

§4 Körper und Galois Theorie

Erinnerung Ein Körper F ist ein kommutativer Ring mit $1 \neq 0$ und mit $F^\times = F - \{0\}$.

Beispiele sind $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z} \dots$

1. Def Sei F ein Körper. Ein Teilkörper $E \subseteq F$ ist ein Unterring, der ebenfalls ein Körper ist

Bsp $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ Teilkörper

$\mathbb{Z} \subseteq \mathbb{Q}$ kein Teilkörper (aber Teilring)

Man schreibt dann $F|E$ (lies "F über E")

und nennt F eine Erweiterungskörper von E .

Lemma Ist F ein Körper, E ein nichtleeres

Menge von Teilkörpern, dann ist $E = \bigcap E$ ein Teilkörper.

Beweis Für $a, b \in E$ gilt $a+b, -a \in E$ (§ 1.7)

sowie $a \cdot b \in E, 1 \in E, a^{-1} \in E$ falls $a \neq 0$

weil diese Elemente in jedem Teilkörper in E liegen. $\square$

Korollar Ist F ein Körper, $S \subseteq F$ irgendeine Teilmenge, so gibt es einen kleinsten Teilkörper,

der S enthält, nämlich $\langle S \rangle = \bigcap_{\text{Körper}} \{E \subseteq F \mid E \text{ Teilkörper, } S \subseteq E\}$. 187

Nun nennt $\langle \emptyset \rangle_{\text{Körper}} = \bigcap \{E \subseteq F \mid E \text{ Teilkörper}\} = F_0$.

den Primkörper von F .

2. Def Sei F ein Körper, sei $i: \mathbb{Z} \rightarrow F$ der eindeutige Ringhomomorphismus (vgl. ÜA 6.2), $i(k) = k \cdot 1$ mit Kern $\ker(i) = (l) \subseteq \mathbb{Z}$, $l \geq 0$. Man nennt l die Charakteristik von F , $l = \text{char}(F)$.

Bsp $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$

$\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$, p Primzahl.

3. Satz Die Charakteristik eines Körpers ist 0 oder eine Primzahl. Für den Primkörper $F_0 \subseteq F$ gilt:

$$\text{char}(F) = 0 \Rightarrow F_0 \cong \mathbb{Q}$$

$$\text{char}(F) = p > 0 \Rightarrow F_0 \cong \mathbb{Z}/p\mathbb{Z}, \quad p \text{ Primzahl}$$

Beweis Sei $(l) = \ker(i)$, $i: \mathbb{Z} \rightarrow F$, $l \geq 0$.

Dann ist $\mathbb{Z}/(l)$ isomorph zu einem Teilkörper von F , also ein Integritätsbereich. Folglich $l = 0$ oder l Primzahl, vgl. §3, 24.

Für $l > 0$ ist $\mathbb{Z}/(l)$ ein Körper. Wskt ist

$$0, 1, 2 \cdot 1, 3 \cdot 1, \dots, (l-1) \cdot 1 \in F_0 \Rightarrow F_0 = i(\mathbb{Z})$$

$$\cong \mathbb{Z}/(l).$$

Für $k=0$ i.) $i(\mathbb{Z}) \subseteq F_0$, für $a, b \in i(\mathbb{Z})$, [88]
 $b \neq 0$ folgt $\frac{a}{b} \in F_0$, also mit § 3.13

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad} & Q(\mathbb{Z}) = \mathbb{Q} \\ i \searrow & \downarrow \tau & \\ & E & \end{array} \quad i(Q) \subseteq F_0 \Rightarrow F_0 \cong \mathbb{Q}. \quad \square$$

4. Sei $F|E$ ein Erweiterungskörper, sei $u \in F$.

Wir betrachten den Einsetzungshomomorphismus

$$\begin{aligned} \Phi_u: E[T] &\rightarrow F, \quad \Phi_u(a_0 + a_1 T + \dots + a_n T^n) \\ &= a_0 + a_1 u + a_2 u^2 + \dots + a_n u^n \end{aligned}$$

vgl. § 3.23. Wir setzen $E[u] = \Phi_u(E[T])$.

Weiter sei $E(u)$ der von E und u erzeugte
 Teilkörper von F , also $E \subseteq E(u) \subseteq F$.
 Es gibt zwei Fälle.

Fall 1: Φ_u ist injektiv

Dann heißt u transzendent über E .

Sei $E(T) = Q(E[T])$ der Quotientenkörper von
 $E[T]$. Die Elemente von $E(T)$ sind also

rational Funktionen $\frac{f}{h} \quad f, h \in E[T], h \neq 0$

Mit § 3.13 erhalten wir eine injektive

(Ring)homomorphismus $\overline{\Phi}_u: E(T) \rightarrow E(u)$

Lemma Wenn $u \in F$ transzendent ist über E ,

dann ist $\overline{\Phi}_u : E(T) \rightarrow E(u)$ ein Isomorphismus.

Bew. Für $f, h \in E(T)$ ist $f(u) \stackrel{\text{DEF}}{=} \Phi_u(f) \in E(u)$

$$h(u) \stackrel{\text{DEF}}{=} \Phi_u(h) \in E(u)$$

Ist $h \neq 0$, so ist $h(u) \neq 0$ (weil Φ_u injektiv)

$$\text{also } \frac{f(u)}{h(u)} \in E(u) \Rightarrow \Phi_u(E(T)) \subseteq E(u)$$

$$\text{Sowie } u \in \Phi_u(E(T)) \Rightarrow E(u) = \Phi_u(E(T))$$

Da Φ_u injektiv ist, folgt $E(u) \cong E(T)$.

Fall 2 : Φ_u ist nicht injektiv.

Dann heißt u algebraisch über E

Da $E(T)$ ein Hauptidealring ist, ist $\ker(\Phi_u) = (f)$

für ein Polynom $f \in E(T)$. Da $E(u)$ ein Integritäts-

bereich ist, ist (f) ein Primideal (§3.24) und

damit ein maximales Ideal (§3.25), damit ist

$$E[u] = \Phi_u(E(T)) = \{ a_0 + a_1 u + \dots + a_m u^m \mid a_n \in E,$$

$m \geq 0 \}$ ein Körper. Wegen $E[u] \subseteq E(u)$

folgt hier

$$E[u] = E(u).$$

#

Das eindeutige Polynom $\mu_u = T^m + a_{m-1}T^{m-1} + \dots + a_0$

in $E[T]$ mit $(\mu_u) = \ker(\Phi_u)$ heißt dann

Minimalpolynom von u .

