

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 $\sigma \cdot (zw) = (\sigma \cdot z) \cdot (\sigma \cdot w)$.
- 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 $\mathbb{Q}(x_1, \dots, x_n) = \mathbb{Q}[x_1, \dots, x_n]$ (die x_i sind algebraisch!) 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

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

sodass wir die Zahl $\sigma \cdot (z + w)$ durch Anwendung der Definition ausrechnen können:

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

der Multiplikationsfall geht völlig analog.

- „ \implies “: Sei m das Minimalpolynom von x_1 . Dann gilt

$$m(x_2) = m(\sigma \cdot x_1) = \sigma \cdot m(x_1) = \sigma \cdot 0 = 0,$$

also ist x_2 in der Tat galoissch konjugiert zu x_1 . Die Multiplikation mit σ darf man deswegen an m vorbeiziehen, weil m nur rationale Koeffizienten hat. Wenn man $m = \sum_i a_i X^i$ schreibt, kann man eine formale Begründung wie folgt führen:

$$m(\sigma \cdot x_2) = \sum_i a_i (\sigma \cdot x_2)^i = \sum_i (\sigma \cdot a_i) \cdot (\sigma \cdot x_2)^i = \sum_i \sigma \cdot (a_i x_2^i) = \sigma \cdot \sum_i a_i x_2^i = \sigma \cdot m(x_2).$$

„ \impliedby “: Wir kürzen die Galoisgruppe der Nullstellen kurz mit „ G “ ab. Dann betrachten wir das Polynom

$$g(X) := \prod_{\sigma \in G} (X - \sigma \cdot x_1).$$

Dieses ist sicher normiert und hat x_1 als Nullstelle. Außerdem sind seine Koeffizienten rational: Denn sie sind invariant unter der Wirkung der Galoisgruppe. Das folgt aus der für jedes $\tau \in G$ gültigen Beziehung

$$\tau \cdot g(X) = \tau \cdot \prod_{\sigma \in G} (X - \sigma \cdot x_1) = \prod_{\sigma \in G} (X - \tau \cdot \sigma \cdot x_1) = \prod_{\sigma \in G} (X - \sigma \cdot x_1) = g(X)$$

(wieso gilt diese?) und Koeffizientenvergleich.

Da nach Voraussetzung x_1 zu x_2 galoissch konjugiert ist, muss nach Aufgabe 4b) von Blatt 10 auch x_2 eine Nullstelle von $g(X)$ sein, einer der Faktoren

$$x_2 - \sigma \cdot x_1, \quad \sigma \in G,$$

muss also verschwinden. Das zeigt die Behauptung.

Bemerkung: Das betrachtete Polynom $g(X)$ wird im Allgemeinen nicht das Minimalpolynom von x_1 sein; das stört aber auch nicht weiter.

Aufgabe 2. Abstrakte Beispiele für Galoisgruppen

- Sei $f(X)$ ein normiertes *separables* quadratisches Polynom mit rationalen Koeffizienten. Berechne die Galoisgruppe der Nullstellen von $f(X)$ 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 Elemente 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.

Variante: Mit der Formel $|\text{Gal}_{\mathbb{Q}}(x_1, x_2)| = [\mathbb{Q}(x_1, x_2) : \mathbb{Q}]$ kann man die Fallunterscheidungen ein wenig kürzer fassen und muss auch nicht mehr Aufgabe 1c) kennen. Falls die Diskriminante ein Quadrat in \mathbb{Q} ist, sind die beiden Lösungen rational und es gilt einfach $\mathbb{Q}(x_1, x_2) = \mathbb{Q}$, also wird der Grad in diesem Fall 1 sein. Ansonsten wird der Grad mehr als 1 sein [tatsächlich genau 2], weswegen die Galoisgruppe dann noch das zweite Element enthalten muss.

- 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.

Bemerkung: Es kann auch nicht sein, dass x_2 oder x_3 primitive Elemente zu x_1, x_2, x_3 sind: Das folgt sofort aus Proposition 4.4 und ist konsistent mit der informalen Faustregel, dass galoissch Konjugierte dieselben algebraischen Eigenschaften haben sollten. [Diese darf man natürlich nicht zu wörtlich nehmen. Etwa können manche galoissch Konjugierten einer Zahl reell und manch andere echt komplex sein.]

Aufgabe 3. Manchmal sind alle Symmetrien gerade

- Zeige, dass die Menge A_n der geraden Permutationen in n Ziffern eine Untergruppe der S_n ist.
- 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.

- Die Identitätspermutation liegt in A_n , da sie gerade ist.

Seien σ und τ zwei Permutationen aus A_n , also zwei gerade Permutationen. Dann ist auch die Komposition $\sigma \circ \tau$ eine gerade Permutation (wieso?) und daher in A_n enthalten.

Sei schließlich σ eine Permutation aus A_n . Dann ist auch σ^{-1} eine gerade Permutation (wieso?), also in A_n enthalten.

Bemerkung: Wenn man das nötige abstrakte Vorwissen mitbringt, kann man auch wie folgt argumentieren: Die Signumsabbildung ist ein Gruppenhomomorphismus $S_n \rightarrow \{\pm 1\}$. Die Menge A_n ist daher als Kern dieses Homomorphismus eine Untergruppe.

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

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

Diese Zahl liegt offensichtlich in $\mathbb{Q}(x_1, \dots, x_n)$. Außerdem sieht man, dass wegen der vorausgesetzten Separabilität 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. Grad primitiver Elemente

Sei $f(X)$ ein normiertes separables Polynom vom Grad n und t ein primitives Element seiner Nullstellen.

