Aufgabe F17T1A1 (12 Punkte)

Sei $L|\mathbb{Q}$ eine endliche galoissche Körpererweiterung. Die Norm eines Elements $x \in L$ sei gegeben als

$$N(x) \quad := \quad \prod_{\sigma \in \mathrm{Gal}(L|\mathbb{Q})} \sigma(x).$$

(a) Zeigen Sie, dass $N(x) \in \mathbb{Q}$ für alle $x \in L$ und $N(xy) = N(x)N(y)$ für alle $x, y \in L$ gilt.

(b) Betrachten Sie den Spezialfall $L = \mathbb{Q}[\sqrt{5}]$. Zeigen Sie, dass $N(r + \sqrt{5}s) = r^2 - 5s^2$ für $r, s \in \mathbb{Q}$ gilt.

(c) Betrachten Sie in L den Teilring $\mathbb{Z}[\sqrt{5}] = \{r + s\sqrt{5} \mid r, s \in \mathbb{Z}\}$. Zeigen Sie, dass für $x \in \mathbb{Z}[\sqrt{5}]$ gilt, dass x genau dann eine Einheit in $\mathbb{Z}[\sqrt{5}]$ ist, wenn $N(x) \in \{1, -1\}$ gilt.

(d) Zeigen Sie, dass 11 kein Primelement in $\mathbb{Z}[\sqrt{5}]$ ist.

Lösung:

zu (a) Sei $G = \mathrm{Gal}(L|\mathbb{Q})$. Für jedes $x \in L$ und $\tau \in G$ gilt

$$\tau N(x) \quad = \quad \tau\left(\prod_{\sigma \in G} \sigma(x)\right) \quad = \quad \prod_{\sigma \in G} \tau(\sigma(x)) \quad = \quad \prod_{\sigma \in G} (\tau \circ \sigma)(x) \quad = \quad \prod_{\sigma \in G} \sigma(x) \quad = \quad N(x).$$

Dabei wurde im zweiten Schritt verwendet, dass τ als Körperautomorphismus verträglich mit der Multiplikation ist, und im vorletzten Schritt, dass mit σ auch $\tau \circ \sigma$ die gesamte Gruppe G durchläuft (denn die Abbildung $G \to G$, $\sigma \mapsto \tau \circ \sigma$ ist eine Bijektion). Aus der Gleichung $\tau N(x) = N(x)$ für jedes $\tau \in G$ folgt, dass $N(x)$ im Fixkörper L^G von G enthalten ist. Nach dem Hauptsatz der Galoistheorie gilt $L^G = L^{\mathrm{Gal}(L|\mathbb{Q})} = \mathbb{Q}$, also gilt $N(x) \in \mathbb{Q}$. Für beliebige $x, y \in L$ gilt darüber hinaus

$$N(x)N(y) \quad = \quad \left(\prod_{\sigma \in G} \sigma(x)\right)\left(\prod_{\sigma \in G} \sigma(y)\right) \quad = \quad \prod_{\sigma \in G} (\sigma(x)\sigma(y)) \quad = \quad \prod_{\sigma \in G} \sigma(xy) \quad = \quad N(xy).$$

zu (b) Das Polynom $f = x^2 - 5 \in \mathbb{Q}[x]$ ist irreduzibel und hat $\sqrt{5}$ als Nullstelle. Deshalb gilt $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = \mathrm{grad}(f) = 2$. Als algebraische Erweiterung von $\mathbb{Q}$ ist L separabel und als Erweiterung vom Grad 2 auch normal. Insgesamt ist $L|\mathbb{Q}$ also eine Galois-Erweiterung, und es gilt $|\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 2$. Auf Grund des Fortsetzungssatzes, angewendet auf das irreduzible Polynom f und die beiden Nullstellen $\sqrt{5}$ und $-\sqrt{5}$, gibt es ein $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ mit $\sigma(\sqrt{5}) = -\sqrt{5}$. Weil σ ein $\mathbb{Q}$-Automorphismus von L ist, gilt dann $\sigma(r + s\sqrt{5}) = r - s\sqrt{5}$ für alle $r, s \in \mathbb{Q}$. Wegen $|\mathrm{Gal}(L|\mathbb{Q})| = 2$ ist also $\mathrm{Gal}(L|\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}, \sigma\}$, und es folgt $N(r + s\sqrt{5}) = \mathrm{id}_{\mathbb{Q}}(r + s\sqrt{5})\sigma(r + s\sqrt{5}) = (r + s\sqrt{5})(r - s\sqrt{5}) = r^2 - 5s^2$ für alle $r, s \in \mathbb{Q}$.

zu (c) Sei $R = \mathbb{Z}[\sqrt{5}]$. Zunächst bemerken wir, dass $N(r + s\sqrt{5}) = r^2 - 5s^2 \in \mathbb{Z}$ für alle $r, s \in \mathbb{Z}$ gilt. Die Funktion N nimmt auf dem Ring R also nur ganze Zahlen als Werte an. "$\Rightarrow$" Ist x eine Einheit von R, also $x \in R^\times$, dann gibt es ein $y \in R$ mit $xy = 1$. Mit dem Ergebnis aus Teil (a) folgt $N(x)N(y) = N(xy) = N(1) = N(1 + 0 \cdot \sqrt{5}) = 1^2 - 5 \cdot 0^2 = 1$. Aus $N(x)N(y) = 1$ und $N(x), N(y) \in \mathbb{Z}$ folgt $N(x) \in \{\pm 1\}$. "$\Leftarrow$" Sei $x = r + s\sqrt{5} \in R$ mit $r, s \in \mathbb{Z}$. Setzen wir $y = r - s\sqrt{5}$, dann ist $y \in \mathbb{R}$, und es gilt $xy = (r + s\sqrt{5})(r - s\sqrt{5}) = N(x)$. Ist $N(x) = 1$, dann folgt $xy = 1$. Ist $N(x) = -1$, dann folgt $x(-y) = 1$. In beiden Fällen ist x eine Einheit in R.

zu (d) Es gilt $(4 + \sqrt{5})(4 - \sqrt{5}) = 4^2 - 5 \cdot 1^2 = 16 - 5 = 11$, und wegen $N(4 \pm \sqrt{5}) = 11 \notin \{\pm 1\}$ sind die Elemente $4 \pm \sqrt{5}$ beides keine Einheiten. Also ist 11 in R kein irreduzibles Element. Als Teilring des Körpers $\mathbb{R}$ ist R ein Integritätsbereich. Als Primelement in einem Integritätsbereich müsste 11 auch irreduzibel sein. Dies zeigt, dass 11 kein Primelement ist.