(Eindeutig, weil wir Leitkoeffizient $a_m = 1$ haben)

Man nennt dann $E[u] = E(u)$ ein

einfach algebraisches Körpererweiterung mit

primitiver Erzeug. u

5. Beispiel (a) Betrachte $\mathbb{R}|\mathbb{Q}$, $u = \sqrt{2} \in \mathbb{R}$.

Beh $u \notin \mathbb{Q}$. Denn: $u \in \mathbb{Q} \Rightarrow u = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$

$a^2 = 2 \cdot b^2$ aber a^2, b^2 haben eine gerade Anzahl von Primfaktoren, die Anzahl ist eine ungerade (§ 3.27 "Hauptsatz der Arithmetik") ∇

Beh Der Kern von $\Phi_u: \mathbb{Q}[T] \rightarrow \mathbb{Q}[u]$ ist das Ideal $(T^2 - 2)$.

Denn: $T^2 - 2$ hat u als Nullstelle
 $\Rightarrow T^2 - 2 \in \ker(\Phi_u)$. $T^2 - 2$ ist irreduzibel,
in $\mathbb{Q}[T]$, denn sonst $T^2 - 2 = (T - r)(T - s)$

für $r, s \in \mathbb{Q} \Rightarrow r^2 = 2$ und $s^2 = 2$ ∇ $\square$

Folglich gilt $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[T] / (T^2 - 2)$.

(b) Betrachte $\mathbb{R}|\mathbb{Q}$, $u = \pi = 3.14159 \dots$

Kreiszahl, F. von Lindemann 1882;

π ist transzendent über $\mathbb{Q}$, d.h. für

jedes Polynom $h \in \mathbb{Q}[T]$ mit $h \neq 0$

gilt $h(\pi) \neq 0$. $\square$

6. Def Sei $F|E$ ein Erweiterungskörper.

Dann ist F ein Vektorraum über E
(Skalarmultiplikation $E \times F \rightarrow F, (a, v) \mapsto av$)

Der Grad der Körpererweiterung ist $|F:E| = \dim_E(F)$.

Beispiel: $|\mathbb{C}:\mathbb{R}| = 2$, und $|\mathbb{R}:\mathbb{Q}| = \infty$.

Satz Sei $F|E$ ein Erweiterungskörper, sei $u \in F$.

Dann ist u genau dann algebraisch über E ,

wenn gilt $|E(u):E| < \infty$.

Für das Minimalpolynom μ_u ^(von u) gilt dann

$$\deg(\mu_u) = |E(u):E|$$

Bew. Sei $u \in F$ algebraisch über E mit

Minimalpolynom $\mu = \mu_u$. Für $f \in E[T]$

beliebig sich $f = \mu \cdot q + r$, $\deg(r) < \deg(\mu)$

$\Rightarrow f(u) = r(u)$. Folglich ist $1, u, u^2, \dots, u^{m-1}$

ein Erzeugendensystem des Vektorraums $E[u]$,

$m = \deg(\mu)$. Wenn $1, \dots, u^{m-1}$ linear abhängig,

so gäbe es $a_0, \dots, a_{m-1} \in E$ mit

$$a_0 + a_1 u + \dots + a_{m-1} u^{m-1} = 0, \text{ nicht alle } a_i = 0$$

$\Rightarrow f(u) = 0$, $\deg(f) \leq m-1 < \deg(\mu)$,

Aber $f \in (\mu) = \ker(\Phi_u)$ $\nmid$.

Also ist $\dim_E E(u) = n$.

92

Ist u transzendent über E , so ist $1, u, u^2, \dots, u^n, \dots$
linear unabhängig über $E \Rightarrow \dim_E E(u) = \infty$. $\square$

7. Satz Sei $F|E$ und $K|F$ Körpererweiterungen.

Dann sind äquivalent:

(i) $|K:E| < \infty$

(ii) $|K:F| < \infty$ und $|F:E| < \infty$

Sind die Bedingung erfüllt, so gilt

$$|K:E| = |K:F| \cdot |F:E|.$$

Beis. (i) $\Rightarrow$ (ii): Angen., $\dim_E K = n < \infty$. Wähl

ein E -Basis $w_1, \dots, w_n$ von K . Dann ist $w_1, \dots, w_n$

ein F -Erzeugendensystem von $K \Rightarrow \dim_F K < \infty$ und

weil $K \supseteq F \supseteq E$ ist $\dim_E F \leq \dim_E K$. $\square$

(ii) $\Rightarrow$ (i): Sei $u_1, \dots, u_l$ ein E -Basis von F ,

sei $v_1, \dots, v_m$ ein F -Basis von K . Beh: die

Elemente $\{u_i v_j \mid i=1, \dots, l, j=1, \dots, m\}$ bilden eine E -
Basis von K .

$$\text{Denn: } z \in K \Rightarrow z = \sum_{j=1}^m \xi_j v_j \quad \xi_j \in F$$

$$\Rightarrow \xi_j = \sum_{i=1}^l \alpha_{ij} u_i, \quad \alpha_{ij} \in E$$

$$\Rightarrow z = \sum_{j=1}^m \sum_{i=1}^l \alpha_{ij} u_i v_j, \quad \text{also ein Erzeugendensystem.}$$

Linear unabhängig: angenommen, $\beta_{ij} \in E$ mit

$$\sum_{j=1}^m \sum_{i=1}^l \beta_{ij} u_i v_j$$

$$\beta_{ij} u_i \in F$$

$$\Rightarrow \sum_{i=1}^l \beta_{ij} u_i = 0 \text{ für alle } j \Rightarrow \text{alle } \beta_{ij} = 0$$

□

8. Def (a) Ein Polynom der Form $a_0 + a_1 T + \dots + a_{m-1} T^{m-1} + T^m$ heißt normiert ($m \geq 1$)

(b) Ist $F|E$ ein Körpererweiterung, $u_1, \dots, u_m \in F$, so ist $E(u_1, \dots, u_m)$ der von $E \cup \{u_1, \dots, u_m\} \subseteq F$ erzeugte Teilkörper, vgl. §4,1.

(c) Sei $F|E$ ein Körpererweiterung, sei $f \in E[T]$ normiert. Wir nennen F ein Zerfällungskörper von f , wenn es $u_1, \dots, u_m \in F$ gibt, $m = \deg(f)$, mit $f = (T - u_1)(T - u_2) \dots (T - u_m)$ und wenn $F = E(u_1, \dots, u_m)$.

Satz Sei E ein Körper, sei $f \in E[T]$ normiert, $\deg(f) = m$. Dann existiert ein Zerfällungskörper $F|E$ von f , mit $|F:E| \leq \infty$.

Beweis Schritt $f = q_1 \cdots q_n$, $q_i \in E[T]$

94

irreduzibel + normiert ($E[T]$ ist faktoriell, weil euklidisch,
 $f \neq 0$, $f \notin E[T]^*$), $n \leq m$

Induktion nach $m-n$.

$m=n$: $\deg(q_i) = 1$ also $q_i = (T - u_i)$, $u_i \in E$
set $F = E$, fertig.