- Zeige, dass jedes weitere primitive Element t' denselben Grad wie t hat.
- Zeige, dass der Grad von t höchstens $n!$ ist.
- Zeige, dass der Grad von t sogar ein Teiler von $n!$ ist.

Lösung.

- a) Nach Voraussetzung gilt $\mathbb{Q}(t) = \mathbb{Q}(x_1, \dots, x_n) = \mathbb{Q}(t')$. Daher folgt $\deg_{\mathbb{Q}} t = [\mathbb{Q}(t) : \mathbb{Q}] = [\mathbb{Q}(x_1, \dots, x_n) : \mathbb{Q}] = [\mathbb{Q}(t') : \mathbb{Q}] = \deg_{\mathbb{Q}} t'$.
- b) 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. Als Formel:

$$\deg_{\mathbb{Q}} t = |\text{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)| \leq |S_n| = n!.$$

Variante: Es gilt für jedes $k = 0, \dots, n-1$ die Abschätzung

$$[\mathbb{Q}(x_1, \dots, x_k, x_{k+1}) : \mathbb{Q}(x_1, \dots, x_k)] \leq n - k,$$

denn mit Polynomdivision über dem Rechenbereich $\mathbb{Q}(x_1, \dots, x_k)$ sieht man, dass sich das Polynom $f(X)$ über $\mathbb{Q}(x_1, \dots, x_k)$ aufspaltet als

$$f(X) = (X - x_1) \cdots (X - x_k) \cdot g_k(X)$$

für einen verbleibenden Faktor $g_k(X) \in \mathbb{Q}(x_1, \dots, x_k)[X]$ vom Grad $n - k$. Da $f(x_{k+1}) = 0$ und die anderen Nullstellen nicht gleich x_{k+1} sind, muss $g_k(x_{k+1})$ gelten, also ist $g_k(X)$ ein annullierendes Polynom für x_{k+1} über $\mathbb{Q}(x_1, \dots, x_k)$.

Damit gilt die Abschätzungskette

$$\begin{aligned} \deg_{\mathbb{Q}} t &= [\mathbb{Q}(t) : \mathbb{Q}] = [\mathbb{Q}(x_1, \dots, x_n) : \mathbb{Q}] \\ &= [\mathbb{Q}(x_1, \dots, x_n) : \mathbb{Q}(x_1, \dots, x_{n-1})] \cdots [\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)] \cdot [\mathbb{Q}(x_1) : \mathbb{Q}] \\ &\leq 1 \cdot 2 \cdots (n-1) \cdot n = n!. \end{aligned}$$

- c) Da die Galoisgruppe der Nullstellen eine Untergruppe der S_n ist, ist nach dem Satz von Lagrange $|\text{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)|$ ein Teiler von $|S_n| = n!$. Mit der Formel aus b) zeigt das schon die Behauptung.

Bemerkung: Die Variante für Teilaufgabe b) lässt sich nicht auf die stärkere Behauptung von Teilaufgabe c) übertragen.

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

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

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

Lösung.

- a) Eine galoissche Resolvente $V(X_1, \dots, X_n)$ für ein Polynom $f(X)$ mit den Nullstellen x_1, \dots, x_n ist ein Polynom, sodass für je zwei verschiedene Permutationen $\sigma, \tau \in S_n$ jeweils die Zahlen $V(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ und $V(x_{\tau(1)}, \dots, x_{\tau(n)})$ verschieden sind. Das ist aber unmöglich, wenn manche der Nullstellen übereinstimmen, d. h. wenn $x_i = x_j$ für $i \neq j$ gilt.
- b) *Variante 1 (durch Probieren):* Seien x_1 und x_2 die beiden (verschiedenen) Nullstellen von $X^2 + X + 1$. (Sie sind ω und ω^2 , wobei $\omega = \exp(2\pi i/3)$, aber das müssen wir für diese Aufgabe gar nicht wissen.) Dann ist etwa $V(X_1, X_2) := X_1$ eine galoissche Resolvente, denn in der Liste

σ	$V(x_{\sigma(1)}, x_{\sigma(2)})$
id	$V(x_1, x_2) = x_1$
$(1, 2)$	$V(x_2, x_1) = x_2$

kommt keine Zahl doppelt vor.

Bemerkung: Es stimmt also ganz allgemein, dass für quadratische Polynome $f(X) = X^2 + bX + c$ jede Nullstelle x_i schon ein primitives Element für $\mathbb{Q}(x_1, x_2)$ ist. Das kann man auch direkt sehen, denn es gilt $x_2 = -b - x_1$ und $x_1 = -b - x_2$ und daher $\mathbb{Q}(x_2) = \mathbb{Q}(x_1)$.

Variante 2 (mit der Technik aus der nächsten Teilaufgabe): Wir listen für alle $i, j, k, \ell \in \{1, 2\}$ mit $k \neq \ell$ die für Teilaufgabe c) relevanten Zahlen auf:

i	j	k	ℓ	$n \cdot x_i - x_j / x_k - x_\ell $
1	1	1	2	0
1	2	1	2	2
2	1	1	2	2
2	2	1	2	0
1	1	2	1	0
1	2	2	1	2
2	1	2	1	2
2	2	2	1	0

Wenn man nur kurz nachdenkt, kann man sich die meisten Kombinationen sogar sparen. Auf jeden Fall folgt, dass die Wahl $C := 2$ möglich ist und daher

$$x_1 + 2x_2$$

ein primitives Element ist.

- 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 für den Betrag $|\delta|$ der Differenz:

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