Auflösbarkeit von algebraischen Gleichungen

Stephan Ehlen

30. Januar 2019

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät

Universität zu Köln

Auflösbarkeit durch Radikale

Im Folgenden haben alle Körper die Charakterisitk 0 (wenn nicht anders erwähnt).

Definition 1

Eine endliche Körpererweiterung L/K heißt **durch Radikale** *auflösbar*, falls es einen Erweiterungskörper E/L sowie eine endliche Kette von Körpererweiterungen

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

gibt, so dass E_{i+1} aus E_i jeweils durch *Adjunktion einer Wurzel* entsteht, d.h. $E_{i+1} = E_i(\alpha_i)$, wobei es ein $n_i \in \mathbb{N}$ gibt, so dass

$$\alpha_i^{n_i} \in E_i$$

gilt. Ist L der Zerfällungskörper eines Polynoms $f \in K[X]$, so sagt man entsprechend, dass sich die algebraische Gleichung $f(x) = 0$ durch Radikale auflösen lässt.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbarkeit durch Radikale

Im Folgenden haben alle Körper die Charakterisitk 0 (wenn nicht anders erwähnt).

Definition 1

Eine endliche Körpererweiterung L/K heißt **durch Radikale** *auflösbar*, falls es einen Erweiterungskörper E/L sowie eine endliche Kette von Körpererweiterungen

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

gibt, so dass E_{i+1} aus E_i jeweils durch *Adjunktion einer Wurzel* entsteht, d.h. $E_{i+1} = E_i(\alpha_i)$, wobei es ein $n_i \in \mathbb{N}$ gibt, so dass

$$\alpha_i^{n_i} \in E_i$$

gilt. Ist L der Zerfällungskörper eines Polynoms $f \in K[X]$, so sagt man entsprechend, dass sich die algebraische Gleichung $f(x) = 0$ durch Radikale auflösen lässt.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbare Erweiterungen

Definition 2

Eine endliche Körpererweiterung L/K heißt *auflösbar*, falls es eine Erweiterung E/L gibt, so dass E/K eine endliche Galoiserweiterung ist und die Galoisgruppe $\mathrm{Gal}(E/K)$ auflösbar ist.

Definition 3

Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

besitzt, in der alle Faktoren G_i/G_{i-1} abelsch sind.

1. Beispiel: Wir haben gesehen, dass p-Gruppen auflösbar sind.
2. Beispiel: Die symmetrische Gruppe S_5 ist nicht auflösbar (Beweis ist im Skript enthalten).
3. Fakt: Die Erweiterung L/K ist genau dann durch Radikale auflösbar ist, wenn L/K auflösbar ist.
4. Anwendung: Nutze dann Galoistheorie und Gruppentheorie, um die Auflösbarkeit genauer zu untersuchen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbare Erweiterungen

Definition 2

Eine endliche Körpererweiterung L/K heißt *auflösbar*, falls es eine Erweiterung E/L gibt, so dass E/K eine endliche Galoiserweiterung ist und die Galoisgruppe $\mathrm{Gal}(E/K)$ auflösbar ist.

Definition 3

Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

besitzt, in der alle Faktoren G_i/G_{i-1} abelsch sind.

1. Beispiel: Wir haben gesehen, dass p-Gruppen auflösbar sind.
2. Beispiel: Die symmetrische Gruppe S_5 ist *nicht* auflösbar (Beweis ist im Skript enthalten).
3. **Fakt**: Die Erweiterung L/K ist genau dann durch Radikale auflösbar ist, wenn L/K auflösbar ist.
4. Anwendung: Nutze dann Galoistheorie und Gruppentheorie, um die Auflösbarkeit genauer zu untersuchen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbare Erweiterungen

Definition 2

Eine endliche Körpererweiterung L/K heißt *auflösbar*, falls es eine Erweiterung E/L gibt, so dass E/K eine endliche Galoiserweiterung ist und die Galoisgruppe $\mathrm{Gal}(E/K)$ auflösbar ist.

Definition 3

Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

besitzt, in der alle Faktoren G_i/G_{i-1} abelsch sind.

1. Beispiel: Wir haben gesehen, dass p-Gruppen auflösbar sind.
2. Beispiel: Die symmetrische Gruppe S_5 ist *nicht* auflösbar (Beweis ist im Skript enthalten).
3. **Fakt**: Die Erweiterung L/K ist genau dann durch Radikale auflösbar ist, wenn L/K auflösbar ist.
4. Anwendung: Nutze dann Galoistheorie und Gruppentheorie, um die Auflösbarkeit genauer zu untersuchen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbare Erweiterungen

Definition 2

Eine endliche Körpererweiterung L/K heißt *auflösbar*, falls es eine Erweiterung E/L gibt, so dass E/K eine endliche Galoiserweiterung ist und die Galoisgruppe $\mathrm{Gal}(E/K)$ auflösbar ist.

Definition 3

Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

besitzt, in der alle Faktoren G_i/G_{i-1} abelsch sind.

1. Beispiel: Wir haben gesehen, dass p-Gruppen auflösbar sind.
2. Beispiel: Die symmetrische Gruppe S_5 ist *nicht* auflösbar (Beweis ist im Skript enthalten).
3. **Fakt**: Die Erweiterung L/K ist genau dann durch Radikale auflösbar ist, wenn L/K auflösbar ist.
4. Anwendung: Nutze dann Galoistheorie und Gruppentheorie, um die Auflösbarkeit genauer zu untersuchen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbare Erweiterungen

Definition 2

Eine endliche Körpererweiterung L/K heißt *auflösbar*, falls es eine Erweiterung E/L gibt, so dass E/K eine endliche Galoiserweiterung ist und die Galoisgruppe $\mathrm{Gal}(E/K)$ auflösbar ist.

