \tau \circ \sigma^{-1})(\alpha) = \alpha \quad \Leftrightarrow$$
$$\forall\, \tau \in \mathrm{Gal}(L|M) : (\sigma \circ \tau \circ \sigma^{-1})(\sigma(\beta)) = \sigma(\beta) \quad \Leftrightarrow \quad \forall\, \tau \in \mathrm{Gal}(L|M) : \sigma(\tau(\beta)) = \sigma(\beta) \quad \Leftrightarrow$$
$$\forall\, \tau \in \mathrm{Gal}(L|M) : \tau(\beta) = \beta \quad \Leftrightarrow \quad \beta \in L^{\mathrm{Gal}(L|M)} \quad \Leftrightarrow \quad \beta \in M \quad \Leftrightarrow \quad \sigma(\beta) \in \sigma(M) \quad \Leftrightarrow \quad \alpha \in M'.$$

Dabei wurde im fünften Schritt erneut die Bijektivität von σ verwendet, und im siebten (drittletzten) der Hauptsatz der Galoistheorie. Die Äquivalenz zeigt, dass tatsächlich $M' = L^U$ gilt.

„$\Leftarrow$" Sei $M'' = \sigma(M)$. Wie wir unter „$\Rightarrow$" gezeigt haben, ist M'' der Fixkörper von $\sigma\mathrm{Gal}(L|M)\sigma^{-1}$, auf Grund der Voraussetzung also von $\mathrm{Gal}(L|M')$. Nach dem Hauptsatz der Galoistheorie gilt $L^{\mathrm{Gal}(L|M')} = M'$. Aus Aus $M'' = L^{\mathrm{Gal}(L|M')}$ und $L^{\mathrm{Gal}(L|M')} = M'$ folgt $M' = M'' = \sigma(M)$.

zu (b) Auf Grund des Fortsetzungssatzes, angewendet auf das irreduzible Polynom f, existiert ein Element $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Weil σ ein K-Homomorphismus ist, gilt $\sigma(K(\alpha)) = K(\sigma(\alpha)) = K(\beta)$. Nach Teil (a) folgt daraus $\mathrm{Gal}(L|K(\beta)) = \sigma\mathrm{Gal}(L|K(\alpha))\sigma^{-1}$. Die Untergruppen $\mathrm{Gal}(L|K(\alpha))$ und $\mathrm{Gal}(L|K(\beta))$ sind also konjugiert zueinander; daraus folgt, dass sie isomorph sind.

zu (c) Sei $f = x(x^2+1) = x^3 + x \in \mathbb{Q}[x]$. Die Nullstellenmenge dieses Polynoms ist $N = \{0, i, -i\}$, somit ist $L = \mathbb{Q}(N)$ der Zerfällungskörper von f. Aus $i \in N \subseteq \mathbb{Q}(N)$ und $N = \{0, i, -i\} \subseteq \mathbb{Q}(i)$ folgt $\mathbb{Q}(N) = \mathbb{Q}(i)$. Die Erweiterung $L|\mathbb{Q}$ ist normal, da L Zerfällungskörper des Polynoms f über $\mathbb{Q}$ ist. Als normale Erweiterung ist $L|\mathbb{Q}$ insbesondere algebraisch, und jede algebraische Erweiterung von $\mathbb{Q}$ ist wegen $\mathrm{char}(\mathbb{Q}) = 0$ separabel. Insgesamt ist $L|\mathbb{Q}$ also eine Galois-Erweiterung.

Wir bestimmen die Ordnung der Galois-Gruppe $G = \mathrm{Gal}(f|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(i)|\mathbb{Q})$. Das Polynom $g = x^2 + 1$ ist normiert, irreduzibel und hat i als Nullstelle. Es ist g also das Minimalpolynom von i über $\mathbb{Q}$, und folglich gilt $[L : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = \mathrm{grad}(g) = 2$. Da $L|Q$ eine Galois-Erweiterung ist, erhalten wi r $|G| = |\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 2$.

Betrachten wir nun die beiden Nullstellen $\alpha = 0$ und $\beta = i$ von f. Dann ist $\mathbb{Q}(\alpha) = Q$ und $\mathbb{Q}(\beta) = L$. Es folgt $|\mathrm{Gal}(L|\mathbb{Q}(\alpha))| = [L : \mathbb{Q}(\alpha)] = [L : \mathbb{Q}] = 2$ und $|\mathrm{Gal}(L|\mathbb{Q}(\beta))| = [L : \mathbb{Q}(\beta)] = [L : L] = 1$. Als Gruppen unterschiedlicher Ordnung können $\mathrm{Gal}(L|\mathbb{Q}(\alpha))$ und $\mathrm{Gal}(L|\mathbb{Q}(\beta))$ nicht isomorph sein. ‘