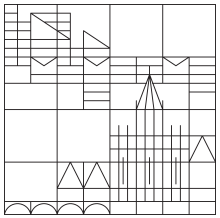
Letzte Vorlesung im Wintersemester 2004/05

Einführung in die Algebra (B III)

Gottfried Barthel
FB Mathematik und Statistik



Universität Konstanz

C.8 **Endliche Körper** **(#1)**

Klassifikationssatz für endliche Körper: Ist p prim und $q := p^k$ mit $k \geqq 1$, so gibt es – bis auf Isomorphie – genau einen Körper $\mathbb{F}_q$ mit q Elementen**.**

Beweis: Für das Polynom $f_q := T^q - T \in \mathbb{F}_p[T]$ aus C.3, Anwendung gilt $f_q' \equiv 1$; damit hat f_q nach dem Lemma aus C.6 nur einfache Nullstellen in seinem Zerfällungskörper $L := \mathbb{F}_p(N_{f_q})$**.** Wegen der in C.3 bereits gezeigten Gleichheit

$$L = L' = \{a \in L\,;\; a^q = a\} = N_{f_q}$$

gilt also

$$\#\mathbb{F}_p(N_{f_q}) \;=\; \#N_{f_q} \;=\; \deg f_q \;=\; q\,.$$

Damit ist die ***Existenz*** gezeigt.

→ #2

C.8 Klassifikation endlicher Körper (#2)

Weiter gilt in einem Körper K mit q Elementen notwendig

$$\#(K^\times) = q-1 \quad \text{und damit} \quad a^{q-1} = 1 \quad \text{für jedes } a \neq 0$$

(nach dem „Kleinen Satz von Fermat“ aus der Gruppentheorie, siehe GG : B.6, Folgerung)**.** Daraus folgt

$$a^q = a \quad \text{für alle } a \in K,$$

also $K = N_{f_q}$ und somit auch

$$K = \mathbb{F}_p(N_{f_q})\,.$$

Damit ist auch die ***Eindeutigkeit*** (bis auf Isomorphie) gezeigt**.** ✓

* * *

→ #3

C.8 Endliche Körper (#3)

Folgerung (Normalität endlicher Körper): Jeder endliche Körper $\mathbb{F}_q$ ist eine normale Erweiterung seines Primkörpers $\mathbb{F}_p$ (und damit auch jedes Zwischenkörpers $\mathbb{F}_{q'}$).

Beweis: Das folgt sofort aus der soeben gezeigten Gleichung

$$K = \mathbb{F}_p(N_{f_q})\,,$$

weil der Zerfällungskörper eines Polynoms stets normal über dem Grundkörper ist (siehe C.4, Charakterisierung von endlichen normalen KE).

→ #4

Bemerkung: Ein endlicher Körper $\mathbb{F}_{q'}$ ist Zwischenkörper von $\mathbb{F}_q/\mathbb{F}_p$ genau dann, wenn gilt:

$$\log_p(q') \mid \log_p(q)$$

(d.h. mit $q = p^k$ und $q' = p^{k'}$ gilt $k' \mid k$).

Beweis: Ist $\mathbb{F}_{q'}$ ein Zwischenkörper, so gilt mit dem Körpergrad $\ell := [\mathbb{F}_q : \mathbb{F}_{q'}]$ notwendig $q = (q')^\ell$ und damit $k = \ell \cdot k'$.
Gilt umgekehrt $k = \ell \cdot k'$, so folgt für ein beliebiges $a \in \mathbb{F}_{q'}$ aus $a^{q'} = a$ sofort

$$a^q = \underbrace{\Big(\dots\big((a^{q'})^{q'}\big)^{\cdots}\Big)^{q'}}_{\ell\text{-fach}} = a$$

und damit $a \in \mathbb{F}_q$. ☑

→ #5

Satz vom primitiven Element für endliche Körper: Ein endlicher Körper $\mathbb{F}_q$ ist eine ***einfache Erweiterung*** seines Grundkörper $\mathbb{F}_p$ (und damit auch jedes Zwischenkörpers $\mathbb{F}_{q'}$).