Definition 3

Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

besitzt, in der alle Faktoren G_i/G_{i-1} abelsch sind.

1. Beispiel: Wir haben gesehen, dass p-Gruppen auflösbar sind.
2. Beispiel: Die symmetrische Gruppe S_5 ist *nicht* auflösbar (Beweis ist im Skript enthalten).
3. **Fakt**: Die Erweiterung L/K ist genau dann durch Radikale auflösbar ist, wenn L/K auflösbar ist.
4. Anwendung: Nutze dann Galoistheorie und Gruppentheorie, um die Auflösbarkeit genauer zu untersuchen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbare Erweiterungen

Definition 2

Eine endliche Körpererweiterung L/K heißt *auflösbar*, falls es eine Erweiterung E/L gibt, so dass E/K eine endliche Galoiserweiterung ist und die Galoisgruppe $\mathrm{Gal}(E/K)$ auflösbar ist.

Definition 3

Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

besitzt, in der alle Faktoren G_i/G_{i-1} abelsch sind.

1. Beispiel: Wir haben gesehen, dass p-Gruppen auflösbar sind.
2. Beispiel: Die symmetrische Gruppe S_5 ist *nicht* auflösbar (Beweis ist im Skript enthalten).
3. **Fakt**: Die Erweiterung L/K ist genau dann durch Radikale auflösbar ist, wenn L/K auflösbar ist.
4. Anwendung: Nutze dann Galoistheorie und Gruppentheorie, um die Auflösbarkeit genauer zu untersuchen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Sei $G \subset S_5$ die Galoisgruppe von P.
Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Sei $G \subset S_5$ die Galoisgruppe von P.
Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Sei $G \subset S_5$ die Galoisgruppe von P.
Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Sei $G \subset S_5$ die Galoisgruppe von P.
Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Sei $G \subset S_5$ die Galoisgruppe von P.
Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen 5. Grades

Lemma 4

Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5. Grades, welches 3 reelle und 2 komplexe Nullstellen besitze. Dann ist die Galoisgruppe von P isomorph zur vollen Permutationsgruppe S_5.

Beweis.

Sei $G \subset S_5$ die Galoisgruppe von P.
Komplexe Konjugation $\tau \in G$ vertauscht die beiden komplexen Nullstellen und hält die reellen Nullstellen fest.
G operiert transitiv auf den Nullstellen von P; deshalb: nach der Bahnformel gilt $5 \mid |G|$.
Cauchy: es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$.
Die Elemente τ und σ erzeugen die Gruppe S_5. (S_5 wird von einer beliebigen Transposition und einem 5-er Zykel erzeugt). □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5\sqrt[4]{5}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen, die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5\sqrt[4]{5}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen, die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel

Die allgemeine Gleichung 5. Grades

Wir wollen zeigen, dass die allgemeine Gleichung 5. Grades nicht (durch Radikale) auflösbar ist. Wäre sie auflösbar, so wäre jede Gleichung 5. Grades auflösbar, z.B. sei $f(X) := X^5 - 16X + 2 \in \mathbb{Q}[X]$.

1. $g(X) := X^5 - 16X$
2. $g'(X) = 5(X^4 - \frac{16}{5})$
3. Nullstellen von g' sind bei $\pm\sqrt[4]{\frac{16}{5}} = \pm\frac{2}{\sqrt[4]{5}}$
4. 2. Ableitung ist ungleich 0 an diesen Stellen, also Extrema.
5. Die Werte von g an diesen Stellen sind $\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) < 0$ sowie $-\frac{32}{\sqrt[4]{5}}(\frac{1}{5} - 1) > 0$ und betraglich $|\frac{128}{5^{5/4}}| > \frac{128}{25} > 5 > 2$.
6. Damit hat f genau 3 reelle Nullstellen; die anderen beiden müssen komplex sein.
7. Außerdem ist f irreduzibel nach dem Eisenstein-Kriterium ($p = 2$).
8. Damit ist also die Galoisgruppe von f die volle S_5.
9. Die Gruppe S_5 ist nicht auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Etwas lineare Algebra

Satz 1

Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum, $f \in \mathrm{End}(V)$ sowie $P \in K[X]$ ein normiertes Polynom ohne mehrfache Nullstellen, welches über K vollständig in Linearfaktoren zerfällt mit $P(f) = 0$. Dann ist f über K diagonalisierbar und die Eigenwerte von f sind Nullstellen von P.

Beweis.

Nach dem Chinesischen Restsatz erhalten wir einen Isomorphismus

$$\varphi : K[X]/(P) \to K[X]/(X - \lambda_1) \times \ldots \times K[X]/(X - \lambda_r).$$

Sei $a_j \in K[X]$, so dass $\varphi(a_j + P) = (0, \ldots, 1, \ldots, 0)$, wobei die 1 an der j-ten Stelle steht woraus $\varphi(\sum_j a_j) = (1, 1, \ldots, 1)$ und $\sum_j a_j + (P) = 1 + (P)$ folgt. Sei $v \in V$. Dann ist $\sum_{j=0}^{r} a_j(f)(v) = v$ eine Zerlegung von v in Eigenvektoren von f, denn: $(X - \lambda_j)a_j(X) \in (P)$, d.h. $(f - \lambda_j \mathrm{id}_V) \circ a_j(f) = 0$, also, für alle $v \in V$ ist $f(a_j(f)(v)) = \lambda_j \cdot a_j(f)(v)$. Damit ist f diagonalisierbar und die Eigenwerte sind die λ_j. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Etwas lineare Algebra

Satz 1

Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum, $f \in \mathrm{End}(V)$ sowie $P \in K[X]$ ein normiertes Polynom ohne mehrfache Nullstellen, welches über K vollständig in Linearfaktoren zerfällt mit $P(f) = 0$. Dann ist f über K diagonalisierbar und die Eigenwerte von f sind Nullstellen von P.

