Hauptsatz der Galoistheorie

Sei $L|K$ eine endliche Galois-Erweiterung (d.h. eine endl. normale und separable Erweiterung) und $G = \mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$ die zugehörige Galoisgruppe. Es sei

$\mathcal{U}$ die Menge der Untergruppen von G und

$\mathcal{Z}$ die Menge der Zwischenkörper von $L|K$.

Dann sind $\phi : \mathcal{U} \to \mathcal{Z},\ U \mapsto L^U$ und

$\psi : \mathcal{Z} \to \mathcal{U},\ M \mapsto \mathrm{Gal}(L|M)$ zueinander

inverse Bijektionen; wobei für jedes $U \in \mathcal{U}$ durch $L^U = \{x \in L \mid \sigma(x) = x \; \forall \sigma \in U\}$ jeweils der sog. Fixkörper von U bezeichnet wird.

(ausführlich: $U = \mathrm{Gal}(L|L^U) \quad \forall U \in \mathcal{U}$

und $M = L^{\mathrm{Gal}(L|M)} \quad \forall M \in \mathcal{Z}$)

Zusätze zum Hauptsatz der Galoistheorie:

(i) Die Abbildungen Φ und Ψ sind antiton d.h.

$\forall U, V \in \mathcal{U}: U \subseteq V \Leftrightarrow L^U \supseteq L^V$

$\forall M, M' \in \mathcal{Z}: M \subseteq M' \Leftarrow$

$\mathrm{Gal}(L|M) \supseteq \mathrm{Gal}(L|M')$

ung
reite-
-)

G und
von L|K.
und
zueinander

(ii). ~~„Extremfälle"~~) $L^{\{id_L\}} = L$, $L^G = K$ und ebenso $Gal(L|K) = G$, $Gal(L|L) = \{id_L\}$

(iii) Sei $U \in \mathcal{U}$ und $M = L^U$ der zugeh. Zwischenkörper. Dann gilt $[M:K] = (G:U) = \frac{|G|}{|U|}$ und $[L:M] = |U|$.

(iv) Sei $U \in \mathcal{U}$ und $M = L^U$. Dann gilt die Äquivalenz

$U \trianglelefteq G \Leftrightarrow M|K$ normal $\Leftrightarrow M|K$ galois'sch

H24T2A5 Sei $f = x^6 - 6 \in \mathbb{Q}[x]$.

(a) gezeigt: Der Zerfällungskörper $L \subseteq \mathbb{C}$ von f über $\mathbb{Q}$ ist geg. durch $L = \mathbb{Q}(\sqrt[6]{6}, \sqrt{-3})$, und es

ist $[L:\mathbb{Q}] = 12$.

(b) bereits gezeigt: $L|\mathbb{Q}$ ist eine Galois-Erweiterung

noch z.zg.: $G = \mathrm{Gal}(L|\mathbb{Q})$ besitzt einen Normalteiler der Ordnung 6

Da $L|\mathbb{Q}$ eine endliche Galois-Erw. ist, gilt $|G| = [L:\mathbb{Q}] = 12$.

Die Normalteiler von G von Ordnung 6 sind wegen $|G| = 12$ genau die Normalteiler vom Index 2, denn für jeden Normalteiler N von G gilt $(G:N) = \frac{|G|}{|N|} = \frac{12}{|N|}$. Sei $M = \mathbb{Q}(\sqrt{-3})$, wegen $\sqrt{-3} \in L$ ist dies ein Zwischenkörper von $L|\mathbb{Q}$.

Da -3 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, gilt

Vorlesung $[\mathbb{Q}(\sqrt{-3}):\mathbb{Q}] = 2$. Sei $N = \mathrm{Gal}(L|M)$. Laut Galoistheorie gilt dann $(G:N) = [M:\mathbb{Q}] = 2$, somit $|N| = 6$. Als Erweiterung vom Grad 2 ist $M|\mathbb{Q}$ normal, und daraus folgt lt. Galoistheorie $N \trianglelefteq G$.

(Neben M enthält L auch noch die quadratischen Zahlkörper $\mathbb{Q}(\sqrt{6})$ und $\mathbb{Q}(\sqrt{-2})$ wegen $\sqrt{6} = (\sqrt[6]{6})^3 \in L$ und $\sqrt{-2} = \frac{\sqrt{6}}{\sqrt{-3}} \in L$. Diese liefern zwei weitere Normalteiler der Ordnung 6 in G.)

(c) Untersuchen Sie, ob G eine abelsche Gruppe ist.