$m-n > 0$: $0 \in \deg(q_1) \geq 2$ (nicht alle q_i haben
Grad 1). Dann ist $(q_1) \subseteq E[T]$ ein maximales
Ideal (vgl. § 3.25) also ist $F_1 = E[T]/(q_1)$
ein Körper nach § 3.24. Via $E \hookrightarrow E[T] \xrightarrow{p} F_1$
können wir E als Teilkörper von F_1 auffassen;

$p(h) = h + (q_1)$ ist Kern (q_1) und $(q_1) \cap E = \{0\}$.

Wir setzen $u_1 = p(T) \in F_1$.

Dann ist u_1 eine Nullstelle von $q_1 \in F_1[T]$, denn:

$$q_1 = a_0 + a_1 T + \dots + T^l$$

$$q_1(u) = a_0 + a_1 u_1 + \dots + u_1^l = \underbrace{a_1 + a_2 T + \dots + T^l}_{= q_1} + (q_1) = 0$$

In $F_1[T]$ ist also $q_1 = (T - u_1) \tilde{q}_1$

nach § 3.23, $f = (T - u_1) \cdot \tilde{q}_1 \cdot q_2 \cdots q_n$

Nach Induktionsannahme gibt es eine Körpererweiterung

195

$F|F_1$ sowie $u_2, \dots, u_m \in F$ mit

$F = F_1(u_2, \dots, u_m)$ sowie $f = (T - u_2) \cdots (T - u_m)$

Wobei ist $F_1 = E(u_1)$, also $F = E(u_1, u_2, \dots, u_m)$. $\square$

$\neq$

9. Demostr. (a) Sind E, F Körper, $\sigma: E \rightarrow F$

ein Ringhomomorphismus (= Körperhomomorphismus), so

ist σ injektiv, denn $(0) = \{0\}$ sowie $(1) = E$ sind die einzigen Ideale in E .

(b) Ein Ringhomomorphismus $\sigma: E \rightarrow F$ setzt

sich fort zu einem Ringhomomorphismus $\sigma: E[T] \rightarrow F[T]$

via $\sigma(a_0 + a_1 T + \dots + a_m T^m) = \sigma(a_0) + \sigma(a_1)T + \dots + \sigma(a_m)T^m$

(c.) Ist $F|E$ eine Erweiterungskörper, $u \in F$ algebraisch

über E mit Minimalpolynom $\mu = \mu_u$, so ist

μ irreduzibel in $E[T]$, denn (μ) ist ein

Primideal und $\mu \neq 0$.

10. Lemma Sei $F|E$ ein Erweiterungskörper,
 K ein weiterer Körper, $\sigma: E \rightarrow K$ ein Ring-
 Homomorphismus. Sei $u \in F$ algebraisch über E
 mit Minimalpolynom μ . Dann hat σ
 genau so viele Fortsetzungen $\bar{\sigma}: E[u] \rightarrow K$
 wie $\sigma(\mu) \in K[T]$ Nullstellen in K hat.

$$\begin{array}{ccc} E[u] & & \\ \uparrow & \searrow \bar{\sigma} & \\ E & \xrightarrow{\sigma} & K \end{array}$$

Bew. Wenn $\bar{\sigma}$ existiert, dann ist $\bar{\sigma}(u)$ eine
 Nullstelle von $\sigma(\mu)$. Die Existenz von
 Nullstellen von $\sigma(\mu)$ ist also notwendig.

Sei $v \in K$ eine Nullstelle von $\sigma(\mu)$. Betrachte
 den Homomorphismus $\varphi: E[T] \rightarrow K$, $f \mapsto \sigma(f)(v)$

Dann ist $\mu \in \ker(\varphi)$ -invariant $\Rightarrow (\mu) = \ker(\varphi)$,
 wie erhalten wir den Homomorphismus ein

$$\begin{array}{ccc} \text{Homomorphismus} & E[T] / (\mu) & \xrightarrow{\bar{\varphi}} K \\ \bar{\sigma} & \cong \downarrow & \nearrow \bar{\sigma} \\ & E[u] & \end{array}$$

mit $\bar{\sigma}(u) = v$. Da $E[u]$ von $E[u]$
 erzeugt wird, legt $\bar{\sigma}(u) = v$ den Homomorphismus
 $\bar{\sigma}$ eindeutig fest. □

11. Satz Sei E ein Körper, $f \in E[T]$ mit
normiert. Seien $F|E$ sowie $\tilde{F}|E$ zer-
fällungskörper von f über E . Dann gibt
es Isomorphismen $\tau: F \xrightarrow{\sim} \tilde{F}$ mit $\tau|_E = \text{id}_E$.

$$\begin{array}{ccc} F & \xrightarrow[\cong]{\tau} & \tilde{F} \\ \uparrow & & \uparrow \\ E & = & E \end{array}$$

Die Anzahl r dieser Isomorphismen ist
 $r \leq |F:E|$. Falls alle Nullstellen
 $\alpha_i \in F$, $f = (T - \alpha_1) \dots (T - \alpha_m)$

paarweise verschieden sind, so ist $r = |F:E|$.
In anderen gilt $\tilde{F} \cong F$.

Beweis Wir betrachten die etwas allgemeinere Situation

$$\begin{array}{ccc} F & \xrightarrow[\cong]{\tau} & \tilde{F} \\ \uparrow & \text{(gesucht)} & \uparrow \\ E & \xrightarrow[\cong]{\sigma} & \tilde{E} \end{array}$$

$E \xrightarrow[\cong]{\sigma} \tilde{E}$ Isomorphismen
 F zerfällungskörper von f
 $\tilde{F}$ zerfällungskörper von $\sigma(f)$

Induktion nach $|F:E|$ (nach § 4.8 dürfte)
wir annehmen, $|F:E| < \infty$)

$|F:E| = 1 \iff F = E$, $f = (T - \alpha_1) \dots (T - \alpha_m)$
 $\alpha_i \in E$

$\Rightarrow \tilde{F} = (T - \sigma(\alpha_1)) \dots (T - \sigma(\alpha_m))$, also
 $\tilde{F} = F$, $\sigma = \tau$, fertig.