Beweis.

Schreibe $P(X) = (X - \lambda_1) \cdots (X - \lambda_r)$. Nach dem Chinesischen Restsatz erhalten wir einen Isomorphismus

$$\varphi : K[X]/(P) \to K[X]/(X - \lambda_1) \times \ldots \times K[X]/(X - \lambda_r).$$

Sei $a_j \in K[X]$, so dass $\varphi(a_j + P) = (0, \ldots, 1, \ldots, 0)$, wobei die 1 an der j-ten Stelle steht woraus $\varphi(\sum_j a_j) = (1, 1, \ldots, 1)$ und $\sum_j a_j + (P) = 1 + (P)$ folgt. Sei $v \in V$. Dann ist $\sum_{j=0}^{r} a_j(f)(v) = v$ eine Zerlegung von v in Eigenvektoren von f, denn: $(X - \lambda_j)a_j(X) \in (P)$, d.h. $(f - \lambda_j \mathrm{id}_V) \circ a_j(f) = 0$, also, für alle $v \in V$ ist $f(a_j(f)(v)) = \lambda_j \cdot a_j(f)(v)$. Damit ist f diagonalisierbar und die Eigenwerte sind die λ_j. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Etwas lineare Algebra

Satz 1

Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum, $f \in \mathrm{End}(V)$ sowie $P \in K[X]$ ein normiertes Polynom ohne mehrfache Nullstellen, welches über K vollständig in Linearfaktoren zerfällt mit $P(f) = 0$. Dann ist f über K diagonalisierbar und die Eigenwerte von f sind Nullstellen von P.

Beweis.

Schreibe $P(X) = (X - \lambda_1) \cdots (X - \lambda_r)$. Nach dem Chinesischen Restsatz erhalten wir einen Isomorphismus

$$\varphi : K[X]/(P) \to K[X]/(X - \lambda_1) \times \ldots \times K[X]/(X - \lambda_r).$$

Sei $a_j \in K[X]$, so dass $\varphi(a_j + P) = (0, \ldots, 1, \ldots, 0)$, wobei die 1 an der j-ten Stelle steht woraus $\varphi(\sum_j a_j) = (1, 1, \ldots, 1)$ und $\sum_j a_j + (P) = 1 + (P)$ folgt. Sei $v \in V$. Dann ist $\sum_{j=0}^{r} a_j(f)(v) = v$ eine Zerlegung von v in Eigenvektoren von f, denn: $(X - \lambda_j)a_j(X) \in (P)$, d.h. $(f - \lambda_j \mathrm{id}_V) \circ a_j(f) = 0$, also, für alle $v \in V$ ist $f(a_j(f)(v)) = \lambda_j \cdot a_j(f)(v)$. Damit ist f diagonalisierbar und die Eigenwerte sind die λ_j. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Etwas lineare Algebra

Satz 1

Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum, $f \in \mathrm{End}(V)$ sowie $P \in K[X]$ ein normiertes Polynom ohne mehrfache Nullstellen, welches über K vollständig in Linearfaktoren zerfällt mit $P(f) = 0$. Dann ist f über K diagonalisierbar und die Eigenwerte von f sind Nullstellen von P.

Beweis.

Schreibe $P(X) = (X - \lambda_1) \cdots (X - \lambda_r)$. Nach dem Chinesischen Restsatz erhalten wir einen Isomorphismus

$$\varphi : K[X]/(P) \to K[X]/(X - \lambda_1) \times \ldots \times K[X]/(X - \lambda_r).$$

Sei $a_j \in K[X]$, so dass $\varphi(a_j + P) = (0, \ldots, 1, \ldots, 0)$, wobei die 1 an der j-ten Stelle steht woraus $\varphi(\sum_j a_j) = (1, 1, \ldots, 1)$ und $\sum_j a_j + (P) = 1 + (P)$ folgt. Sei $v \in V$. Dann ist $\sum_{j=0}^{r} a_j(f)(v) = v$ eine Zerlegung von v in Eigenvektoren von f, denn: $(X - \lambda_j)a_j(X) \in (P)$, d.h. $(f - \lambda_j \mathrm{id}_V) \circ a_j(f) = 0$, also, für alle $v \in V$ ist $f(a_j(f)(v)) = \lambda_j \cdot a_j(f)(v)$. Damit ist f diagonalisierbar und die Eigenwerte sind die λ_j. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Etwas lineare Algebra

Satz 1

Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum, $f \in \mathrm{End}(V)$ sowie $P \in K[X]$ ein normiertes Polynom ohne mehrfache Nullstellen, welches über K vollständig in Linearfaktoren zerfällt mit $P(f) = 0$. Dann ist f über K diagonalisierbar und die Eigenwerte von f sind Nullstellen von P.

Beweis.

Schreibe $P(X) = (X - \lambda_1) \cdots (X - \lambda_r)$. Nach dem Chinesischen Restsatz erhalten wir einen Isomorphismus

$$\varphi : K[X]/(P) \to K[X]/(X - \lambda_1) \times \ldots \times K[X]/(X - \lambda_r).$$

Sei $a_j \in K[X]$, so dass $\varphi(a_j + P) = (0, \ldots, 1, \ldots, 0)$, wobei die 1 an der j-ten Stelle steht woraus $\varphi(\sum_j a_j) = (1, 1, \ldots, 1)$ und $\sum_j a_j + (P) = 1 + (P)$ folgt. Sei $v \in V$. Dann ist $\sum_{j=0}^{r} a_j(f)(v) = v$ eine Zerlegung von v in Eigenvektoren von f, denn: $(X - \lambda_j)a_j(X) \in (P)$, d.h. $(f - \lambda_j \mathrm{id}_V) \circ a_j(f) = 0$, also, für alle $v \in V$ ist $f(a_j(f)(v)) = \lambda_j \cdot a_j(f)(v)$. Damit ist f diagonalisierbar und die Eigenwerte sind die λ_j. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Definition 5

Eine Galoiserweiterung mit zyklischer Galoisgruppe heißt *zyklische Erweiterung*.