Beweis: Nach Übungsaufgabe 8 von Blatt 15 gilt

$$\mathbb{F}_q^\times \cong C_{q-1}\,.$$

Ist $a \in \mathbb{F}_q^\times$ ein Erzeugendes dieser zyklischen Gruppe, so gilt natürlich

$$\mathbb{F}_q = \mathbb{F}_p(a)\,.$$ ☑

→ #6

Mitteilung: Der „Satz vom primitiven Element“ gilt allgemeiner: Jede endliche separable Körpererweiterung L/K ist einfach.

Insbesondere ist jede endliche Erweiterung in Charakteristik Null und allgemeiner jede endliche Erweiterung eines vollkommenen Körpers einfach.

Zum Beweis genügt es offenbar, sich auf Erweiterungen $L = K(a,b)/K$ mit zwei Erzeugenden zu beschränken und $\#K = \infty$ vorauszusetzen; man zeigt dann, dass eine geeignete Linearkombination $a + \lambda b$ schon den Körper L erzeugt.

* * *

D Galois-Erweiterungen und Hauptsatz der Galois-Theorie *

D.1 Grundbegriffe: Galois-Erweiterungen und Galois-Gruppe

Definition: Eine ***endliche normale separable Körpererweiterung*** L/K heißt (endliche) GALOIS-Erweiterung; die zugehörige Automorphismengruppe

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L) := \{\sigma \in \mathrm{Aut}(L)\ ;\ \sigma|_K = \mathrm{id}_K\}$$

heißt GALOIS-Gruppe (von L über K).
Ist K ein Körper und $f \in K[T] \setminus K$ ein ***separables Polynom*** mit Zerfällungskörper $K(N_f)$, so heißt $\mathrm{Gal}(K(N_f)/K)$ auch die GALOIS-Gruppe von f bzw. der Gleichung $f(x) = 0$.

→ #2

Beispiele von Galois-Erweiterungen:

- Normale (endliche) Erweiterungen vollkommener Körper, z.B.
  - $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\mathbb{F}_q/\mathbb{F}_{q'}$, $\mathbb{C}/\mathbb{R}$, ...
- Zerfällungskörper separabler Polynome, z.B.
  - „Kreisteilungskörper“ $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ (dabei $\zeta_m := e^{2\pi i/m}$ für $m \geqq 2$),
  - $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q}$ (dabei p prim), $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$, ...

Zugehörige Galois-Gruppen: ???

→ #3

Erstes Ziel: Ordnung der Galois-Gruppe

Wollen die folgende

Galois-Gruppenordnungs-Körpergrad-Formel

zeigen:

Für eine (stets als endlich vorausgesetzte) GALOIS-Erweiterung L/K gilt

$$\#\operatorname{Gal}(L/K) \;=\; [L:K].$$

Diese Aussage folgt aus einem allgemeineren, etwas technischen Lemma, das wir im folgenden Abschnitt D.2 formulieren und beweisen.

→ D.2

Lemma: Gegeben endl. KE L/K, L'/K' und Iso $\sigma\colon K \xrightarrow{\cong} K'$; sei

$$\tilde{\Sigma} := \operatorname{Hom}_\sigma(L/K, L'/K') = \left\{ \tilde{\sigma}\colon L \to L' \;;\; \begin{array}{ccc} K & \hookrightarrow & L \\ \sigma\downarrow\cong & @ & \downarrow\tilde{\sigma} \\ K' & \hookrightarrow & L' \end{array} \right\}$$

(Menge der Einbettungen von L/K nach L'/K' über σ). Dann gilt:

(1) $\#\tilde{\Sigma} \leqq [L:K]$;

(2) Ist L/K separabel erzeugt und L'/K' normal, so entweder $\tilde{\Sigma} = \emptyset$ oder $\#\tilde{\Sigma} = [L:K]$.

→ (1), #1

Beweis: Im Fall $\tilde{\Sigma} = \emptyset$ ist nichts zu zeigen; sei also $\tilde{\Sigma} \neq \emptyset$ und $\tilde{\sigma} \in \tilde{\Sigma}$ beliebig gewählt. Seien $x_1, \ldots, x_n \in L$ Erzeugende.

Methode: Induktion nach n.

Ind.anf. $n = 0$: nichts zu zeigen.