$|F: E| \geq 2$ Schritt $F = q \cdot h$, q irreduzibel, $\deg(q) = l \geq 1$ * 88
 q normiert in $E[T]$, h normiert oder $h=1$

$$q = (T - u_1) \cdots (T - u_l) \text{ in } E[T]$$

$$h = (T - u_{l+1}) \cdots (T - u_m) \text{ in } E[T]$$

Es gilt $q = \mu_{u_1}$, denn $q(u_1) = 0$ und q_1 ist irreduzibel in $E[T]$

$$\text{Schritt } g(q) = (T - v_1) \cdots (T - v_l) \text{ in } \tilde{F}[T]$$

Nach Lemma §4.10 gibt es genau k

$$\begin{array}{ccc} \text{Fortsetzung } \tau_i: & E[u_1] & \xrightarrow[\cong]{\tau_i} \tilde{E}[v_i] \\ \uparrow & & \downarrow \\ E & \xrightarrow{\quad s \quad} & \tilde{E} \end{array}$$

$$k = |\{v_1, \dots, v_l\}| \leq l.$$

Nun ist $F|E[u_1]$ bzw. $\tilde{F}|\tilde{E}[v_i]$ ein Zerfällungskörper von F über $E[u_1]$ bzw. $\tilde{E}[v_i]$.

$$\text{Wit } |F: E| = |F: E[u_1]| \cdot \underbrace{|E[u_1]: E|}_{= l \geq 2}$$

$$\begin{array}{ccc} \text{Nach Induktionsannahme hat} & F & \dashrightarrow \tilde{F} \\ \uparrow & & \uparrow \\ E[u_1] & \xrightarrow[\cong]{\tau_i} & \tilde{E}[v_i] \end{array}$$

(höchstens $|F: E[u_1]|$ viele) Fortsetzungen.

Insgesamt: Es gibt Fortsetzungen, Anzahl $\leq |F: E|$

* Nicht alle irreduziblen Faktoren von F haben Grad 1, da sonst $F = E$.

$$\text{und } F \cong \tilde{F}.$$

99

Wenn die u_i paarweise verschieden sind, erhalten wir
so genau die Fortsetzungen.

Ist schließlich $\sigma: F \rightarrow \tilde{F}$ ihr Fortsetzung,

so folgt $\sigma(E[u_i]) = \tilde{E}[\sigma(u_i)]$ wie oben,

damit ist σ wie oben konstruiert. □

12. Def Sei E ein Körper, $f \in E[T]$. Wie

heißt $a \in E$ eine k -fache Wurzel von f ,

$k \geq 1$, wenn $f = (T-a)^k \cdot h$, $h \in E[T]$.

Wir definieren wir den Ableitungsoperator

$$D: E[T] \rightarrow E[T]$$

$$D(a_0 + \dots + a_m T^m) = a_1 + 2a_2 T + \dots + m a_m T^{m-1}$$

$$\text{Es folgt } D(f \cdot h) = (Df)h + f \cdot (Dh)$$

(Leibnizregel $\rightarrow$ Ü 4)

Insbesondere: ist a eine k -fache Wurzel

von f mit $k \geq 2 \Rightarrow T-a \mid Df$, denn

$$\begin{aligned} f &= (T-a)^2 \cdot h \Rightarrow Df = 2(T-a)h + (T-a)^2 Dh \\ &= (T-a)(2h + (T-a) Dh) \end{aligned}$$

Lemma Sei E ein Körper, sei $f \in E[T]$ 100

normiert. Dann sind äquivalent:

(i) $1 \in \text{ggT}(f, Df)$ (in $E[T]$)

(ii) f hat kein Mehrfachwurzel in
Zerfällungskörper $F|E$ (kein k -fachen
Wurzeln mit $k \geq 2$),

Beweis: (ii) $\Rightarrow$ (i): Sei $u \in F$ Nullstelle

$\Rightarrow f = (T-u)g$ in $F[T]$, $(T-u) \nmid g$

$Df = g + (T-u)Dg \Rightarrow (T-u) \nmid Df$

$\Rightarrow$ kein irreduzibler Faktor von f teilt Df in $E[T]$.

$\Rightarrow 1 \in \text{ggT}(f, Df)$ in $E[T]$.

(i) $\Rightarrow$ (ii): $1 = g \cdot f + h \cdot Df$ $\forall g, h \in E[T]$

$u \in F$ Nullstelle von $f \Rightarrow 1 = h(u) \cdot Df(u)$

$\Rightarrow$ kein Nullstelle von f ist Nullstelle von Df

$\Rightarrow (T-u)^2 \nmid f$

□ #

13. Def Sei E ein Körper. Ein normiertes

Polynom $f \in E[T]$ heißt separabel, wenn
 f in Zerfällungskörper $F|E$ kein Mehrfachwurzel
hat.

Satz Ein irreduzibles normiertes Polynom f
ist genau dann separabel, wenn $\forall Df \neq 0$.

Beim Nach Lemma §4.12, gilt für f

$$f \text{ separabel} \Leftrightarrow 1 \in \text{ggT}(f, Df) \Rightarrow Df \neq 0 \text{ (mit } f \neq 1)$$

$$\text{Ist } Df \neq 0, \text{ so folgt } f \nmid Df \Rightarrow 1 \in \text{ggT}(f, Df) \\ \uparrow f \text{ irreduzibel.} \quad \square$$

Beispiel Ist F ein Körper mit $\text{char}(F) = p > 0$, dann gilt für $f = T^p - a$, dass $Df = pT^{p-1} = 0$, aber $f \neq \text{const.}$

14. Def Ein Körper E heißt perfekt, wenn jedes irreduzible normierte Polynom $f \in E[T]$ separabel ist.

Lemma Jeder Körper E mit $\text{char}(E) = 0$ ist perfekt.

Beim Ist $f \neq 0$ normiert, $f = a_0 t^m + \dots + T^m$, so ist

$$Df = a_1 + \dots + \underbrace{mT^{m-1}}_{\neq 0} \neq 0. \quad \square$$

Was ist mit $\text{char}(E) \neq 0$?

Def Sei E ein Körper mit $\text{char}(E) = p > 0$.

Der Frobenius-Endomorphismus ist der Ringhomomorphismus $F_r: E \rightarrow E, a \mapsto a^p$.

Das ist ein Homomorphismus, denn:

$$(a \cdot b)^p = a^p \cdot b^p, \quad 1^p = 1$$

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

$$\text{denn } \binom{p}{k} \in p\mathbb{Z} \text{ für } 0 < k < p.$$

15. Lemma Sei E ein Körper mit $\text{char}(E) = p > 0$,

sei $a \in E$. Dann sind äquivalent;

(i) $T^p - a$ ist irreduzibel

(ii) es gibt kein $b \in E$ mit $b^p = \text{Fr}_p(b) = a$.

Beiw. Wenn $a = b^p$, dann $T^p - a = (T - b)^p$, also

(i) $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (i): Angenommen, $T^p - a$ ist reduzibel, also

$T^p - a = g \cdot h$, g, h normiert. Sei $F|E$ Zerfällungskörper, sei $b \in F$ eine Wurzel, also $b^p = a$.

Dann ist in $F[T]$ $T^p - a = (T - b)^p$. Es folgt

$g = (T - b)^k$, $1 \leq k < p \Rightarrow b^k \in E$.