Sei $M' = \mathbb{Q}(\sqrt[6]{6})$ Beh.: $M'|\mathbb{Q}$ ist keine normale Erweiterung

Wie bereits unter (a) gezeigt, ist $f = x^6 - 6 \in \mathbb{Q}[x]$ irreduzibel und besitzt die Nullstelle $\sqrt[6]{6} \in \mathbb{R}$, die in M' enthalten ist. Würde f über M' in Linearfaktoren zerfallen, dann müsste M' auch die komplexe Nullstelle $\zeta\sqrt[6]{6}$ enthalten, mit der primitiven sechsten Einheitswurzel $\zeta = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Aber dies ist nicht der Fall, denn wegen $\sqrt[6]{6} \in \mathbb{R}$ gilt $M' \subseteq \mathbb{R}$, andererseits aber $\zeta\sqrt[6]{6} \notin \mathbb{R}$. Somit ist $M'|\mathbb{Q}$ nicht

Zahl ist, zyklisch, und somit (somit) ...

normal ($\Rightarrow$ Beh.)

Da $M'|\mathbb{Q}$ nicht normal ist, ist $U' = \mathrm{Gal}(L|M')$ laut Galoistheorie eine Untergruppe von G, die kein Normalteiler ist. Als Gruppe mit einer nicht-normalen Untergruppe ist G nicht abelsch. $\square$

Beispiele für abelsche Galoisgruppen:

(1) $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})|\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{m},\sqrt{n})|\mathbb{Q})$, falls m, n verschiedene quadratfreie Zahlen in $\mathbb{Z}\setminus\{0,1\}$ ($\cong \mathbb{Z}/2\mathbb{Z}$ bzw. $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$)

(2) $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ falls q Primzahlpotenz >1 und $n \in \mathbb{N}$ ($\cong \mathbb{Z}/n\mathbb{Z}$)

(3) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ mit $\zeta_n = e^{2\pi i/n}$ (Kreisteilungskörper) ($\cong (\mathbb{Z}/n\mathbb{Z})^\times$)

...2. Sei

...theorie

...] = 2.

...ung vom

...daraus folgt

...och die qua-

...') und $\mathbb{Q}(\sqrt{-2})$

$\sqrt{-2} = \frac{\sqrt{6}}{\sqrt{-3}} \in L$.

...Normalteiler der

...ne abelsche Gppe ist.

ist kein

, ist $\zeta =$

besitzt die

$\mathbb{Q}'$ enthalten

nest-faktoren

ch die kon-

alten, mit der

urzel $\zeta =$

der Fall, denn

$\mathbb{R}$, andererseits

ist $M'|\mathbb{Q}$ nicht

Aufgabe Zeigen Sie, dass für jede Primzahl p eine Galoiserweiterung $L_p|\mathbb{Q}$ mit $\mathrm{Gal}(L_p|\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$ existiert.

Bekanntlich ist $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ eine Erweiterung vom Grad 2, als solche normal und damit auch algebraisch, wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel, insgesamt galois'sch $\Rightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ ist Gruppe der Ordnung 2, da 2 eine Primzahl ist, zyklisch, und somit isomorph zu $\mathbb{Z}/2\mathbb{Z}$.

Sei nun p eine ungerade Primzahl.

Laut Vorlesung gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}) \cong$

(b) Beweisen Sie: $K_1 \cap K_2 = \mathbb{Q}$ (c) Bestimmen Sie $[L : \mathbb{Q}]$.

$(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p(p-1)\mathbb{Z}$, wobei $\zeta_{p^2} = e^{2\pi i/p^2}$.

Da $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$ somit zyklisch von Ordnung $p(p-1)$ ist, und $p-1$ ein Teiler von $p(p-1)$, gibt es in G eine Untergruppe U mit $|U| = p-1$.

Sei $L_p = \mathbb{Q}(\zeta_{p^2})^U$. Laut Galoistheorie gilt

$$[L_p : \mathbb{Q}] = (G : U) = \frac{|G|}{|U|} = \frac{p(p-1)}{p-1} = p.$$

Da mit $(\mathbb{Z}/p^2\mathbb{Z})^\times$ auch G abelsch ist, gilt $U \trianglelefteq G$, und $L_p/\mathbb{Q}$ ist somit galoisch. Dabei ist $\mathrm{Gal}(L_p/\mathbb{Q})$ eine Gruppe der Ordnung $[L_p : \mathbb{Q}] = p$, und als Gruppe von

Primzahlordnung ist diese zyklisch, also isomorph zu $\mathbb{Z}/p\mathbb{Z}$. □

Übung: Zeigen Sie, dass für jedes $n \in \mathbb{N}$ eine Galois-Erweiterung $L_n|\mathbb{Q}$ mit $\mathrm{Gal}(L_n|\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$ existiert.