Ind.vor.: Sei $n > 0$; Beh. gelte für Erweiterungen mit höchstens $n-1$ Erzeugenden.

Ind.schluss: Sei $f_1 = f_{x_1}$ das Min.poly. zu x_1/K; seien $y_1 = \tilde{\sigma}(x_1), \ldots, y_r$ die Nullstellen von f_1^σ in L'.

• Nach Zusatz zum Nullstellenexistenzsatz aus C.1 gehört zu jedem y_i genau ein Isomo $\hat{\sigma}_i/\sigma\colon K(x_1)/K \xrightarrow{\cong} K'(y_i)/K'$ mit $\hat{\sigma}_i(x_1) = y_i$.

→ (1), #2

D.2 Beweis des Lemmas, (1) (#2)

• Situation: Haben komm. Diagramm

$$\begin{array}{ccccc} K & \hookrightarrow & K(x_1) & \hookrightarrow & L \\ {\scriptstyle\sigma}\downarrow\cong & & {\scriptstyle\hat\sigma_i}\downarrow\cong & & {\scriptstyle\tilde\sigma}\downarrow ? \\ K' & \hookrightarrow & K'(y_i) & \hookrightarrow & L' \end{array}$$

• Erhalten disjunkte Zerlegung $\boxed{\tilde\Sigma = \dot{\bigcup} \tilde\Sigma_i}$ mit

$$\tilde\Sigma_i := \{\tilde\sigma \in \tilde\Sigma\,;\ \tilde\sigma(x_1) = y_i\} \ = \ \mathrm{Hom}_{\hat\sigma_i}(L/K(x_1), L'/K'(y_i))\,;$$

damit auch

$$\boxed{\#\tilde\Sigma \ = \ \sum_{i=1}^{r} \#\tilde\Sigma_i\,.}$$

→ (1), #3

D.2 Beweis des Lemmas, (1) (#3)

• Können jetzt auf

$$\begin{array}{ccc} K(x_1) & \hookrightarrow & L \\ {\scriptstyle\hat\sigma_i}\downarrow\cong & & ?\downarrow ? \\ K'(y_i) & \hookrightarrow & L' \end{array}$$

die Ind.vor. anwenden; erhalten

$$\#\tilde\Sigma_i \ \leqq \ [L : K(x_1)]\,.$$

• Addition liefert

$$\boxed{\#\tilde\Sigma \ \leqq \ r \cdot [L : K(x_1)]\,.}$$

→ (1), #4

D.2 Beweis des Lemmas, (1) (#4)

• Erinnerung: $r = \#\{y \in L'\,;\ f_1^\sigma(y) = 0\} \leqq \deg f_1^\sigma = \deg f_1$, also

$$\boxed{r \ \leqq \ \deg_K(x_1) \ = \ [K(x_1) : K]\,.}$$

• Mit Gradformel folgt

$$\boxed{\#\tilde\Sigma \ \leqq \ [L : K(x_1)] \cdot [K(x_1) : K] \ = \ [L : K]\,.}$$

Damit (1): ✓

→ (2), #1

D.2 Beweis des Lemmas, (2) (#1)

• (2) Setzen jetzt voraus:

— L'/K' normal;

— alle $x_i \in L/K$ separabel;

— weiterhin $\tilde\Sigma \neq \emptyset$.

Folgen dem Induktionsbeweis wie in Teil (1), zusätzlich:

• Weil L'/K' normal, zerfällt f_1^σ;

• weil x_1/K und damit y_1/K' separabel, gilt

$$\boxed{r = \deg_K(x_1) \ = \ [K(x_1) : K]\,.}$$

• Erinnerung:

$$\tilde\Sigma_i := \{\tilde\sigma \in \tilde\Sigma\,;\ \tilde\sigma(x_1) = y_i\} \ = \ \mathrm{Hom}_{\hat\sigma_i}(L/K(x_1), L'/K'(y_i))\,;$$

→ (2), #2

D.2 Beweis des Lemmas, (2) (#2)

• Nach Ind.vorauss. entweder $\tilde{\Sigma}_i = \emptyset$ oder $\#\tilde{\Sigma}_i = [L : K(x_1)]$.