Schreibe $l \cdot k + m \cdot p = 1$ (Lemma von Bézout)

$\Rightarrow b = (b^k)^l \cdot (b^p)^m \in E \Rightarrow T - b \in E[T]$ $\square$

Satz Sei E ein Körper, $\text{char}(E) = p > 0$.

Dann sind äquivalent: (i) E ist perfekt

(ii) $E = \text{Fr}_p(E)$, d.h. $E = \{a^p \mid a \in E\}$

Beiw. Angenommen, $f \in E[T]$ ist normiert,

irreduzibel, nicht separabel, $f = a_0 + \dots + T^m$.

Dann ist $Df = 0$, also $f = \sum_{k=0}^l a_{pk} T^{pk}$

Wäre es mindestens ein $a_{p \cdot k} \notin \text{Fr}_p(E)$, dann

sonst wäre $f = \left(\sum_{k=0}^l b_k T^k \right)^p$, $b_k^p = a_{p \cdot k}$

reduzibel.

Also ist $\text{Fr}_p(E) \neq E$.

(10)

Ist $a \in E$, $a \notin \text{Fr}_p(E)$, so ist $T^p - a$ irreduzibel nach dem vorig. Lemma, aber nicht separabel. $\square$

Korollar Jeder endliche Körper ist perfekt.

Beweis Sei E endlich $\Rightarrow \text{char}(E) = p > 0$.

Dann ist Fr_p injektiv, also bijektiv $\Rightarrow E$ perfekt. $\square$

16. Def Ein Erweiterungskörper $F|E$ heißt algebraisch über E , wenn jedes $u \in F$ algebraisch ist über E .

Aus §4.6 folgt: wenn $|F:E| < \infty$, dann ist $F|E$ algebraisch.

[$u \in F \Rightarrow \dim_E E(u) < \infty \Rightarrow u$ algebraisch]

Im folgenden interessieren uns algebraische Körpererweiterungen.

17. Def Sei $F|E$ eine Körpererweiterung, sei $u \in F$ algebraisch über E . Wir nennen u separabel über E , falls das Minimalpolynom μ_u separabel ist. Wir nennen $F|E$ eine separabel Erweiterung, wenn jedes $u \in F$ separabel über E ist.

18. Satz Sei E ein Körper. Dann sind
 äquivalent: (i) E ist perfekt.
 (ii) jede algebraische Erweiterung $F|E$ ist
 separabel.

Beweis (i) $\Rightarrow$ (ii): Angenommen, $f \in E[T]$

ist normal, irreduzibel, nicht separabel. Dann

ist $Df = 0 \Rightarrow \text{char}(E) = p > 0$, $f = \sum_{k=0}^1 a_{p \cdot k} T^{pk}$

$a_{p \cdot k} = b_k^p$ für $b_k \in E \Rightarrow f = \left(\sum_{k=0}^e b_k T^k \right)^p$

$\hookrightarrow$ weil f irreduzibel.

Ist $F|E$ algebraisch, $u \in F$ mit Minimalpolynom

$\mu_u \in E[T]$, so ist μ_u irreduzibel, also separabel $\square$

(ii) $\Rightarrow$ (i): O.E. $\text{char}(E) = p > 0$. Sei $\alpha \in E$,
 betrachte Zerfällungskörper $F|E$ von $T^p - \alpha = f$.

D., $Df = 0$ ist f nicht irreduzibel, also nach

§ 4, 15 $\alpha \in \text{Fr}_p(E)$. $\square$

Insbesondere: ist $\text{char}(E) = 0$ oder ist E

endlich, so ist jede algebraische Erweiterung

$F|E$ auch separabel.

19. Def Sei E ein Körper. Dann ist

$$\text{Aut}(E) = \{ \sigma: E \rightarrow E \mid \sigma \text{ Isomorphism} \}$$

die Automorphismengruppe von E . (Verschüpfung ist Komposition von Abbildungen).

Beobachtung Ist $\sigma \in \text{Aut}(E)$, so ist die

$$\text{Fixpunktmenge } \text{Fix}(\sigma) = \{ a \in E \mid \sigma(a) = a \} \subseteq E$$

ein Teilkörper, denn $0, 1 \in \text{Fix}(\sigma)$,

a, b Fixpunkte $\Rightarrow a+b, a \cdot b, a^{-1}$ Fixpunkte.
 $a \neq 0$

Ist $H \subseteq \text{Aut}(E)$ eine Untergruppe, so ist

$$\text{Fix}(H) = \{ a \in E \mid \text{für alle } \sigma \in H \text{ ist } \sigma(a) = a \}$$

ein Teilkörper, $\text{Fix}(H) = \bigcap_{\sigma \in H} \text{Fix}(\sigma)$.

Ist $K \subseteq E$ ein Teilkörper von E , so set

$$\text{wir } \text{Aut}_K(E) = \{ \sigma \in \text{Aut}(E) \mid K \subseteq \text{Fix}(\sigma) \}.$$

Dann ist $\text{Aut}_K(E) \subseteq \text{Aut}(E)$ eine Untergruppe

Beispiel Sei E ein Körper, $\text{char}(E) \neq 2$, sei

$f = T^2 - a$ irreduzibel (d.h. a ist kein Quadrat in E)

(etwa $E = \mathbb{R}, a = -1$ oder $E = \mathbb{Q}, a = 2$.)

Sei $F \mid E$ ein zerfallender Körper $\Rightarrow T^2 - a = (T-u)(T+u)$

für ein $u \in F, F = E[u]$

Weg $u^2 = a \in E$ ist $1, u$ ein E -Basis von

$F = E[u]$. Weiter ist $\sigma: x + uy \mapsto x - uy$, $x, y \in E$ ein Automorphismus von F (nachrechnen).

Ist $\alpha \in \text{Aut}_E(F)$, so ist $\alpha(u) = \pm u$, denn $\pm u$ sind die Quadratwurzeln von $a \in E$.

Es folgt $\text{Aut}_E(F) = \{\text{id}_F, \sigma\}$.

Etwa $\text{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\text{id}_{\mathbb{C}}, [z \mapsto \bar{z}]\}$

$\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{\text{id}_{\mathbb{Q}(\sqrt{2})}, [x + \sqrt{2}y \mapsto x - \sqrt{2}y]\}$.
#

20. Satz (Dedekinds Lemma)

[R. Dedekind, 1831-1916, *Id. Mathematik*]

Seien E, F Körper, sei $\text{Hom}(E, F)$ die Menge aller Ringhomomorphismen $E \rightarrow F$. Dann ist

$\text{Hom}(E, F) \subseteq F^E$ linear unabhängig im F -Vektorraum F^E aller Abbildungen $E \rightarrow F$.

Beweis Angenommen, das wäre falsch. Wähle

$\sigma_0, \dots, \sigma_n \in \text{Hom}(E, F)$ paarweise verschieden

mit $\sigma_0 = \sum_{k=1}^n a_k \sigma_k$ $a_k \in F$ und

n minimal.