Satz 2

Sei K ein Körper und $n \geq 2$ eine natürliche Zahl, so dass K alle n-ten Einheitswurzeln enthalte (d.h. $X^n - 1$ zerfällt über K in Linearfaktoren). Außerdem sei $\mathrm{char}(K)$ *kein Teiler von n. Es gelten:*

1. *Ist L/K eine zyklische Erweiterung vom Grad n, so ist $L = K(\alpha)$ mit $\alpha^n \in K$, d.h. L entsteht aus K durch Adjunktion einer n-ten Wurzel.*
2. *Ist $L = K(\alpha)$ mit $\alpha^n \in K$, so ist L/K eine zyklische Erweiterung, deren Grad n teilt.*

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Definition 5

Eine Galoiserweiterung mit zyklischer Galoisgruppe heißt *zyklische Erweiterung*.

Satz 2

Sei K ein Körper und $n \geq 2$ eine natürliche Zahl, so dass K alle n-ten Einheitswurzeln enthalte (d.h. $X^n - 1$ zerfällt über K in Linearfaktoren). Außerdem sei $\mathrm{char}(K)$ *kein Teiler von n. Es gelten:*

1. *Ist L/K eine zyklische Erweiterung vom Grad n, so ist $L = K(\alpha)$ mit $\alpha^n \in K$, d.h. L entsteht aus K durch Adjunktion einer n-ten Wurzel.*
2. *Ist $L = K(\alpha)$ mit $\alpha^n \in K$, so ist L/K eine zyklische Erweiterung, deren Grad n teilt.*

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Definition 5

Eine Galoiserweiterung mit zyklischer Galoisgruppe heißt *zyklische Erweiterung*.

Satz 2

Sei K ein Körper und $n \geq 2$ eine natürliche Zahl, so dass K alle n-ten Einheitswurzeln enthalte (d.h. $X^n - 1$ zerfällt über K in Linearfaktoren). Außerdem sei $\mathrm{char}(K)$ *kein Teiler von n. Es gelten:*

1. *Ist L/K eine zyklische Erweiterung vom Grad n, so ist $L = K(\alpha)$ mit $\alpha^n \in K$, d.h. L entsteht aus K durch Adjunktion einer n-ten Wurzel.*
2. *Ist $L = K(\alpha)$ mit $\alpha^n \in K$, so ist L/K eine zyklische Erweiterung, deren Grad n teilt.*

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Zyklische Erweiterungen

Beweis.

Wir beweisen hier nur den ersten Punkt. Sei L/K zyklisch vom Grad n.
Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
Für $P(X) = X^n - 1$ ist $P(\sigma) = 0$. Da P über K in paarweise verschiedene Linearfaktoren zerfällt, ist σ also diagonalisierbar.
Die Eigenwerte von σ sind also n-te Einheitswurzeln.
Die Eigenwerte bilden sogar einer Untergruppe U von $K^\times$:
sind ζ und η zwei Eigenwerte mit Eigenvektoren α, β, so ist $\alpha\beta$ Eigenvektor mit Eigenwert $\zeta\eta$.
Es ist $|U| = n$, denn sonst wäre $\sigma^m = 1$ für einen echten Teiler von n.
Sei also ζ_n eine primitive n-te Einheitswurzel. Dann gibt es $\alpha \in L$ mit $\sigma(\alpha) = \zeta_n\alpha$. Damit sind die n Potenzen $1 = \alpha^0, \ldots, \alpha^{n-1}$ linear unabhängig als Eigenvektoren zu den verschiedenen Eigenwerten $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$.
Also ist $L = K(\alpha)$ und außerdem $\alpha^n = \sigma(\alpha^n)$ und somit $\alpha^n \in K$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Prime Wurzeln

Korollar 1

Sei K ein Körper und $p \neq \mathrm{char}(K)$ eine Primzahl. K enthalte alle p-ten Einheitswurzeln. Dann ist L/K genau dann eine echte Galoiserweiterung vom Grad p, wenn L aus K durch Adjunktion einer (nicht in K enthaltenen) p-ten Wurzel entsteht.

Beweis.

Eine Galoiserweiterung vom Grad p ist immer zyklisch. Damit entsteht sie also (da K die p-ten Einheitswurzeln enthält) durch Adjunktion einer p-ten Wurzel aus K.
Umgekehrt liefert die Adjunktion einer p-ten Wurzel eine Galoiserweiterung, deren Grad ein Teiler von p ist. Ist diese nicht trivial, so hat sie also Grad p. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Translationssatz

Definition 6

Sei M ein Körper und K, L seien zwei Teilkörper. Dann bezeichen wir mit $KL \subset M$ den von K und L erzeugten Teilkörper von M, das sogenannte *Kompositum* von K und L.