• Bleibt also nur noch zu zeigen:

$$\boxed{\tilde{\Sigma}_i \neq \emptyset \quad \text{für alle } i = 1, \ldots, r\,.}$$

• Wissen: $\tilde{\Sigma}_1 \neq \emptyset$, denn $\tilde{\sigma} \in \tilde{\Sigma}_1$.

• Ziel: Suchen K'-Automo $\tilde{\tau}_i \colon L' \xrightarrow{\cong} L'$ mit $\tilde{\tau}_i(y_1) = y_i$, denn dann gilt

$$\boxed{\tilde{\tau}_i \circ \tilde{\sigma} \;\in\; \tilde{\Sigma}_i\,.}$$

• Wissen (wieder nach Zusatz zum Nullstellenexistenzsatz aus C.1): Zu jedem $i = 1, \ldots, r$ gehört genau ein K'-Isomo $\tau_i \colon K'(y_1) \xrightarrow{\cong} K'(y_i)$.

→ (2), #3

D.2 Beweis des Lemmas, (2) (#3)

• Wollen diesen K'-Isomo $\tau_i \colon K'(y_1) \xrightarrow{\cong} K'(y_i)$ fortsetzen zu dem gesuchten K'-Automo $\tilde{\tau}_i \colon L' \xrightarrow{\cong} L'$.

• Wissen: L'/K' normal, also $L' = K'(N_g)$ Zerf.körper für ein Polynom $g \in K'[T] \setminus K'$.

• Damit L' auch Zerf.körper für g über $K'(y_1)$ sowie für g^{τ_i} über $K'(y_i)$.

• Nach Eindeutigkeitssatz für Zerfällungskörper aus C.3 existiert die gesuchte Fortsetzung.

Damit ist (2) und somit das gesamte Lemma vollständig bewiesen. ✓

Vor der Fortsetzung der Galois-Theorie zunächst noch eine wichtige Anwendung: *Separabel erzeugte endliche Erweiterungen sind separabel.*

→ D.3

D.3 Separabilität (IV) – Anwendungen der Abschätzung

Proposition 1 (Separabel erzeugte endliche Erweiterungen sind separabel): Ist ein endl. algebraischer Erw.körper $L = K(x_1, \ldots, x_n)$ von separablen Elementen erzeugt, so ist L/K eine separable KE.

Beweis: Sei $a \in L \setminus K$ beliebig vom Grad $d := \deg_K(a) > 1$.

Beh.: Das zugeh. Minimalpolynom $f_a \in K[T]$ hat (genau) d Nullstellen in einer normalen Erweiterung L'/K mit $a \in L'$.

• Äquivalente Umformulierung mit Lemma aus C.3 (Eindeutigkeit des Zerfällungskörpers):

$$\#N_f \;=\; \#\mathrm{Hom}_K(K(a), L') \;\overset{!}{=}\; d\,.$$

→ #2

D.3 Separabilität (IV) – Beweis Proposition 1 (#2)

• Seien $f_i = f_{x_i} \in K[T]$ die (nach Vor. separablen) Minimalpolynome der Erzeugenden; sei $p := \prod_{i=1}^{n} f_i \in K[T]$ deren Produkt und $L' := K(N_p)$ der Zerf.körper.

• Nach Konstruktion ist L'/K normal mit $L \subset L'$, also auch $a \in L'$.

• Wenden „Einbettungsanzahl-Körpergrad-Abschätzungs-Lemma“ auf L/K und L'/K (also $K' = K$) mit $\sigma = \mathrm{id}_K$ an: Haben

$$\tilde{\Sigma} = \mathrm{Hom}_K(L, L') \neq \emptyset$$

(denn Einbettung $\tilde{\sigma} = \iota \colon L \hookrightarrow L'$ ist offenbar Element von $\tilde{\Sigma}$).

