

Musterlösung Serie 25

RADIKALERWEITERUNGEN UND AUFLÖSBARE GRUPPEN

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

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

Lösung: Sei $L = K(\alpha_1, \dots, \alpha_m)$ wie in der Definition einer Radikalerweiterung, d.h. es existieren $\alpha_1, \dots, \alpha_m$ und $n_1, \dots, n_m \in \mathbb{N}$ mit $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$. 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 $a_1, \dots, a_k$ des Minimalpolynoms von α über K , wobei $a_1 = \alpha$, ebenfalls $a_i^n \in K$, also ist $\tilde{L} = K(a_1, \dots, a_k)$ mit jeweils $a_i^n \in K \subset K(a_1, \dots, a_{i-1})$.

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 $K(\alpha_1, \dots, \alpha_{m-1}) : K$ liegt. Sei $\sigma \in \text{Gal}(\tilde{L} : K)$ 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.

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

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

(b) Zeigen Sie: $\text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \cong C_{p-1}$.

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

Die Irreduzibilität von Φ_p beweisen wir ähnlich wie in Aufgabe ???. 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 $0 \leq k \leq p-2$ 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 $\text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \rightarrow \text{Aut}(\langle \xi \rangle), \sigma \mapsto \sigma|_{\langle \xi \rangle}$ 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 $\text{Aut}(C_p) \cong C_{p-1}$ ist. Somit haben $\text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})$ und $\text{Aut}(\langle \xi \rangle)$ dieselbe Kardinalität und die Restriktion ist somit auch surjektiv, also ein Gruppenisomorphismus.

- 122.** Zeigen Sie, 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 33.(a) auch A_5 auflösbar sein – mit Lemma 7.10 ist dies jedoch nicht der Fall (A_5 ist einfach und nicht-abelsch). Aus der Vorlesung folgt somit, dass keine Nullstelle des Polynoms durch Radikale auflösbar ist.

- 123.** Sei G eine Gruppe und $N \trianglelefteq G$ eine normale Untergruppe.

- (a) Zeigen Sie: Die Gruppe G ist auflösbar, dann und nur dann falls N und G/N auflösbar sind.

Hinweis: Vergleichen Sie mit Aufgabe 33 (a) der Serie 5.

- (b) Sei G eine endliche Gruppe. Zeigen Sie: G ist genau dann auflösbar, falls eine Folge von Untergruppen $H_i \leq G$ existiert mit $\{e\} = H_0 \leq \dots \leq H_n = G$, sodass für all $0 \leq i \leq n-1$ gilt:

$$H_i \trianglelefteq H_{i+1} \quad \text{und} \quad H_{i+1}/H_i \text{ ist zyklisch der Ordnung } p_i \text{ für eine Primzahl } p_i.$$

Hinweis: Verwenden Sie den Hauptsatz über endlich erzeugte abelsche Gruppen.

Lösung:

- (a) Falls N und G/N auflösbar sind, dann wurde Auflösbarkeit von G in Aufgabe 33 (a) der Serie 5 bereits bewiesen.

Wir nehmen an, dass G auflösbar ist. Dann existieren Untergruppen

$$\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G,$$

so dass $G_i \trianglelefteq G_{i+1}$ und G_{i+1}/G_i ist abelsch für alle $0 \leq i < n$ gilt. Wir definieren $N_i := G_i \cap N$. Dies gibt eine Folge

$$\{e\} = N_0 \leq N_1 \leq \dots \leq N_n = N,$$

mit $N_i \trianglelefteq N_{i+1}$ für alle $0 \leq i < n$. Der natürliche Gruppenhomomorphismus

$$N_{i+1}/N_i \rightarrow G_{i+1}/G_i, \quad nN_i \mapsto nG_i$$

ist injektiv, denn sein Kern ist trivial. Also ist der Quotient N_{i+1}/N_i (isomorph zu einer) Untergruppe einer abelschen Gruppe. Diese Quotienten sind abelsch und somit ist N auflösbar. Dual hierzu definieren wir $M_i := G_i N$, dann erhalten wir eine Kette

$$N = M_0 \leq M_1 \leq \dots \leq M_n = G.$$

Sei $g \in M_i$. Dann existieren $g_1, \dots, g_k \in G_i$ und $n_1, \dots, n_k \in N$ mit

$$g = g_1 n_1 g_2 \dots g_k n_k.$$

Sei $x \in G_{i+1}$, dann gilt für jedes $1 \leq j \leq k$ die Relation $x g_j x^{-1} \in G_i$, weil G_i normal in G_{i+1} ist, und $x n_j x^{-1} \in N$, weil N normal in G ist. Für jedes $x \in N$ gilt $x g x^{-1} \in M_i$ weil $x \in N$. In beiden Fällen gilt $x g x^{-1} \in M_i$. Es folgt $M_i \trianglelefteq M_{i+1}$. Der natürliche Gruppenhomomorphismus