Satz 3 (Translationssatz)

Sei M ein Körper und $K, L \subset M$ Teilkörper. Es sei $L/(K \cap L)$ eine endliche Galoiserweiterung. Dann ist auch KL/K eine endliche Galoiserweiterung und es wir erhalten einen Isomorphismus (durch Restriktion)

$$\mathrm{Gal}(KL/K) \cong \mathrm{Gal}(L/(K \cap L)).$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Translationssatz

Satz 3 (Translationssatz)

Sei M ein Körper und $K, L \subset M$ Teilkörper. Es sei $L/(K \cap L)$ eine endliche Galoiserweiterung. Dann ist auch KL/K eine endliche Galoiserweiterung und es wir erhalten einen Isomorphismus (durch Restriktion)

$$\mathrm{Gal}(KL/K) \cong \mathrm{Gal}(L/(K \cap L)).$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Translationssatz

Satz 3 (Translationssatz)

Sei M ein Körper und $K, L \subset M$ Teilkörper. Es sei $L/(K \cap L)$ eine endliche Galoiserweiterung. Dann ist auch KL/K eine endliche Galoiserweiterung und es wir erhalten einen Isomorphismus (durch Restriktion)

$$\mathrm{Gal}(KL/K) \cong \mathrm{Gal}(L/(K \cap L)).$$

Beweis.

Klar: KL/K ist eine endliche Galoiserweiterung: 1) sie ist separabel, denn ein Erzeuger von $L/K \cap L$ erzeugt auch KL/K und 2) ist L über $K \cap L$ Zerfällungskörper von $f \in K \cap L[X]$, so ist f insbesondere in $K[X]$ und KL Zerfällungskörper von f über K.
Die Abbildung $\mathrm{Gal}(KL/K) \to \mathrm{Gal}(L/K \cap L)$ gegeben durch $\sigma \mapsto \sigma\,|_L$ ist injektiv. Der Fixkörper des Bildes ist $L \cap K$ und damit ist die Abbildung auch surjektiv. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Translationssatz

Korollar 2

Sei M ein Körper und $S \subset T \subset M$ sowie $K \subset M$ Teilkörper wobei T/S eine endliche Galoiserweiterung sei, so ist TK/SK ebenfalls eine endliche Galoiserweiterung und die Restriktion liefert eine Injektion von Galoisgruppen:

$$\mathrm{Gal}(TK/SK) \hookrightarrow \mathrm{Gal}(T/S).$$

Beweis.

Es ist $T/T \cap SK$ eine Galoiserweiterung, denn $T \cap SK$ ist ein Zwischenkörper von T/S. Nach dem Translationssatz ist dann auch TK/SK eine Galoiserweiterung mit Galoisgruppe isomorph zu $\mathrm{Gal}(T/T \cap SK) \subset \mathrm{Gal}(T/S)$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbarkeit

Satz 4

Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Beweis.

Sei L/K auflösbar.
OBdA ist L/K eine Galoiserweiterung und $G := \mathrm{Gal}(L/K)$ auflösbar.
Es existiert also eine echt absteigende Normalreihe

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$$

von G mit zyklischen Faktoren G_j/G_{j+1} von Primzahlordnung (Satz 5.9 (i)).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbarkeit

Satz 4

Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Beweis.

Sei L/K auflösbar.
OBdA ist L/K eine Galoiserweiterung und $G := \mathrm{Gal}(L/K)$ auflösbar.
Es existiert also eine echt absteigende Normalreihe

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$$

von G mit zyklischen Faktoren G_j/G_{j+1} von Primzahlordnung (Satz 5.9 (i)).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbarkeit

Satz 4

Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Beweis.

Sei L/K auflösbar.
OBdA ist L/K eine Galoiserweiterung und $G := \mathrm{Gal}(L/K)$ auflösbar.
Es existiert also eine echt absteigende Normalreihe

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$$

von G mit zyklischen Faktoren G_j/G_{j+1} von Primzahlordnung (Satz 5.9 (i)).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Auflösbarkeit

Satz 4

Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Beweis.

Sei L/K auflösbar.
OBdA ist L/K eine Galoiserweiterung und $G := \mathrm{Gal}(L/K)$ auflösbar.
Es existiert also eine echt absteigende Normalreihe

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$$

von G mit zyklischen Faktoren G_j/G_{j+1} von Primzahlordnung (Satz 5.9 (i)).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

die entsprechende Kette der Zwischenkörper nach dem Hauptsatz der Galoistheorie.

Hierbei ist jeweils K_{j+1}/K_j eine Galoiserweiterung und der Grad $[K_{j+1} : K_j]$ is eine Primzahl.

Galois sieht man so: Es ist L/K_j galois mit Galoisgruppe G_j. Da $G_{j+1} \subset G_j$ ein Normalteiler ist, ist $K_{j+1} = L^{G_{j+1}}$ auch galois über K_j. Es ist

$\mathrm{Gal}(K_{j+1}/K_j) \cong G_{j+1}/G_j$

Sei z eine primitive $|G|$-te Einheitswurzel.

Ersetzen wir die Kette durch

$$K_0(z) \subset K_1(z) \subset \ldots \subset K_r(z) = L(z),$$

so erhalten wir nach dem Translationssatz eine neue Kette von Galoiserweiterungen von Primzahlgrad.

Da $K_j(z)$ für $p \mid |G|$ alle p-ten Einheitswurzeln enthält, entstehen die jeweiligen Erweiterungen nach Korollar 1 durch Adjunktion einer p-ten Wurzel. Damit ist $L(z)$ und damit $L \subset L(z)$ durch Radikale auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

die entsprechende Kette der Zwischenkörper nach dem Hauptsatz der Galoistheorie.
Hierbei ist jeweils K_{j+1}/K_j eine Galoiserweiterung und der Grad $[K_{j+1} : K_j]$ is eine Primzahl.
Galois sieht man so: Es ist L/K_j galois mit Galoisgruppe G_j. Da $G_{j+1} \subset G_j$ ein Normalteiler ist, ist $K_{j+1} = L^{G_{j+1}}$ auch galois über K_j. Es ist
$\mathrm{Gal}(K_{j+1}/K_j) \cong G_{j+1}/G_j$
Sei z eine primitive $|G|$-te Einheitswurzel.
Ersetzen wir die Kette durch