Dann $\sigma_0(u) = \sum_{k=1}^n a_k \sigma_k(u)$

für alle $u \in E$.

107

sowie $\sigma_0(u) \sigma_0(v) = \sum_{k=1}^n a_k \sigma_k(u) \sigma_0(v)$

$$\sigma_0(uv) = \sum_{k=1}^n a_k \sigma_k(uv) = \sum_{k=1}^n a_k \sigma_k(u) \sigma_k(v),$$

also $0 = \sum_{k=1}^n a_k \underbrace{(\sigma_k(v) - \sigma_0(v))}_{= b_k} \sigma_k(u)$

Wegen Minimalität des Gegenbeispiels ist $b_k = 0$ für

$k = 1, \dots, n$. Für jedes k gibt es ein $u \in F$ mit

$$\sigma_k(u) \neq \sigma_0(u) \Rightarrow \text{alle } a_k = 0 \quad \text{⚡} \quad \square$$

Korollar Sei $F|E$ sowie $K|E$ Körper-

erweiterungen, mit $|F:E| = n < \infty$. Dann gibt

es höchstens n verschiedene $\sigma \in \text{Hom}(F, K)$

mit $\sigma|_E = \text{id}_E$,

$$\begin{array}{ccc} F & \xrightarrow{\sigma} & K \\ \uparrow & & \uparrow \\ E & \xlongequal{\quad} & E \end{array}$$

Beweis Sei $u_1, \dots, u_n$ eine E -Basis von F .

Angenommen, $\sigma_0, \dots, \sigma_m$ wären paarweise

verschiedene Lösungen, also $\sigma_i \neq \sigma_j$ für $i \neq j$

$$\sigma_i: F \rightarrow K, \quad \sigma_i|_E = \text{id}_E.$$

1108

Betrachte das LGS $\sum_{k=0}^m \sigma_k(u_l) x_k = 0, \quad l=1, \dots, m.$

Dann gibt es eine Lösung $(c_0, \dots, c_m) \neq (0, \dots, 0),$

also $\sum_{k=0}^m \sigma_k(u_l) c_k = 0 \quad l=1, \dots, m.$

Sei $u \in F, \quad u = \sum_{l=1}^m a_l u_l, \quad a_l \in E.$

$$\sum_{k=0}^m \sigma_k(u) c_k = \sum_{k=0}^m \left(\sum_{l=1}^m \sigma_k(a_l) \sigma_k(u_l) \right) c_k = 0,$$

also $\sum_{k=0}^m c_k \sigma_k = 0, \quad \text{ein Widerspruch zum Satz. } \square$

21. Theorem (Satz von Artin)

[E. Artin, 1898-1962, österr. Mathematiker,
zusammen mit E. Noether Begründer der
modernen Algebra]

Sei F ein Körper, sei $G \subseteq \text{Aut}(F)$ eine
endliche Untergruppe, sei $K = \text{Fix}(G) \subseteq F.$

Dann gilt $|F:K| = |G|.$

Beweis Nach §4.20 gilt $|G| \leq |F:K|$.

(das ist auch wahr, wenn $|F:K| = \infty \dots$)

Sei $|G| = m$. Angenommen, es gibt $u_0, \dots, u_m \in F$ linear unabhängig über K . Betrachte das LGS

$$\sum_{k=0}^m \sigma(u_k) x_k = 0, \text{ für } \sigma \in G \text{ in } F^{m+1}$$

Wähle eine Lösung $(c_0, \dots, c_m) \neq (0, \dots, 0)$ in mit möglichst vielen Einträgen $c_i = 0$.

OE $c_0 = 1$, also $\sigma(u_0) = - \sum_{k=1}^m \sigma(u_k) c_k$

für alle $\sigma \in G$. Insbesondere $u_0 = - \sum_{k=1}^m u_k c_k$.

Dann ist mindestens ein $c_k \notin K$, OE $c_1 \notin K$.

Wähle $\tau \in G$ mit $\tau(c_1) \neq c_1$.

$$\tau^{-1} \sigma(u_0) = - \sum_{k=1}^m \tau^{-1} \sigma(u_k) c_k$$

$$\Rightarrow \sigma(u_0) = - \sum_{k=1}^m \sigma(u_k) \cdot \tau(c_k)$$

$$\text{also } 0 = \sum_{k=1}^m \sigma(u_k) \underbrace{(\tau(c_k) - c_k)}_{= b_k}$$

$$b_0 = 0$$

$$b_1 \neq 0$$

$$c_k = 0 \Rightarrow b_k = 0$$

$\Rightarrow$ Lösung $(0, \underbrace{b_1}_{\neq 0}, \dots, b_m)$ mit mehr

Einträge $\neq 0$

4

□

22 Def Ein Körpererweiterung $F|E$ heißt

normal, wenn für jedes irreduzible normierte Polynom $f \in E[T]$, dass in F ein Wurzel hat, f in Linear Faktoren in $F[T]$ zerfällt.

Ein Erweiterungen $F|E$ heißt Galois-Erweiterung, wenn $|F:E| < \infty$ und wenn $F|E$ normal und separabel ist.

[E. Galois, 1811-1832, franz. Mathematik]

Theorem Sei $F|E$ eine Körpererweiterung.

Dann sind äquivalent:

- (i) F ist Zerfällungskörper eines separablen normierten Polynoms $f \in E[T]$
- (ii) $E = \text{Fix}(G)$ für eine endliche Gruppe $G \leq \text{Aut}(F)$
- (iii) $F|E$ ist eine Galois-Erweiterung.

Wenn die Bedingung erfüllt sind, so gilt

$G = \text{Aut}_E(F)$ und man nennt $G = \text{Gal}(F|E)$ die Galois-Gruppe von $F|E$.

⊗ Nachher wird nur verlangt, dass $F|E$ algebraisch, normal und separabel ist.

(iii)

Beweis: (i) $\Rightarrow$ (ii): Wir set $G = \text{Aut}_E(F)$.

Sei $K = \text{Fix}(G) \supseteq E \Rightarrow G = \text{Aut}_K(F)$.

Nach Artin gilt $|G| = |F:K|$. Da

f separabel ist, $\deg(f) = m$, hat f m paarweise
verschiedene Nullstellen in F . Nach §4.11

gilt $|G| = m = |F:E|$. $\uparrow$ Es folgt $K = E$.

(ii) $\Rightarrow$ (iii): Nach Artin gilt $|F:E| = |G|$.

