Aufgabe 9 von Blatt 15

Sei $f \in \mathbb{Q}[X]$ normiert, separabel, $x_1, \ldots, x_n$ seien die (alle) Nullstellen von f. Mindestens eine der Nullstellen sei nicht-reell.

Behauptung. *Es gibt eine Permutation $\sigma \in S_n$ mit folgenden zwei Eigenschaften:*

1. $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_n)$.
2. σ *hat Ordnung 2, d. .h.* $\sigma \neq \mathrm{id}$ *und* $\sigma^2 = \mathrm{id}$.

Beweis (danke an Martin!). Man weiß: Hat ein Polynom mit reellen Koeffizienten eine nicht-reelle Nullstelle, so ist auch das komplex Konjugierte der Nullstelle eine Nullstelle des Polynoms.

[Denn: Gelte ganz allgemein $p(x) = 0$, wobei p nur reelle Koeffizienten hat und $x \in \mathbb{C}$ eine beliebige Nullstelle ist. Dann gilt: $0 = \overline{0} = \overline{p(x)} = p(\overline{x})$, wobei somit auch $\overline{x}$ eine Nullstelle von p ist. Der letzte Schritt der Rechnung folgt daraus, dass p nur reelle Koeffizienten besitzt.]

Wir ordnen nun die Nullstellen von f so an, dass die reellen Nullstellen hinten stehen $(x_{r+1}, \ldots, x_n)$, und dass die komplex-konjugierten Paare vorne nebeneinander stehen, also dass gilt:

$$x_2 = \overline{x_1}, \quad x_4 = \overline{x_3} \quad \ldots \quad x_r = \overline{x_{r-1}}.$$

Wir definieren nun folgende Permutation:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & r-1 & r & r+1 & \cdots & n \\ 2 & 1 & 4 & 3 & \cdots & r & r-1 & r+1 & \cdots & n \end{pmatrix}$$

Dann ist zumindest klar, dass die Ordnung von σ zwei ist. Es ist aber noch nicht klar, dass σ ein Element der Galoisgruppe ist.

Um das zu zeigen, gehen wir direkt nach Definition vor: Sei $H \in \mathbb{Q}[X_1, \ldots, X_n]$ eine beliebige algebraische Relation der Nullstellen, d. h. es gilt $H(x_1, \ldots, x_n) = 0$.

Zu zeigen ist, dass auch gilt:

$$H(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = H(x_2, x_1, x_4, x_3, \ldots, x_r, x_{r-1}, x_{r+1}, \ldots, x_n) = 0$$

Dazu folgende Rechnung:

$$\begin{aligned} 0 &= H(x_1, \ldots, x_n) \\ &= \overline{H(x_1, \ldots, x_n)} \\ &= H(\overline{x_1}, \ldots, \overline{x_n}) \\ &= H(x_2, x_1, x_4, x_3, \ldots, x_r, x_{r-1}, x_{r+1}, \ldots, x_n) \end{aligned}$$

Der Schritt von der zweiten in die dritte Zeile ist deswegen erlaubt, weil H nur reelle Koeffizienten besitzt. Damit ist der Beweis abgeschlossen. □