$$K_0(z) \subset K_1(z) \subset \ldots \subset K_r(z) = L(z),$$

so erhalten wir nach dem Translationssatz eine neue Kette von Galoiserweiterungen von Primzahlgrad.
Da $K_j(z)$ für $p \mid |G|$ alle p-ten Einheitswurzeln enthält, entstehen die jeweiligen Erweiterungen nach Korollar 1 durch Adjunktion einer p-ten Wurzel. Damit ist $L(z)$ und damit $L \subset L(z)$ durch Radikale auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

die entsprechende Kette der Zwischenkörper nach dem Hauptsatz der Galoistheorie.
Hierbei ist jeweils K_{j+1}/K_j eine Galoiserweiterung und der Grad $[K_{j+1} : K_j]$ is eine Primzahl.
Galois sieht man so: Es ist L/K_j galois mit Galoisgruppe G_j. Da $G_{j+1} \subset G_j$ ein Normalteiler ist, ist $K_{j+1} = L^{G_{j+1}}$ auch galois über K_j. Es ist
$\mathrm{Gal}(K_{j+1}/K_j) \cong G_{j+1}/G_j$
Sei z eine primitive $|G|$-te Einheitswurzel.
Ersetzen wir die Kette durch

$$K_0(z) \subset K_1(z) \subset \ldots \subset K_r(z) = L(z),$$

so erhalten wir nach dem Translationssatz eine neue Kette von Galoiserweiterungen von Primzahlgrad.
Da $K_j(z)$ für $p \mid |G|$ alle p-ten Einheitswurzeln enthält, entstehen die jeweiligen Erweiterungen nach Korollar 1 durch Adjunktion einer p-ten Wurzel. Damit ist $L(z)$ und damit $L \subset L(z)$ durch Radikale auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

die entsprechende Kette der Zwischenkörper nach dem Hauptsatz der Galoistheorie.
Hierbei ist jeweils K_{j+1}/K_j eine Galoiserweiterung und der Grad $[K_{j+1} : K_j]$ is eine Primzahl.
Galois sieht man so: Es ist L/K_j galois mit Galoisgruppe G_j. Da $G_{j+1} \subset G_j$ ein Normalteiler ist, ist $K_{j+1} = L^{G_{j+1}}$ auch galois über K_j. Es ist
$\mathrm{Gal}(K_{j+1}/K_j) \cong G_{j+1}/G_j$
Sei z eine primitive $|G|$-te Einheitswurzel.
Ersetzen wir die Kette durch

$$K_0(z) \subset K_1(z) \subset \ldots \subset K_r(z) = L(z),$$

so erhalten wir nach dem Translationssatz eine neue Kette von Galoiserweiterungen von Primzahlgrad.
Da $K_j(z)$ für $p \mid |G|$ alle p-ten Einheitswurzeln enthält, entstehen die jeweiligen Erweiterungen nach Korollar 1 durch Adjunktion einer p-ten Wurzel. Damit ist $L(z)$ und damit $L \subset L(z)$ durch Radikale auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

die entsprechende Kette der Zwischenkörper nach dem Hauptsatz der Galoistheorie.
Hierbei ist jeweils K_{j+1}/K_j eine Galoiserweiterung und der Grad $[K_{j+1} : K_j]$ is eine Primzahl.
Galois sieht man so: Es ist L/K_j galois mit Galoisgruppe G_j. Da $G_{j+1} \subset G_j$ ein Normalteiler ist, ist $K_{j+1} = L^{G_{j+1}}$ auch galois über K_j. Es ist
$\mathrm{Gal}(K_{j+1}/K_j) \cong G_{j+1}/G_j$
Sei z eine primitive $|G|$-te Einheitswurzel.
Ersetzen wir die Kette durch

$$K_0(z) \subset K_1(z) \subset \ldots \subset K_r(z) = L(z),$$

so erhalten wir nach dem Translationssatz eine neue Kette von Galoiserweiterungen von Primzahlgrad.
Da $K_j(z)$ für $p \mid |G|$ alle p-ten Einheitswurzeln enthält, entstehen die jeweiligen Erweiterungen nach Korollar 1 durch Adjunktion einer p-ten Wurzel. Damit ist $L(z)$ und damit $L \subset L(z)$ durch Radikale auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

die entsprechende Kette der Zwischenkörper nach dem Hauptsatz der Galoistheorie.
Hierbei ist jeweils K_{j+1}/K_j eine Galoiserweiterung und der Grad $[K_{j+1} : K_j]$ is eine Primzahl.
Galois sieht man so: Es ist L/K_j galois mit Galoisgruppe G_j. Da $G_{j+1} \subset G_j$ ein Normalteiler ist, ist $K_{j+1} = L^{G_{j+1}}$ auch galois über K_j. Es ist
$\mathrm{Gal}(K_{j+1}/K_j) \cong G_{j+1}/G_j$
Sei z eine primitive $|G|$-te Einheitswurzel.
Ersetzen wir die Kette durch

$$K_0(z) \subset K_1(z) \subset \ldots \subset K_r(z) = L(z),$$

so erhalten wir nach dem Translationssatz eine neue Kette von Galoiserweiterungen von Primzahlgrad.
Da $K_j(z)$ für $p \mid |G|$ alle p-ten Einheitswurzeln enthält, entstehen die jeweiligen Erweiterungen nach Korollar 1 durch Adjunktion einer p-ten Wurzel. Damit ist $L(z)$ und damit $L \subset L(z)$ durch Radikale auflösbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei umgekehrt L/K durch Radikale auflösbar.
D.h. L ist ein Zwischenkörper der Erweiterung E/K und