• Weil L/K separabel erzeugt und L'/K normal ist, gilt nach Lemma, Aussage (2)

$$\#\tilde{\Sigma} \;=\; [L : K]\,.$$

→ #3

D.3 Separabilität (IV) – Beweis Proposition 1 (#3)

• Sei $N_f = \{a_1 := a, \ldots, a_r\} \subset L'$ (also $r \leqq d$, zu zeigen $r \stackrel{!}{=} d$); erhalten wie im Beweis des Lemmas eine disjunkte (?...!) Zerlegung

$$\tilde{\Sigma} = \dot{\bigcup} \tilde{\Sigma}_i \quad \text{mit} \quad \tilde{\Sigma}_i := \{\tilde{\sigma} \in \tilde{\Sigma}\,;\, \tilde{\sigma}(a) = \tilde{\sigma}(a_i)\}\,.$$

• Nach (1) aus Lemma gilt

$$\#\tilde{\Sigma}_i \;\leqq\; [L : K(a)] \quad \text{für alle } i = 1, \ldots, r\,;$$

erhalten damit folgende Abschätzung

$$\#\tilde{\Sigma} \;=\; \sum_{i=1}^{r} \#\tilde{\Sigma}_i \;\leqq\; r \cdot [L : K(a)]\,.$$

→ #4

D.3 Separabilität (IV) – Beweis Proposition 1 (#4)

• Andererseits gilt $\#\tilde{\Sigma} \;=\; [L : K]$ sowie

$$[L : K] \;=\; [L : K(a)] \cdot \underbrace{[K(a) : K]}_{\deg_K(a) = d \geqq r}$$

und damit insgesamt

$$r \cdot [L : K(a)] \;\leqq\; d \cdot [L : K(a)] \;=\; [L : K] \;\leqq\; r \cdot [L : K(a)]\,,$$

woraus die gesuchte Gleichheit

$$\boxed{d = \deg_K(a) = r = \#N_f}$$

folgt. ✓

→ Prop.2

D.3 Separabilität (IV) – Proposition 2 (#1)

Proposition 2 (Satz vom primitiven Element): Ist L/K endlich und separabel, so gibt es $a \in L$ mit $L = K(a)$ (d.h. L/K ist einfach).

Insbesondere ist jede endliche Erweiterung in Charakteristik Null und allgemeiner jede endliche Erweiterung eines vollkommenen Körpers einfach.

• Wissen bereits aus C.8 : Gilt für endliche Körper.

• Beweisskizze (Erinnerung): Es genügt offenbar, sich auf Erweiterungen $L = K(x,y)/K$ mit zwei Erzeugenden zu beschränken und $\#K = \infty$ vorauszusetzen; man zeigt dann, dass eine geeignete Linearkombination $x + \lambda\, y$ schon den Körper L erzeugt – aber wie?

→ #2

D.3 Separabilität (IV) – Beweis Proposition 2 (#2)

zeigen ... aber wie?

• Konkreter: Sei $n = [L : K]$; sei $L'/L/K$ eine Erweiterung, so dass L'/K normal ist, z.B. der simultane Zerfällungskörper der Minimalpolynome f_x, f_y (damit auch L'/L normal).

• Wissen: $\#\,\mathrm{Hom}_K(L, L') = [L : K] = n$; seien $\sigma_1, \ldots, \sigma_n$ diese (paarweise verschiedenen) Einbettungen.

• *Genügt zu zeigen:* Es gibt ein $a \in L$ mit $\sigma_i(a) \neq \sigma_j(a)$ für $i \neq j$.

• Begründung: Damit einerseits $\#\,\mathrm{Hom}_K(K(a), L') \geqq n$ und folglich

$$[K(a) : K] \;\geqq\; \#\,\mathrm{Hom}_K(K(a), L') \;\geqq\; n$$

(schon wieder das Abschätzungslemma D.2 !) und andererseits natürlich

$$[K(a) : K] \;\leqq\; [L : K] \;=\; n\,.$$

→ #3

D.3 Separabilität (IV) – Beweis Proposition 2 (#3)

• Um $a \in L$ mit paarweise verschiedenen Bildern $\sigma_i(a)$ in L' zu finden, setzt man

$$\xi_{ij} := \sigma_i(x) - \sigma_j(x)\,,\ \eta_{ij} := \sigma_i(y) - \sigma_j(y) \quad \text{für } i \neq j$$

und betrachtet das Polynom

$$g := \prod_{i \neq j} (\xi_{ij} + \eta_{ij}\, T) \ \in L'[T]\,.$$

• Für jeden Faktor gilt $\xi_{ij} + \eta_{ij}\, T \not\equiv 0$, weil zwei verschiedene Einbettungen $\sigma_i \neq \sigma_j$ nicht auf beiden Erzeugenden x, y gleiche Werte annehmen können.