Sei $f \in E[T]$ normiert und irreduzibel, mit
einer Nullstelle $a \in F$. Setze $\{ \sigma(a) \mid \sigma \in G \}$

$= \{ a_1 = a, \dots, a_m \}$, $a_i \neq a_j$ für $i \neq j$. Es

folgt $f(a_i) = 0$ für $i = 1, \dots, m$. Betrachte

$g = (T - a_1) \cdots (T - a_m)$, dann gilt $\sigma(g) = g$

für alle $\sigma \in G \Rightarrow g \in E[T]$ und $g \mid f$.

Aber f ist irreduzibel, also $g = f$. Damit

ist f separabel und $F|E$ ist normal.

(iii) $\Rightarrow$ (i): Schritt $F = E(b_1, \dots, b_n)$

112

$b_i \in F$ algebraisch mit Minimalpolynom $\mu_i \in E[T]$.

Da $F|E$ Galois-Erweiterung ist, zerfällt jedes

μ_i in $F[T]$ in Linearfaktoren, ohne Mehrfachwurzeln. Ist $\alpha \in F$ Wurzel von μ_i und von μ_j , so folgt also $\mu_i = \mu_j$. Sei $0 \leq$

$$\{ \mu_1, \dots, \mu_n \} = \{ \mu_1, \dots, \mu_r \} \quad \mu_i \neq \mu_j \\ \text{für } 1 \leq i < j \leq r.$$

Dann hat $F = \mu_1 \cdots \mu_r$ kein Mehrfachwurzel,

also ist $F \in E[T]$ separabel und F ist

Zerfällungskörper von F . □

23. Beispiele (a) $E = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$

ist Galois-Erweiterung mit $\text{Gal}(F|E) = \{ \text{id}, \sigma \}$,

$$\sigma(\sqrt{2}) = -\sqrt{2}.$$

Ebenso: $\mathbb{C}|\mathbb{R}$ ist Galois-Erweiterung mit

$$\text{Gal}(\mathbb{C}|\mathbb{R}) = \{ \text{id}, \omega \mapsto \bar{\omega} \}.$$

(b) E beliebiger Körper, $m \geq 1$, Polynome in m Variablen

$$E[T_1, T_2, \dots, T_m] = E[T_1][T_2] \cdots [T_m] \text{ mit}$$

Quotientenkörper $E(T_1, \dots, T_m)$ (rationale Funktionen

in m Variablen. Dann wirkt $\text{Sym}(m)$ auf

$$E(T_1, \dots, T_m) \text{ durch } \sigma(T_i) = T_{\sigma(i)}.$$

Ist $H \subseteq \text{Sym}(m)$ ein Unterperm, so

ist mit $K = \text{Fix}(H) \subseteq E(T_1, \dots, T_m)$ eine
Galois-Erweiterung mit $\text{Gal}(E(T_1, \dots, T_m) | K) = H$.
Mit dem Satz von Cayley folgt: jede endliche
Gruppe ist eine Galois-Gruppe.

(c) Ist E nicht perfekt (also $\text{char}(E) = p > 0$,
 $\text{Fr}_p(E) \neq E$, $a \in E$ kein p -Potenz, so ist
 $f = T^p - a$ irreduzibel (vgl §4, 15). Der (§4.6)
Zerfällungsrang von f ist $|F:E| = p$.
Ist $b \in F$ Nullstelle, so ist $(T-b)^p = f \Rightarrow$
 b ist einzige Nullstelle von f , insbesondere
ist $F|E$ nicht Galois-Erweiterung (und $\text{Aut}_E(F) = \{id\}$).

24. Theorem (Fundamentalsatz der Galois-Theorie)

Sei $F|E$ eine Galois-Erweiterung mit Galois-
Gruppe $G = \text{Gal}(F|E) = \text{Aut}_E(F)$. Sei

$$\mathcal{U} = \{ H \in G \mid H \text{ Untergruppe} \}$$

$$\mathcal{Z} = \{ K \subseteq F \mid K \text{ Teilkörper mit } E \subseteq K \subseteq F \}.$$

Dann sind die Abbildungen

$$\mathcal{U} \rightarrow \mathcal{Z}, \quad H \mapsto \text{Fix}(H) \subseteq F$$

$$\mathcal{Z} \rightarrow \mathcal{U}, \quad K \mapsto \text{Aut}_K(F) \in G$$

zueinander inverse Bijektionen, und die
Formeln gelten.

Wird also dann $[G:H] = | \text{Fix}(H) : E |$

$$|H| = |F : \text{Fix}(H)|$$

und $F/\text{Fix}(H)$ ist Galois-Erweiterung mit Galois-Gruppe $\text{Gal}(F/\text{Fix}(H)) = H$.

Wird gilt: $N \in \mathcal{U}$ ist normal in G genau dann,

wenn $\text{Fix}(N)/E$ normal ist. Dann ist auch

$\text{Fix}(N)/E$ Galois-Erweiterung, mit $\text{Gal}(\text{Fix}(N)/E) \cong G/N$.

Beweis Sei $H \in \mathcal{U}$ und $K = \text{Fix}(H) \in F$. Dann ist

nach §4.22 (ii) F/K Galois mit $\text{Gal}(F/K) = H$,

Wird ist $|H| = |F:K|$ nach Artin, mit Lagrange

$$|G| = [G:H] \cdot |H| \quad \text{folgt} \quad [G:H] = [K:E] \quad (\S 4.7).$$

"

$$|F:E|$$

□

Sei $K \in \mathcal{Z}$. Nach §4.22 (i) ist F Zerfällungskörper

eines separablen normierten Polynoms $f \in E[T] \in K[T]$,

damit ist auch F/K Galois. Sei $H = \text{Aut}_K(F) \cong G$,

dann ist $\text{Gal}(F/K) = H$ und $K = \text{Fix}(H)$.

Also haben wir zwei Paare linearer Abbildungen $U \rightarrow \mathcal{Z}$
 $\mathcal{Z} \rightarrow U$

wie oben.

□

Zu den Normalteilern / normalen Erweitern.

115

Sei $H \in \mathcal{U}$, $\sigma \in G$. Dann gilt $T(\sigma(H)) =$

$$\text{Fix}(\sigma H \sigma^{-1}) = \sigma(\text{Fix}(H))$$

$\Gamma \eta \in H, u \in F$, dann $\sigma \eta \sigma^{-1}(u) = u \Leftrightarrow \eta \sigma^{-1}(u) = \sigma^{-1}(u)$

$$\Leftrightarrow \sigma^{-1}(u) \in \text{Fix}(\eta) \Leftrightarrow u \in \sigma(\text{Fix}(\eta))$$

□

Ist also $N \trianglelefteq G$, so gilt für $K = \text{Fix}(N)$, dass

$$\sigma(K) = K \quad \text{für alle } \sigma \in G. \quad \text{Wegen } N = \text{Aut}_K(F)$$

ist N genau der Kern der G -Wirkung $G \times K \rightarrow K$,

also wirkt G/N auf K mit Fixkörper E .