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

ist eine Körperkette, bei der in jeder Erweiterung eine Wurzel adjungiert wird: $E_i = E_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in E_{i-1}$.
OBdA sei $L = E$.
OBdA erhalten wir die Erweiterungen durch Adjunktion einer Wurzel von Primzahlordnung p_i, also $\alpha_i^{p_i} \in E_{i-1}$. Sei $n := p_1 \cdots p_r$ und z eine primitive n-te Einheitswurzel.
Nach Satz 2 ist nun $E_{j+1}(z)/E_j(z)$ eine zyklische (Galois-)erweiterung.
Wir erhalten mittels des Translationssatzes eine Kette

$$K \subset K(z) = E_0(z) \subset E_1(z) \subset \ldots \subset E_m(z) = E(z)$$

von Galoiserweiterungen mit abelschen Galoisgruppen (bemerke: $K(z)/K$ ist eine abelsche Erweiterung, denn $\mathbb{Q}(z)/\mathbb{Q}$ ist eine endliche, abelsche Galoiserweiterung und $K(z)/K$ somit ebenfalls, nach dem Translationssatz).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei umgekehrt L/K durch Radikale auflösbar.
D.h. L ist ein Zwischenkörper der Erweiterung E/K und

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

ist eine Körperkette, bei der in jeder Erweiterung eine Wurzel adjungiert wird: $E_i = E_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in E_{i-1}$.
OBdA sei $L = E$.
OBdA erhalten wir die Erweiterungen durch Adjunktion einer Wurzel von Primzahlordnung p_i, also $\alpha_i^{p_i} \in E_{i-1}$. Sei $n := p_1 \cdots p_r$ und z eine primitive n-te Einheitswurzel.
Nach Satz 2 ist nun $E_{j+1}(z)/E_j(z)$ eine zyklische (Galois-)erweiterung.
Wir erhalten mittels des Translationssatzes eine Kette

$$K \subset K(z) = E_0(z) \subset E_1(z) \subset \ldots \subset E_m(z) = E(z)$$

von Galoiserweiterungen mit abelschen Galoisgruppen (bemerke: $K(z)/K$ ist eine abelsche Erweiterung, denn $\mathbb{Q}(z)/\mathbb{Q}$ ist eine endliche, abelsche Galoiserweiterung und $K(z)/K$ somit ebenfalls, nach dem Translationssatz).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei umgekehrt L/K durch Radikale auflösbar.
D.h. L ist ein Zwischenkörper der Erweiterung E/K und

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

ist eine Körperkette, bei der in jeder Erweiterung eine Wurzel adjungiert wird: $E_i = E_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in E_{i-1}$.
OBdA sei $L = E$.
OBdA erhalten wir die Erweiterungen durch Adjunktion einer Wurzel von Primzahlordnung p_i, also $\alpha_i^{p_i} \in E_{i-1}$. Sei $n := p_1 \cdots p_r$ und z eine primitive n-te Einheitswurzel.
Nach Satz 2 ist nun $E_{j+1}(z)/E_j(z)$ eine zyklische (Galois-)erweiterung.
Wir erhalten mittels des Translationssatzes eine Kette

$$K \subset K(z) = E_0(z) \subset E_1(z) \subset \ldots \subset E_m(z) = E(z)$$

von Galoiserweiterungen mit abelschen Galoisgruppen (bemerke: $K(z)/K$ ist eine abelsche Erweiterung, denn $\mathbb{Q}(z)/\mathbb{Q}$ ist eine endliche, abelsche Galoiserweiterung und $K(z)/K$ somit ebenfalls, nach dem Translationssatz).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei umgekehrt L/K durch Radikale auflösbar.
D.h. L ist ein Zwischenkörper der Erweiterung E/K und

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

ist eine Körperkette, bei der in jeder Erweiterung eine Wurzel adjungiert wird: $E_i = E_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in E_{i-1}$.
OBdA sei $L = E$.
OBdA erhalten wir die Erweiterungen durch Adjunktion einer Wurzel von Primzahlordnung p_i, also $\alpha_i^{p_i} \in E_{i-1}$. Sei $n := p_1 \cdots p_r$ und z eine primitive n-te Einheitswurzel.
Nach Satz 2 ist nun $E_{j+1}(z)/E_j(z)$ eine zyklische (Galois-)erweiterung.
Wir erhalten mittels des Translationssatzes eine Kette

$$K \subset K(z) = E_0(z) \subset E_1(z) \subset \ldots \subset E_m(z) = E(z)$$

von Galoiserweiterungen mit abelschen Galoisgruppen (bemerke: $K(z)/K$ ist eine abelsche Erweiterung, denn $\mathbb{Q}(z)/\mathbb{Q}$ ist eine endliche, abelsche Galoiserweiterung und $K(z)/K$ somit ebenfalls, nach dem Translationssatz).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei umgekehrt L/K durch Radikale auflösbar.
D.h. L ist ein Zwischenkörper der Erweiterung E/K und

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

ist eine Körperkette, bei der in jeder Erweiterung eine Wurzel adjungiert wird: $E_i = E_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in E_{i-1}$.
OBdA sei $L = E$.
OBdA erhalten wir die Erweiterungen durch Adjunktion einer Wurzel von Primzahlordnung p_i, also $\alpha_i^{p_i} \in E_{i-1}$. Sei $n := p_1 \cdots p_r$ und z eine primitive n-te Einheitswurzel.
Nach Satz 2 ist nun $E_{j+1}(z)/E_j(z)$ eine zyklische (Galois-)erweiterung.
Wir erhalten mittels des Translationssatzes eine Kette

$$K \subset K(z) = E_0(z) \subset E_1(z) \subset \ldots \subset E_m(z) = E(z)$$

von Galoiserweiterungen mit abelschen Galoisgruppen (bemerke: $K(z)/K$ ist eine abelsche Erweiterung, denn $\mathbb{Q}(z)/\mathbb{Q}$ ist eine endliche, abelsche Galoiserweiterung und $K(z)/K$ somit ebenfalls, nach dem Translationssatz).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei umgekehrt L/K durch Radikale auflösbar.
D.h. L ist ein Zwischenkörper der Erweiterung E/K und