• Damit gilt auch $\boxed{g \not\equiv 0}$.

→ #4

D.3 Separabilität (IV) – Beweis Proposition 2 (#4)

• Wegen $\#K = \infty$ gibt es ein $c \in K$ mit $g(c) \neq 0$, also

$$\xi_{ij} + c\,\eta_{ij} \neq 0 \quad \text{für alle } i \neq j\,.$$

• Einsetzen in die Definition von ξ_{ij}, η_{ij} und Umformen liefert

$$\sigma_i(x + cy) \neq \sigma_j(x + cy) \quad \text{für alle } i \neq j\,. \qquad \boxed{\checkmark}$$

Zurück zur Galois-Theorie ...

→ D.4

D.4 Beispiele von Galois-Gruppen #

• Erinnerung an die Galois-Gruppenordnungs-Körpergrad-Formel aus D.1:

Für eine (stets als endlich vorausgesetzte) Galois-Erweiterung L/K (d.h. normal und separabel) gilt

$$\boxed{\#\,\mathrm{Gal}(L/K) \ = \ [L:K]}\,.$$

• Erinnerung an die Beispiele von Galois-Erweiterungen aus D.1:

$$\mathbb{Q}(\sqrt{d})/\mathbb{Q},\ \ \mathbb{F}_q/\mathbb{F}_{q'}\,,\ \ \mathbb{C}/\mathbb{R},\ \mathbb{Q}(\zeta_m)/\mathbb{Q},$$
$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q},\ \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}\ \ldots$$

• Erinnerung an die zugehörigen Galois-Gruppen: ???

→ #2

D.4 Beispiele von Galois-Gruppen (#2)

Übung:

- Es genügt, die Wirkung auf den Erzeugenden zu beschreiben:
- $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \left\{\mathrm{id}_L,\, \kappa : \left[\sqrt{d} \mapsto -\sqrt{d}\right]\right\}$ (Konjugation des quadratischen Zahlkörpers),
- $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'}) = \langle \phi_{q'} \rangle$ mit $\phi_{q'} \colon a \mapsto a^{q'}$ („relativer Frobenius-Homomorphismus“)
- $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \kappa : z \mapsto \overline{z}\}$ (komplexe Konjugation)
- $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \left\{\pi_k : [\zeta_m \mapsto \zeta_m^k]\,;\ 1 \leqq k \leqq m-1\,,\ (k,m) = 1\right\}$
- Wie sehen die anderen Gruppen aus?

→ #3

• Skizzieren hier nur den Fall $\boxed{L/K := \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}}$ (Zerfällungskörper von $f := T^4 - 2$ über $\mathbb{Q}$):

• Es gilt $[L : K] = 8$ und damit für $G := \mathrm{Gal}(L/K)$ auch $\mathrm{ord}\, G = 8$.

• Mit $w := \sqrt[4]{2}$ (die übliche positive reelle Wurzel) gilt

$$N_f \;=\; \{w, iw, -w, -iw\}$$

• Jeder Automorphismus $\sigma \in G$ bildet N_f in sich ab und induziert damit eine Permutation von N_f.

• Es muss notwendig

$$\sigma(-w) = -\sigma(w) \quad \text{und} \quad \sigma(-iw) = -\sigma(iw)$$

gelten.

→ #4

• Es gibt genau acht derartige Permutationen von N_f, und damit bilden diese die gesamte Galois-Gruppe: Für $\sigma(w)$ gibt es vier Wahlmöglichkeiten; damit ist zugleich $\sigma(-w)$ festgelegt; für $\sigma(iw)$ bleiben dann noch zwei Möglichkeiten.