F22T2A5 Übung: F23T1A3, H22T1A3

Seien $K_1 = \mathbb{Q}(\sqrt{3})$, $K_2 = \mathbb{Q}(\sqrt{6})$, aufgefasst als Teilkörper von $\mathbb{C}$.

(a) Zeigen Sie, dass das Kompositum $L = K_1K_2$ mit $\mathbb{Q}(\sqrt{2},\sqrt{3})$ übereinstimmt.

(b) Beweisen Sie: $K_1 \cap K_2 = \mathbb{Q}$ (c) Bestimmen Sie $[L:\mathbb{Q}]$.

(d) Zeigen Sie, dass $L|\mathbb{Q}$ galois'sch ist, und bestimmen Sie $G = \mathrm{Gal}(L|\mathbb{Q})$ bis auf Isomorphie.

(e) Geben Sie alle Zwischenkörper von $L|\mathbb{Q}$ an (mit Nachweis).

zu (a) Nach Def. des Kompositums gilt $K_1 \cdot K_2 = K_1(K_2)$, d.h. $K_1 \cdot K_2$ ist der von K_2 über K_1 erzeugte Teilkörper von $\mathbb{C}$. Zu zeigen ist also

$$\mathbb{Q}(\sqrt{3})\left(\mathbb{Q}(\sqrt{6})\right) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

„$\supseteq$" zzg: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})\left(\mathbb{Q}(\sqrt{6})\right)$ und $\{\sqrt{2}, \sqrt{3}\} \subseteq \mathbb{Q}(\sqrt{3})\left(\mathbb{Q}(\sqrt{6})\right)$

$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{3})] \leq [\mathbb{Q}(\sqrt{3})(\sqrt{6}) : \mathbb{Q}(\sqrt{3})]$

Die erste Aussage folgt aus $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$.
Wegen $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ gilt auch $\sqrt{3} \in \mathbb{Q}(\sqrt{3})(\sqrt{6})$
Wegen $\sqrt{6} \in \mathbb{Q}(\sqrt{6})$ gilt auch $\sqrt{6} \in \mathbb{Q}(\sqrt{3})(\sqrt{6})$
Damit liegt auch $\sqrt{2} = \frac{\sqrt{6}}{\sqrt{3}}$ in $\mathbb{Q}(\sqrt{3})(\sqrt{6})$
„$\subseteq$" z.Zg: $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ und
$\mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ Die erste Aussage ist wegen
$\{\sqrt{3}\} \subseteq \{\sqrt{2},\sqrt{3}\}$ offensichtlich. Außerdem ist mit
$\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ auch $\sqrt{6} = \sqrt{2}\cdot\sqrt{3}$ in
$\mathbb{Q}(\sqrt{2},\sqrt{3})$ enthalten.

zerfallen, dann müsste $\mathbb{Q}$ auch die Kon

zu (b) „⊇" klar, da $\mathbb{Q}$ gem. Teilkörper von $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$ ist. Ang., es gilt $\mathbb{Q} \overset{(*)}{\subsetneq} K_1 \cap K_2$. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}] = 2$ für jedes quadratfreie d in $\mathbb{Z} \setminus \{0, 1\}$. Gradformel, $K_1 \cap K_2$ ist Zwischenkörper von $K_1 | \mathbb{Q} \Rightarrow 2 = [K_1 : \mathbb{Q}] = [K_1 : K_1 \cap K_2] \cdot [K_1 \cap K_2 : \mathbb{Q}] \Rightarrow [K_1 \cap K_2 : \mathbb{Q}] \in \{1, 2\}$

$(*) \Rightarrow [K_1 \cap K_2 : \mathbb{Q}] = 2, [K_1 : K_1 \cap K_2] = 1$

$\Rightarrow \mathbb{Q}(\sqrt{3}) = K_1 \cap K_2$ Da auch $6 \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei ist, folgt genauso $\mathbb{Q}(\sqrt{6}) = K_1 \cap K_2$, insgesamt $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{6})$. Aber laut Vl

die Kom-

gesamt gelöst ⇒ $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$

ipe von

gilt

gilt

eie d in

ist Zwischen-

$= [K_1 : K_1 \cap K_2]$

$\in \{1, 2\}$

$\cap K_2] = 1$

$\in \mathbb{Z}[10, 17]$

$\mathbb{Q}(\sqrt{6}) = K_1 \cap K_2$,

Aber laut Vl

gilt $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$ falls d, d' zwei verschiedene quadratfreie Zahlen in $\mathbb{Z} \setminus \{0, 1\}$ sind.