Damit ist $K|E$ Galois mit $\text{Gal}(K|E) \cong G/N$.

Ist $K \in \mathcal{Z}$ mit $K|E$ normal und ist $a \in K$ mit Minimalpolynom $\mu \in E[T]$, so folgt

$$\mu = (T - a_1) \cdots (T - a_m) \quad \text{in } K[T] \quad (\text{mit } K|E \text{ normal}).$$

Ist $\sigma \in G$, so ist $\sigma(a_i) \in \{a_1, \dots, a_m\}$. Damit

ist also $\sigma(K) \subseteq K$ für jedes $\sigma \in G$, somit

$$\sigma^{-1}(K) \subseteq K \Rightarrow \sigma(K) = K \quad \text{für alle } \sigma \in G.$$

Betrachte $N = \text{Aut}_K(F)$. Dann folgt $N \trianglelefteq G$,

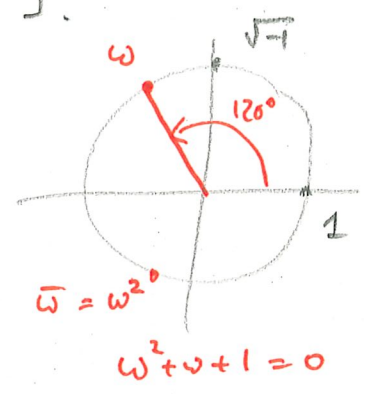
denn: $\sigma \in G, \nu \in N, a \in K \Rightarrow$

$$\underbrace{\sigma \nu \sigma^{-1}(a)}_{\in K} = \sigma \nu^{-1}(a) = a, \quad \text{also } \sigma \nu \sigma^{-1} \in N.$$

□

25. Ein Beispiel $f = T^3 - 2 \in \mathbb{Q}[T]$.

Set $\omega = \exp\left(\frac{2\pi}{3}\sqrt{-1}\right)$



$u_1 = \sqrt[3]{2} \in \mathbb{R}$

$u_2 = \omega \cdot \sqrt[3]{2} \in \mathbb{C}$

$u_3 = \omega^2 \cdot \sqrt[3]{2} \in \mathbb{C}$

Dann gilt $f = (T - u_1)(T - u_2)(T - u_3)$, also

ist $\mathbb{Q}(u_1, u_2, u_3) = \mathbb{Q}(\omega, \sqrt[3]{2}) \subseteq \mathbb{C}$ ein

zerfallungskörper von f . Nach §4.22 (i) ist

$\mathbb{Q}(\omega, \sqrt[3]{2}) | \mathbb{Q}$ ein Galois-Erweiterung.

Wirk gilt $\omega^3 = 1$, $T^3 - 1 = (T - 1)(T^2 + T + 1)$

$\Rightarrow T^2 + T + 1$ ist Minimalpolynom von ω (über $\mathbb{Q}$)

$|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ nach §4.6

$|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$

$|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| = 2$, damit

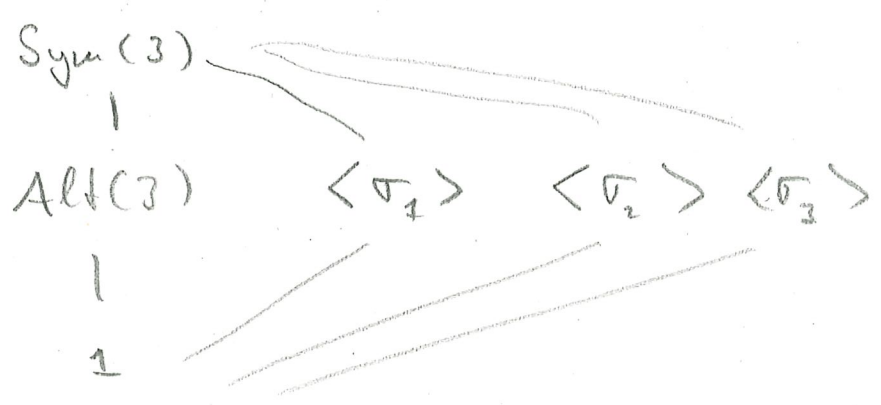
$|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}| = 3 \cdot 2 = 6$. [Ein Basis ist

$1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega \cdot \sqrt[3]{2}, \omega \sqrt[3]{4}.$]

$\Rightarrow |Gal(\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q})| = 6$, die Gruppe operiert

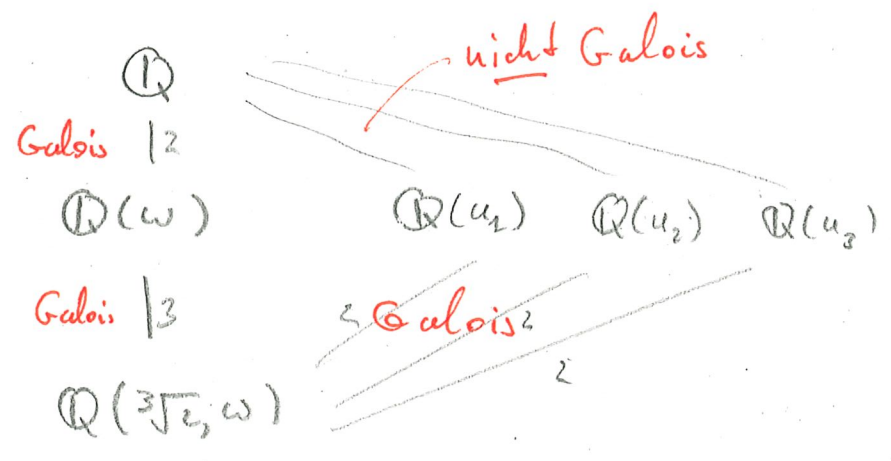
trans auf $\{u_1, u_2, u_3\} \Rightarrow Gal(\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q})$
 $= Sym(\{u_1, u_2, u_3\}) \cong Sym(3)$

Untergruppe von $Sym(3)$:



σ_k vertauscht u_ℓ, u_m für $\{1, 2, 3\} = \{k, \ell, m\}$

Zwischkörper



$\mathbb{Q}(\omega) \mid \mathbb{Q}$ ist auch Galois, denn $\text{Alt}(3) \trianglelefteq \text{Sym}(3)$

$$\begin{aligned}
 \underline{\text{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})} &\cong \frac{\text{Sym}(3)}{\text{Alt}(3)} \\
 &= \{\text{id}, z \mapsto \bar{z}\}
 \end{aligned}$$

Dagegen ist $\mathbb{Q}(u_k) \mid \mathbb{Q}$ nicht Galois, denn

$$|\mathbb{Q}(u_k) : \mathbb{Q}| = 3, \text{ aber } \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(u_k)) = \{\text{id}\}$$

$\mathbb{Q}(u_k)$ ist kein Zerfällungskörper.