• Um die Gruppenstruktur zu bestimmen, betrachten wir die folgenden zwei Elemente:

$$\begin{aligned} \rho: &\quad w \mapsto iw\,,\; iw \mapsto -w \\ \kappa: &\quad w \mapsto w\,,\; iw \mapsto -iw \end{aligned}$$

• Es gilt $\mathrm{ord}(\rho) = 4$ (Einschränkung der Multiplikation mit i auf den invarianten Teilkörper $L \subset \mathbb{C}$) und $\mathrm{ord}(\kappa) = 2$ (Einschränkung der komplexen Konjugation).

→ #5

• Für die Untergruppe $\langle\rho\rangle \cong C_4$ gilt $[G : \langle\rho\rangle] = 2$; damit ist sie ein Normalteiler; wegen $\kappa \neq \rho^k$ gilt $G = \langle\rho, \kappa\rangle$.

• Weiter gilt $\kappa\rho = \rho^3\kappa$ (nachrechnen!).

Schlussfolgerung: Somit hat die betrachtete Körpererweiterung $L/K := \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ die Galois-Gruppe

$$\boxed{G \;\cong\; D_4}$$

(Diedergruppe).

→ D.5

I: Von der Körpererweiterung zur Galois-Gruppe

(A) Galois-Gruppenordnungs-Körpergrad-Formel: Für eine (hier stets als endlich vorausgesetzte) Galois-Erweiterung L/K gilt

$$\boxed{\#\,\mathrm{Gal}(L/K) \;=\; [L : K]}\,. \qquad \boxed{\checkmark}$$

(B) Galois-Zwischenkörper-Satz: Ist L/K eine Galois-Erweiterung und $L/E/K$ ein Zwischenkörper, so gilt:

(1) L/E ist Galoissch, und die zugehörige Gruppe $\mathrm{Gal}(L/E)$ ist eine Untergruppe von $\mathrm{Gal}(L/K)$.

→ (B), (2)

(2) Wenn sogar E/K normal ist, so induziert jedes $\sigma \in \mathrm{Gal}(L/K)$ durch Einschränkung einen K-Automorphismus von E, und die so definierte Abbildung

$$\mathrm{Gal}(L/K) \xrightarrow{\sigma \mapsto \sigma|_E} \mathrm{Gal}(E/K)$$

ist ein surjektiver Gruppenhomomorphismus mit Kern $\mathrm{Gal}(L/E)$; insbesondere ist dann $\mathrm{Gal}(L/E)$ ein Normalteiler.

Bemerkung: (a) Der Beweis ist mit den bisherigen Vorarbeiten nur noch eine Übungsaufgabe ...

(b) Wie das Beispiel $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ zeigt, ist die Normalitätsbedingung in (2) eine echte Einschränkung an den Zwischenkörper!

→ II

II: Von der Galois-Gruppe zur Körpererweiterung

Bemerkung & Definition (Fixkörper): Ist $H < \mathrm{Aut}(L)$ eine Untergruppe der Automorphismengruppe eines Körpers L, so ist

$$K = L^H := \mathrm{Fix}_L(H) := \{x \in L \,;\, \forall_{\sigma \in H}\ \sigma(x) = x\}$$

ein Teilkörper von L, genannt *Fixkörper* zu H.

(C) Galois-Fixkörper-Satz: Ist L ein Körper und $G < \mathrm{Aut}(L)$ endlich mit Fixkörper $K := L^G$, so ist L/K Galoissch und $\mathrm{Gal}(L/K) \cong G$.

→ (C), (#2)

Beweisskizze (nach der Vorlesung von Herrn Baur im SoSem. 2004): Zu zeigen: L/K endlich, normal, separabel mit Grad $[L:K] = |G| =: n$.

• *Separabilität:* Für bel. $a \in L$ ist Bahn $G \cdot a = \{a_1, \ldots, a_m\}$ der G-Wirkung endlich. Betrachte

$$f_a := \prod_{i=1}^{m} (T - a_i)\,,$$

dann gilt für bel. $\sigma \in G$:

$$f_a^\sigma = \prod_{i=1}^{m} (T - a_i)^\sigma = \prod_{i=1}^{m} (T - \sigma a_i) = f_a\,,$$

also $f_a \in K[T]$; damit a separabel über K vom Grad

$$[K(a):K] = m \mid n\,.$$

→ (C), (#3)

• *Normalität und Endlichkeit:* Ergibt sich aus der folgenden Behauptung.