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

ist eine Körperkette, bei der in jeder Erweiterung eine Wurzel adjungiert wird: $E_i = E_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in E_{i-1}$.
OBdA sei $L = E$.
OBdA erhalten wir die Erweiterungen durch Adjunktion einer Wurzel von Primzahlordnung p_i, also $\alpha_i^{p_i} \in E_{i-1}$. Sei $n := p_1 \cdots p_r$ und z eine primitive n-te Einheitswurzel.
Nach Satz 2 ist nun $E_{j+1}(z)/E_j(z)$ eine zyklische (Galois-)erweiterung.
Wir erhalten mittels des Translationssatzes eine Kette

$$K \subset K(z) = E_0(z) \subset E_1(z) \subset \ldots \subset E_m(z) = E(z)$$

von Galoiserweiterungen mit abelschen Galoisgruppen (bemerke: $K(z)/K$ ist eine abelsche Erweiterung, denn $\mathbb{Q}(z)/\mathbb{Q}$ ist eine endliche, abelsche Galoiserweiterung und $K(z)/K$ somit ebenfalls, nach dem Translationssatz).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei $N \supset E(z) \supset K$ die normale Hülle von $E(z)/K$, dies ist dann eine endliche Galoiserweiterung.

Sei $\mathrm{Gal}(N/K) = \{\sigma_1, \ldots, \sigma_r\}$. Setze $M_0 = K, M_1 = K(z)$, sowie $M_2 = M_1(\sigma_1(\alpha_1))$, $M_3 = M_2(\sigma_1(\alpha_2)), \ldots,$
$M_{m+1} = M_m(\sigma_1(\alpha_m)), M_{m+2} = M_{m+1}(\sigma_2(\alpha_1)), \ldots$.
Wir erhalten eine Kette von Körpererweiterungen

$$M_0 \subset M_1 \subset \ldots \subset M_t = N$$

in der jeder Schritt eine abelsche (ggf. triviale) Erweiterung darstellt.
Wir erhalten nach dem Hauptsatz der Galoistheorie, dass $\mathrm{Gal}(N/M_0)$ auflösbar ist (und es ist $L \subset N$). Damit haben wir den Beweis abgeschlossen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei $N \supset E(z) \supset K$ die normale Hülle von $E(z)/K$, dies ist dann eine endliche Galoiserweiterung.
Sei $\mathrm{Gal}(N/K) = \{\sigma_1, \ldots, \sigma_r\}$. Setze $M_0 = K, M_1 = K(z)$, sowie
$M_2 = M_1(\sigma_1(\alpha_1))$, $M_3 = M_2(\sigma_1(\alpha_2)), \ldots,$
$M_{m+1} = M_m(\sigma_1(\alpha_m)), M_{m+2} = M_{m+1}(\sigma_2(\alpha_1)), \ldots.$
Wir erhalten eine Kette von Körpererweiterungen

$$M_0 \subset M_1 \subset \ldots \subset M_t = N$$

in der jeder Schritt eine abelsche (ggf. triviale) Erweiterung darstellt.
Wir erhalten nach dem Hauptsatz der Galoistheorie, dass $\mathrm{Gal}(N/M_0)$ auflösbar ist (und es ist $L \subset N$). Damit haben wir den Beweis abgeschlossen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei $N \supset E(z) \supset K$ die normale Hülle von $E(z)/K$, dies ist dann eine endliche Galoiserweiterung.
Sei $\mathrm{Gal}(N/K) = \{\sigma_1, \ldots, \sigma_r\}$. Setze $M_0 = K, M_1 = K(z)$, sowie
$M_2 = M_1(\sigma_1(\alpha_1))$, $M_3 = M_2(\sigma_1(\alpha_2)), \ldots,$
$M_{m+1} = M_m(\sigma_1(\alpha_m)), M_{m+2} = M_{m+1}(\sigma_2(\alpha_1)), \ldots.$
Wir erhalten eine Kette von Körpererweiterungen

$$M_0 \subset M_1 \subset \ldots \subset M_t = N$$

in der jeder Schritt eine abelsche (ggf. triviale) Erweiterung darstellt.
Wir erhalten nach dem Hauptsatz der Galoistheorie, dass $\mathrm{Gal}(N/M_0)$ auflösbar ist (und es ist $L \subset N$). Damit haben wir den Beweis abgeschlossen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis (Forts.)

Sei $N \supset E(z) \supset K$ die normale Hülle von $E(z)/K$, dies ist dann eine endliche Galoiserweiterung.
Sei $\mathrm{Gal}(N/K) = \{\sigma_1, \ldots, \sigma_r\}$. Setze $M_0 = K, M_1 = K(z)$, sowie
$M_2 = M_1(\sigma_1(\alpha_1))$, $M_3 = M_2(\sigma_1(\alpha_2)), \ldots,$
$M_{m+1} = M_m(\sigma_1(\alpha_m)), M_{m+2} = M_{m+1}(\sigma_2(\alpha_1)), \ldots.$
Wir erhalten eine Kette von Körpererweiterungen

$$M_0 \subset M_1 \subset \ldots \subset M_t = N$$

in der jeder Schritt eine abelsche (ggf. triviale) Erweiterung darstellt.
Wir erhalten nach dem Hauptsatz der Galoistheorie, dass $\mathrm{Gal}(N/M_0)$ auflösbar ist (und es ist $L \subset N$). Damit haben wir den Beweis abgeschlossen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln