Musterlösung Serie 25

RADIKALERWEITERUNGEN UND AUFLÖSBARE GRUPPEN

---

123. Sei $L : K$ eine Radikalerweiterung in $\mathbb{C}$ und sei $\tilde{L}$ die normale Hülle von $L : K$.

Zeige: $\tilde{L} : K$ ist eine Radikalerweiterung.

Lösung: Sei $L = K(\alpha_1, \ldots, \alpha_m)$ wie in der Definition einer Radikalerweiterung, d.h. es existieren $\alpha_1, \ldots, \alpha_m$ und $n_1, \ldots, n_m \in \mathbb{N}$ mit $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$. Wir beweisen die Aussage mittels vollständiger Induktion nach m.

Sei zuerst $m = 1$, also $L = K(\alpha)$ mit $\alpha^n \in K$. Dann teilt das Minimalpolynom von α über K das Polynom $X^n - \alpha^n$. Also gilt für alle Nullstellen $a_1, \ldots, a_k$ des Minimalpolynoms von α über K, wobei $a_1 = \alpha$, ebenfalls $a_i^n \in K$, also ist $\tilde{L} = K(a_1, \ldots, a_k)$ mit jeweils $a_i^n \in K \subset K(a_1, \ldots, a_{i-1})$.

Sei nun die Aussage bewiesen für $m-1$. Sei $f \in K[X]$ das Minimalpolynom von α_m. Sei b eine weitere Nullstelle von f in $\tilde{L}$. Es genügt zu zeigen, dass b^{n_m} in der normalen Hülle $\tilde{L}_{m-1}$ der Körpererweiterung $K(\alpha_1, \ldots, \alpha_{m-1}) : K$ liegt. Sei $\sigma \in \mathrm{Gal}(\tilde{L} : K)$ mit $\sigma(\alpha_m) = b$. Dann ist $b^{n_m} = \sigma(\alpha_m)^{n_m} = \sigma(\alpha_m^{n_m})$. Da nun $\alpha_m \in \tilde{L}_{m-1}$, ist auch $\sigma(\alpha_m)^{n_m} = b^{n_m} \in \tilde{L}_{m-1}$ und wir sind fertig.

124. Sei $\zeta := e^{2\pi i/p}$ für eine ungerade Primzahl p.

(a) Zeige: $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. (*Hinweis:* Eisenstein-Kriterium.)

(b) Zeige: $\mathrm{Gal}\big(\mathbb{Q}(\xi) : \mathbb{Q}\big) \cong C_{p-1}$.

Lösung: (a) Es gilt $\zeta^p = 1$, also ist ζ eine Nullstelle des Polynoms $X^p - 1$. Aus der Zerlegung $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X + 1)$ folgt, dass ζ sogar eine Nullstelle des Polynoms $\Phi_p := X^{p-1} + \ldots + X + 1 \in \mathbb{Z}[X]$ ist. Wir wollen nun zeigen, dass Φ_p irreduzibel ist. Daraus wird folgen, dass Φ_p das Minimalpolynom von ζ "uber $\mathbb{Q}$ ist, und somit, dass $[\mathbb{Q}(\zeta)/\mathbb{Q}] = \deg \Phi_p = p - 1$ ist.

Die Irreduzibilit"at von Φ_p beweisen wir ähnlich wie in Aufgabe 87. Mit der Substitution $X \leftrightarrow Y + 1$ ist

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}.$$

Also ist $\Phi_p(Y)$ ein normiertes Polynom vom Grad $p - 1$, und der k-te Koeffizient ist $\binom{p}{k+1}$. Somit erfüllt $\Phi_p(Y)$ die Voraussetzungen des Eisenstein-Kriteriums für die Primzahl p, nämlich:

- Der höchste Koeffizient ist 1, also nicht durch p teilbar,

- für $0 \leqslant k \leqslant p-2$ ist $\binom{p}{k+1}$ durch p teilbar, also sind alle tieferen Koeffizienten durch p teilbar,
- der konstante Term ist $\binom{p}{1} = p$, also nicht durch p^2 teilbar.

(b) Die p-ten Einheitswurzeln bilden eine Gruppe, die isomorph zu C_p ist. Die Restriktion $\mathrm{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \to \mathrm{Aut}(\langle\xi\rangle), \sigma \mapsto \sigma|_{\langle\xi\rangle}$ ist wohldefiniert, da alle primitiven Einheitswurzeln nach (a) dasselbe Minimalpolynom haben, und injektiv, da ein Element der Galoisgruppe durch das Bild von ξ eindeutig festgelegt ist. Weiter wissen wir aus der Algebra I, dass $\mathrm{Aut}(C_p) \cong C_{p-1}$ ist. Somit haben $\mathrm{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})$ und $\mathrm{Aut}(\langle\xi\rangle)$ dieselbe Kardinalität und die Restriktion ist somit auch surjektiv, also ein Gruppenisomorphismus.

125. Zeige, dass die Nullstellen des Polynoms $X^5 - 6X + 3 \in \mathbb{Q}[X]$ nicht durch Radikale ausdrückbar sind.

Lösung: Das Polynom ist irreduzibel nach dem Schönemann-Eisenstein Kriterium mit der Primzahl 3. Ausserdem können wir mit Methoden der Analysis feststellen, dass das Polynom genau zwei nicht-reelle Nullstellen hat. Mit Proposition 21.8 ist die Galoisgruppe dieses Polynoms isomorph zu S_5. Da $A_5 \trianglelefteq S_5$ und $S_5/A_5 \cong C_2$, ist S_5/A_5 abelsch. Wäre S_5 auflösbar, so müsste mit Aufgabe 51 auch A_4 auflösbar sein – mit Aufgabe 49.(b) ist dies jedoch nicht der Fall (A_4 ist einfach und nicht-abelsch). Aus der Vorlesung folgt somit, dass keine Nullstelle des Polynoms durch Radikale auflösbar ist.

126. Sei $n \geqslant 5$ eine natürliche Zahl.

(a) Zeige, dass die Gruppe A_n einfach ist.
Hinweis: Sei $N \trianglelefteq A_n$ ein nichttrivialer Normalteiler. Zeige, dass N einen 3-Zykel der Form $ngn^{-1}g^{-1}$ mit $n \in N$ und $g \in A_n$ enthält.

(b) Folgere daraus, dass A_n die einzige normale Untergruppe von S_n ist.

Lösung: (a) Wir wissen aus der Algebra I, dass A_n von allen 3-Zykeln erzeugt ist, und auch, dass alle 3-Zykeln zueinander konjugiert sind. Wenn wir also beweisen können, dass N einen 3-Zykel enthält, dann enthält N alle 3-Zykeln und wir sind fertig.

Sei $n \in N$ ein nichttriviales Element. Schreibe $n = \sigma_1 \ldots \sigma_m$ als Produkt elementfremder Zyklen. Nun unterscheiden wir drei Fälle.

Fall 1: Einer der Zykeln hat Länge > 3.

Sei dieser Zykel $(a_1\, a_2\, \ldots\, a_l)$ mit $l > 3$. Sei $g = (a_1\, a_2\, a_3)$. Dann ist $ngn^{-1}g^{-1} = (a_1\, a_3\, a_2)$. Ausserdem ist dieses Element sicher in N, da wegen der Normalität $gn^{-1}g^{-1} \in N$ ist.

Fall 2: Einer der Zykel ist ein 3-Zykel und ein anderer Zykel ist ein 2- oder 3-Zykel.

Seien diese Zykeln $(a_1\, a_2\, a_3)$ und entweder $(b_1\, b_2)$ oder $(b_1\, b_2\, b_3)$. Sei $h = (a_1\, a_2\, b_1)$. Dann ist $nhn^{-1}h^{-1} = (a_1\, b_1\, a_3\, b_2\, a_2) \in N$ und wir sind im 1. Fall.

Fall 3: Alle Zyklen sind Transpositionen.

Da $n \in A_n$ ist, ist $k \geqslant 2$. Seien diese Zyklen $(a_1\, a_2)$ und $(b_1\, b_2)$. Sei $h = (a_1\, b_1\, c)$ für ein $c \notin \{i, j, k, l\}$. Dann ist

$$nhn^{-1}h^{-1} = \begin{cases} (a_1\, a_2\, b_2\, c\, b_1) & \text{falls } n(c) = c \\ (a_2\, b_2\, n(c))(a_1\, c\, b_1) & \text{falls } n(c) \neq c \end{cases}$$

und wir haben uns auf die vorigen Fälle reduziert.

(b) Sei $\{e\} \neq N \neq S_n$ eine normale Untergruppe. Dann ist $N \cap A_n \trianglelefteq A_n$. Da A_n einfach ist, gilt $N \cap A_n = \{e\}$ oder $N \supseteq A_n$.

Nehmen wir zuerst an, dass $N \supseteq A_n$ gilt. Wegen $2 = [S_n : A_n] = [S_n : N][N : A_n]$ muss daher $N = A_n$ gelten.

Sei nun $N \cap A_n = \{e\}$. Seien $g, h \in N \backslash A_n$ nicht notwendigerweise verschieden. Falls keine solchen g, h existieren, ist $N = \{e\}$ und wir sind fertig. Dann hat das Produkt von g und h Signum 1, liegt also in A_n, daher gilt $gh = e$. Insbesondere sind auch g^2 und h^2 in A_n, also gleich e. Es folgt $g = g^{-1} = h = h^{-1}$. Somit kann N nur ein einziges nichttriviales Element α haben, und dieses muss Ordnung 2 haben. Ausserdem muss $\sigma\alpha\sigma^{-1} = \alpha$ für jedes $\sigma \in S_n$ gelten. Das kann aber nicht sein.

127. (a) Zeige, dass für $n = 2, 3, 4$ die Gruppe S_n auflösbar ist.

(b) Zeige, dass für $n \geqslant 5$ die Gruppe S_n nicht auflösbar ist.

Lösung: (a) Für $n = 2$ ist die Gruppe bereits abelsch und $\{e\} \trianglelefteq S_2$ ist eine Normalreihe wie in der Definition.

Für $n = 3$ ist A_3 abelsch und $\{e\} \trianglelefteq A_2 \trianglelefteq S_3$ ist eine Normalreihe wie in der Definition.

Für $n = 4$ ist $\{e\} \trianglelefteq N \trianglelefteq A_4 \trianglelefteq S_4$ mit $N = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \cong C_2 \times C_2$ eine Subnormalreihe, denn $|A_4/N| = \frac{|A_3|}{|N|} = 3$ und alle Gruppen der Ordnung 3 sind abelsch.

(b) Nach Aufgabe 126.(b) ist A_n der einzige nichttriviale Normalteiler von S_n und noch dazu einfach. Also müsste eine Normalreihe mit $A_n \trianglelefteq S_n$ beginnen, kann aber nicht mehr weitergeführt werden.