• *Beh.:* Hat $a \in L$ maximalen Grad $m := [K(a):K]$, so gilt $L = K(a)$. (Beachten: Grade beschränkt wegen $m \mid n < \infty$.)

• *Bew.:* Gäbe es $y \in L \setminus K(a)$, so hätte die (separable) KE $K(a,y)/K$ ein primitives Element, und dieses hätte dann notwendig größeren Grad.

• Damit also $L = K(N_{f_a})$ normal über K, nach Konstruktion endlich, und $G < \mathrm{Gal}(L/K)$, also

$$n = |G| \leqq |\mathrm{Gal}(L/K)| = [L:K] = [K(a):K] = m \leqq n\,;$$

somit $|G| = |\mathrm{Gal}(L/K)| = n = [L:K]$ und deshalb $G = \mathrm{Gal}(L/K)$. ✓

• Fehlt noch Analogon zur Aussage (2) des Zwischenkörper-Satzes (B); dieses folgt aus (D).

→ (D)

D.5 Kernaussagen der Galois-Theorie II, (D)

(D) Konjugierten-Satz: Sei $L/E/K$ Zwischenkörper (dabei L/K nicht als GALOIS-Erw vorausgesetzt!); dann gilt für jeden K-Automo $\sigma \in \mathrm{Aut}_K(L)$ die Beziehung

$$\mathrm{Aut}_{\sigma(E)}(L) = \kappa_\sigma\Big(\mathrm{Aut}_E(L)\Big)\,.$$

Beweisidee: Das folgt sofort aus der Betrachtung der Wirkung

$$(\sigma, E) \mapsto \sigma(E)$$

von $\mathrm{Aut}_K(L)$ auf der Menge der Zwischenkörper, weil $\mathrm{Aut}_E(L)$ dabei die Stabilisatorgruppe zu E ist: Stabilisatorgruppen längs einer Bahn sind konjugiert. ✓

• Haben damit alle Zutaten zusammen ...

→ **D.6: HSGT**

D.6 Hauptsatz der Galois-Theorie (#1)

(Hauptsatz der Galois-Theorie): Es sei L/K eine (endliche) Galois-Erweiterung mit Gruppe $G = \mathrm{Gal}(L/K)$. Es bezeichne $\mathcal{UG}(G)$ den Verband (??...!!) der Untergruppen von G und $\mathcal{ZK}(L/K)$ den Verband (??...!!) der Zwischenkörper von L/K. Wir betrachten die beiden Abbildungen Fix und Gal im folgenden Diagramm

$$\begin{array}{rccc} \mathrm{Fix}: & \mathcal{UG}(G) & \rightleftarrows & \mathcal{ZK}(L/K) \quad : \mathrm{Gal} \\ & H & \longmapsto & \mathrm{Fix}(H) = L^H \\ & \mathrm{Gal}(L/E) & \longleftarrow & E \end{array} \quad ,$$

die einer Untergruppe $U < G$ den zugehörigen Fixkörper und die einem Zwischenkörper $L/E/K$ die Galoisgruppe $\mathrm{Gal}(L/E)$ zuordnen.

→ HSGT (#2)

D.5 Hauptsatz der Galois-Theorie (#2)

Es gilt:

- Diese Abbildungen sind zueinander inverse Bijektionen, die zudem einen Verbands-Antiisomorphismus darstellen. (In einfacheren Worten besagt das schlichtweg, dass sich unter diesen Bijektionen die Ordnungsrelationen umkehren.)
- Es gilt
$$\#\,\mathrm{Gal}(L/E) = [L:E] \quad \text{und} \quad [L:L^H] = \#H\,.$$
- Ein Zwischenkörper E ist über dem Grundkörper K genau dann normal und damit auch Galoissch, wenn die Untergruppe $\mathrm{Gal}(L/E)$ in $\mathrm{Gal}(L/K)$ normal,, d.h. also ein Normalteiler, ist. In diesem Fall gilt
$$\mathrm{Gal}(E/K) \;\cong\; \mathrm{Gal}(L/K) \;\Big/\; \mathrm{Gal}(L/E)\,.$$