$$G_{i+1}/G_i \rightarrow M_{i+1}/M_i, \quad gG_i \mapsto gM_i$$

ist surjektiv. Also ist der Quotient M_{i+1}/M_i abelsch. Wir definieren $\tilde{M}_i := M_i/N$. Dies ist eine Kette von Untergruppen von G/N mit

$$\{e\} = \tilde{M}_0 \leq \tilde{M}_1 \leq \dots \leq \tilde{M}_n = G/N.$$

Die Relation $M_i \trianglelefteq M_{i+1}$ impliziert $\tilde{M}_i \trianglelefteq \tilde{M}_{i+1}$. Nach dem dritten Isomorphiesatz haben wir einen Isomorphismus

$$M_{i+1}/M_i \cong \tilde{M}_{i+1}/\tilde{M}_i.$$

Also sind diese Quotienten abelsch. Folglich ist G/N auflösbar.

- (b) Falls eine solche Folge von Untergruppen existiert, dann ist die Gruppe auflösbar, weil sie die Definition einer auflösbaren Gruppe erfüllt.

Sei A eine endliche, abelsche, nicht-triviale Gruppe. Nach dem Hauptsatz über endlich erzeugte, abelsche Gruppen, existieren $k \geq 1$ und $n_1, \dots, n_k > 1$ mit

$$A \cong \bigoplus_{i=1}^k \mathbb{Z}/n_i \mathbb{Z}.$$

Sei p eine Primzahl mit $p|n_1$. Wir betrachten die Gruppe

$$B_1 := p\mathbb{Z}/n_1\mathbb{Z}.$$

Nun definieren wir die Untergruppe $B \leq A$ als

$$B := \{(x_1, \dots, x_k) \in A : x_1 \in B_1\}.$$

Es gilt $A/B \cong \mathbb{Z}/p\mathbb{Z}$. Dieser Isomorphismus erhält man durch die Projektion auf die erste Koordinate. Zusammenfassend haben wir bewiesen: für jede endliche, abelsche, nicht-triviale Gruppe A existiert eine Untergruppe $B \leq A$, so dass die Ordnung von A/B eine Primzahl ist.

Wir lösen die Aufgabe nun mit Induktion über die Anzahl Primfaktoren von $N := |G|$. Falls N nur einen Primfaktor hat, dann gilt $N = 1$. In diesem Fall gilt die Aussage. Wir nehmen nun an N hat $n + 1$ Primfaktoren und die Aussage sei bereits für alle auflösbaren Gruppen, deren Ordnung n Primfaktoren hat, bewiesen. Da G auflösbar ist, existiert eine nicht-triviale, normale Untergruppe $N \leq G$, so dass G/N abelsch ist. Also existiert nach der obigen Aussage eine normale Untergruppe $\tilde{H} \trianglelefteq G/N$, so dass die Ordnung von $(G/N)/\tilde{H}$ eine Primzahl ist. Nun existiert eine Untergruppe $N \trianglelefteq H \trianglelefteq G$ mit $\tilde{H} = H/N$ und die Ordnung von G/H ist eine Primzahl, also ist dies eine zyklische Gruppe und die Ordnung von H hat n Primfaktoren. Nach Aufgabe (a) ist H auflösbar. Nun existieren nach Induktionsannahme Untergruppen $\{e\} = H_0 \leq \dots \leq H_n = H$, so dass für alle $0 \leq i < n$ die Relation $H_i \trianglelefteq H_{i+1}$ gilt und H_{i+1}/H_i abelsch ist. Wir setzen $G_i := H_i$ für alle $0 \leq i \leq n$ und $G_{n+1} := G$. Dann erfüllt die Folge G_i die Annahmen der Aufgabe.

- 124.** (a) Zeigen Sie, dass für $n = 2, 3, 4$ die Gruppe S_n auflösbar ist.
 (b) Zeigen Sie, dass für $n \geq 5$, A_n die einzige normale Untergruppe von S_n ist.
 (c) Zeigen Sie, dass für $n \geq 5$ 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 $N = \{e, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$ eine Subnormalreihe, denn $|A_4/N| = \frac{|A_3|}{|N|} = 3$ und alle Gruppen der Ordnung 3 sind abelsch.

(b) 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 $g, h \in N \setminus A_n$ 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.

(c) Mit Aufgabe (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.