

Übungsblatt 11 zur Algebra I

Abgabe bis 1. Juli 2013, 17:00 Uhr

Aufgabe 1. Wirkung der galoisschen Gruppe

Seien x_1, \dots, x_n die Nullstellen eines normierten separablen Polynoms $f(X)$ mit rationalen Koeffizienten.

- Seien σ und τ Symmetrien der Nullstellen. Zeige, dass $\sigma \cdot (\tau \cdot x_i) = (\sigma \circ \tau) \cdot x_i$ für alle $i = 1, \dots, n$.
- Sei σ eine Symmetrie der Nullstellen und seien $z, w \in \mathbb{Q}(x_1, \dots, x_n)$. Zeige: $\sigma \cdot (z + w) = \sigma \cdot z + \sigma \cdot w$ und $\sigma \cdot (zw) = (\sigma \cdot z)(\sigma \cdot w)$.
- Zeige, dass genau dann eine Symmetrie σ der Nullstellen mit $x_2 = \sigma \cdot x_1$ existiert, wenn x_1 und x_2 zueinander galoissch konjugiert sind.

Lösung.

- Es gilt $\sigma \cdot (\tau \cdot x_i) = \sigma \cdot x_{\tau(i)} = x_{\sigma(\tau(i))} = x_{(\sigma \circ \tau)(i)} = (\sigma \circ \tau) \cdot x_i$.
- Da z und w in $\mathbb{Q}(x_1, \dots, x_n)$ liegen, gibt es Polynome $g, h \in \mathbb{Q}[X_1, \dots, X_n]$ mit

$$\begin{aligned} z &= g(x_1, \dots, x_n), \\ w &= h(x_1, \dots, x_n). \end{aligned}$$

Daher folgt

$$\begin{aligned} \sigma \cdot (z + w) &= \sigma \cdot (g(x_1, \dots, x_n) + h(x_1, \dots, x_n)) = g(x_{\sigma(1)}, \dots, x_{\sigma(n)}) + h(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \\ &= \sigma \cdot g(x_1, \dots, x_n) + \sigma \cdot h(x_1, \dots, x_n) = \sigma \cdot z + \sigma \cdot w, \end{aligned}$$

der Multiplikationsfall geht völlig analog.

Aufgabe 2. Abstrakte Beispiele für Galoisgruppen

- Sei $f(X)$ ein normiertes quadratisches Polynom mit rationalen Koeffizienten, dessen Nullstellen x_1 und x_2 verschieden seien. Berechne die Galoisgruppe $\text{Gal}_{\mathbb{Q}}(x_1, x_2)$ in Abhängigkeit der Diskriminante von $f(X)$.
- Sei $f(X)$ ein normiertes irreduzibles Polynom vom Grad 3 mit rationalen Koeffizienten und Nullstellen x_1, x_2, x_3 . Sei x_1 kein primitives Element zu $\mathbb{Q}(x_1, x_2, x_3)$. Zeige, dass die Galoisgruppe der Nullstellen genau sechs Element enthält.

Lösung.

- Die gesuchte Galoisgruppe $\text{Gal}_{\mathbb{Q}}(x_1, x_2)$ ist eine Teilmenge der symmetrischen Gruppe S_2 , die nur zwei Elemente enthält: die Identitätspermutation und die, die die beiden Ziffern vertauscht. Bei dieser Aufgabe geht also nur um die Frage, ob diese zweite Permutation σ in der Galoisgruppe enthalten ist oder nicht; mit Aufgabe 1c) kann man diese Frage schnell klären.

Erster Fall: Die Diskriminante ist ein Quadrat in \mathbb{Q} . Dann sind x_1 und x_2 rationale Zahlen. Da sie verschieden sind, sind sie nicht zueinander galoissch konjugiert. Nach Aufgabe 1c) kann σ daher nicht in der Galoisgruppe liegen.

Zweiter Fall: Die Diskriminante ist kein Quadrat in \mathbb{Q} . Dann ist $f(X)$ irreduzibel und somit das gemeinsame Minimalpolynom von x_1 und x_2 , die beiden Nullstellen sind also galoissch konjugiert. Nach Aufgabe 1c) muss die Galoisgruppe daher eine Permutation enthalten, die x_1 auf x_2 abbildet. Da die Identitätspermutation das nicht macht, muss noch die zweite Permutation σ enthalten sein.

- b) Die Galoisgruppe kann höchstens sechs Elemente enthalten, denn es gibt nur sechs Permutationen in drei Ziffern. Umgekehrt muss die Galoisgruppe aber auch mindestens sechs Elemente enthalten, denn

$$|\text{Gal}_{\mathbb{Q}}(x_1, x_2, x_3)| = [\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}(x_1)]}_{\geq 2} \cdot \underbrace{[\mathbb{Q}(x_1) : \mathbb{Q}]}_{=3} \geq 2 \cdot 3 = 6.$$

Die Abschätzung gilt deswegen, weil die einzig andere Option $[\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}(x_1)] = 1$ gleichbedeutend mit $\mathbb{Q}(x_1, x_2, x_3) = \mathbb{Q}(x_1)$ wäre, einem Widerspruch zur Voraussetzung.

Aufgabe 3. Kriterium für gerade Permutationen ???

- a) Zeige, dass die Menge A_n der geraden Permutationen in n Ziffern eine Untergruppe der S_n ist.
 b) Zeige, dass die Galoisgruppe der Nullstellen eines normierten separablen Polynoms $f(X)$ mit rationalen Koeffizienten genau dann vollständig in der alternierenden Gruppe A_n enthalten ist, wenn die Diskriminante von $f(X)$ eine Quadratwurzel in den rationalen Zahlen besitzt.

Lösung.

- a) ...
 b) Seien x_1, \dots, x_n die Nullstellen von $f(X)$. Wir betrachten eine der beiden Quadratwurzeln der Diskriminante,

$$\delta := \prod_{i < j} (x_i - x_j).$$

Diese Zahl liegt offensichtlich in $\mathbb{Q}(x_1, \dots, x_n)$. Außerdem sieht man, dass eine Permutation σ der Galoisgruppe genau dann δ invariant lässt (d. h. $\sigma \cdot \delta = \delta$ erfüllt), wenn σ gerade ist (sonst entsteht ein Minuszeichen).

Nun besitzt die Diskriminante genau dann eine Quadratwurzel in den rationalen Zahlen, wenn δ in \mathbb{Q} liegt [automatisch liegt dann auch $-\delta$ in \mathbb{Q}]. Das ist genau dann der Fall, wenn δ von allen Elementen der Galoisgruppe invariant gelassen wird. Nach obiger Überlegung ist das genau dann der Fall, wenn alle Elemente der Galoisgruppe gerade sind, wenn also die Galoisgruppe eine Teilmenge der alternierenden Gruppe A_n ist.

Aufgabe 4. ???

Sei $f(X)$ ein normiertes separables Polynom vom Grad n und t ein primitives Element seiner Nullstellen. Zeige, dass der Grad von t höchstens $n!$ ist.

Lösung. Wir wissen um die fundamentale Beobachtung, dass die Elemente der Galoisgruppe in Bijektion mit den galoissch Konjugierten von t stehen. Insbesondere enthält die Galoisgruppe also genau so viele Elemente, wie es galoissch Konjugierte von t gibt. Daher ist der Grad von t gerade durch die Anzahl der Elemente der Galoisgruppe gegeben. Diese ist höchstens $n!$, da es nur $n!$ Permutationen in n Ziffern gibt.

Aufgabe 5. Galoissche Resolventen

- a) Wieso ist das Konzept der galoisschen Resolvente nur für separable Polynome definiert worden?
- b) Finde eine galoissche Resolvente für das Polynom $f(X) = X^2 + X + 1$.
- c) Seien x_1, \dots, x_n die Nullstellen eines normierten separablen Polynoms $f(X)$ mit rationalen Koeffizienten. Sei C eine natürliche Zahl mit

$$n \cdot \left| \frac{x_i - x_j}{x_k - x_\ell} \right| \leq C$$

für alle $i, j, k, \ell \in \{1, \dots, n\}$ mit $k \neq \ell$. Zeige, dass

$$V(X_1, \dots, X_n) := X_1 + C X_2 + C^2 X_3 + \dots + C^{n-1} X_n$$

eine galoissche Resolvente für $f(X)$ ist.

Lösung.

- a) ...
- b) ...
- c) Seien σ und τ zwei verschiedene Permutationen. Wir müssen zeigen, dass $V(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \neq V(x_{\tau(1)}, \dots, x_{\tau(n)})$. Dafür wird es hilfreich sein, den größten Index $k \in \{1, \dots, n\}$ mit $\sigma(k) \neq \tau(k)$ zu betrachten. Nach Voraussetzung gilt Abschätzung

$$|x_{\sigma(i)} - x_{\tau(i)}| \leq |x_{\sigma(k)} - x_{\tau(k)}| \cdot \frac{1}{n} \cdot C$$

für alle $i = 1, \dots, n$. Damit ergibt sich:

$$\begin{aligned} |V(x_{\sigma(1)}, \dots, x_{\sigma(n)}) - V(x_{\tau(1)}, \dots, x_{\tau(n)})| &= \left| \sum_{i=1}^n (x_{\sigma(i)} - x_{\tau(i)}) \cdot C^{i-1} \right| \\ &= \left| \sum_{i=1}^k (x_{\sigma(i)} - x_{\tau(i)}) \cdot C^{i-1} \right| \\ &\geq |x_{\sigma(k)} - x_{\tau(k)}| \cdot C^{k-1} - \sum_{i=1}^{k-1} |x_{\sigma(i)} - x_{\tau(i)}| \cdot C^{i-1} \\ &\geq |x_{\sigma(k)} - x_{\tau(k)}| \cdot C^{k-1} - \sum_{i=1}^{k-1} |x_{\sigma(k)} - x_{\tau(k)}| \cdot \frac{1}{n} \cdot C \cdot C^{i-1} \\ &\geq |x_{\sigma(k)} - x_{\tau(k)}| \cdot C^{k-1} - |x_{\sigma(k)} - x_{\tau(k)}| \cdot \sum_{i=1}^{k-1} \frac{1}{n} \cdot C^{i-1} \\ &= |x_{\sigma(k)} - x_{\tau(k)}| \cdot C^{k-1} \cdot \left(1 - \frac{k-1}{n} \right) \\ &> 0. \end{aligned}$$