Skript zur Vorlesung Algebra

Prof. Dr. Roman Sauer

Wintersemester 2023/24

Inhaltsverzeichnis

Einführung

§0.1 Motivation

TODO

- Für quadratische Gleichungen der Form $x^2+bx+c=0$, $b,c\in\mathbb{C}$, sind die einzigen Lösungen explizit gegeben durch

$$x_{12}=-\frac{b}{2}\pm\sqrt{\frac{b^2}{4}-c} \tag{1}$$

  Erstmals systematisch behandelt wurden solche Gleichungen von al Khwarizmi ($\sim$ 800 n. Ch.).

- Für kubische Gleichungen der Form

$$x^3+ax^2+bx+c=0,\ a,b,c\in\mathbb{C} \tag{2}$$

  haben Tartaglia und Cardano im 16. Jh. eine explizite Lösungsformel aufgestellt:

  1. Sei o.B.d.A. $x=y-\frac{a}{3}$ für $y\in\mathbb{C}$. Substituiere dies in eq. (2), so dass jetzt mit $p:=b-\frac{a^2}{3}\in\mathbb{C}$, $q:=c+\frac{2a^3-9ba}{27}\in\mathbb{C}$ zu lösen ist:

$$y^3+py+q \tag{3}$$

  2. Substituiere nun $y=u+v$, so dass $y^3=u^3+v^3+3uv(u+v)=u^3+v^3+3uvy$. Dies ähnelt der Gleichung eq. (3), wenn $u^3+v^3=-q$ und $3uv=-p$ gesetzt wird. Versuche nun also,

$$u^3+v^3=-q \tag{4}$$

$$3uv=-p\Leftrightarrow u^3v^3=\frac{-p^3}{27} \tag{5}$$

     zu lösen. Aus eq. (4) ergibt sich, dass u^3,v^3 die quadratische Gleichung $z^2+qz-\frac{p^3}{27}$ lösen. Es kann nun also eq. (1) verwendet werden - man erhält die sogenannte Formel von Cardano: Beachte beim Ziehen der 3. Wurzel in der Formel von Cardano explizit, dass eq. (5) erfüllt bleibt.

- Ähnlich funktioniert das Lösen von polynomiellen Gleichungen 4. Grades mittels Radikalen.

- Für Gleichungen höheren Grades existiert keine explizite Lösungsformel mehr:

  Satz 0.1 (Abel-Ruffini, 1824)**.** *Polynomielle Gleichungen vom Grad ≥ 5 sind im Allgemeinen nicht durch Radikale lösbar.*

Kurz, nachdem dieser Satz bewiesen wurde, kam die Galois-Theorie auf, welche die algebraischen Überlegungen in Gruppentheorie überführt.

Zunächst finden sich im Folgenden noch Wiederholungen einiger gruppen- und zahlentheoretischer Begriffe aus der Linearen Algebra [LA] und Einführung in Algebra und Zahlentheorie [EAZ], die im Verlauf des Skripts eine Rolle spielen.

§0.2 Grundlegende Definitionen aus EAZ und LA

Definition 0.2 (Radikal)**.** TODO

Definition 0.3. Sei $(G,*)$ eine Gruppe und $H \leq G$ eine Untergruppe. Die (Links-)Nebenklasse von $g \in G$ zu H in G ist die Menge

$$gH := \{gh \mid h \in H\}$$

Der Quotient von H in G ist die Menge der Linksnebenklassen:

$$G/H := \{gH \mid g \in G\}$$

Die kanonische Projektion von G auf G/H ist die Abbildung $\pi : G \to G/H, g \mapsto gH$.

Definition 0.4 (Normalteiler, Quotientengruppe)**.** Sei $(G,*)$ eine Gruppe und $H \leq G$ eine Untergruppe. H heißt Normalteiler, wenn H konjugationsinvariant ist, also

$$\forall g \in G.\ gHg^{-1} = H$$

In diesem Fall schreibt man auch $N \trianglelefteq G$. Genau dann, wenn $H \trianglelefteq G$ gilt, ist die Operation $\cdot : G/H \to G/H$ mit $gH \cdot hH := (gh)H$ wohldefiniert und macht $(G/H,\cdot)$ zu einer Gruppe (der sogenannten "Quotientengruppe"von H in G). Weiter ist die kanonische Projektion von G auf H dann ein Gruppenhomomorphismus.

Beispiel 0.5 (Alternierende Gruppe A_n). Sei $n \in \mathbb{N}$, $[n] := \{1,...,n\}$ und $S_n := \{\pi : [n] \to [n] \mid f\ bijektiv\}$ die symmetrische Gruppe auf $[n]$. Sei weiter $I(\pi) := \{(i,j) \in [n] \times [n] \mid i < j, \pi(i) > \pi(j)\}, \pi \in S_n$ die Menge der Inversionen und $sgn(\pi) := (-1)^{|I(\pi)|}$ die Signumsfunktion. Die alternierende Gruppe $A_n := \{\pi \in S_n \mid sgn(\pi) = 0\}$ ist für alle $n \in \mathbb{N}$ ein Normalteiler der symmetrischen Gruppe , also $A_n \trianglelefteq S_n$. Gleichheit gilt nur für $n = 1$. Für alle $n \geq 2$ gilt $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ und die kanonische Projektion $S_n \to S_n/A_n$ stimmt mit der Signumsabbildung überein.

§0.3 Grundlegende Resultate aus EAZ und LA

Lemma 0.6 (Chinesischer Restsatz)**.** *TODO*

Lemma 0.7. *Die alternierende Gruppe A_n wird für alle $n \geq 3$ von 3-Zykeln erzeugt.*

Beweis. **TODO** (Für den Beweis siehe bspw. Satz 2.5.10 im EAZ-Skript von Dr. Stefan Kühnlein.) □

Lemma 0.8. *Sei $(G,*)$ eine abelsche Gruppe. Dann ist jede Untergruppe $H \leq G$ bereits ein Normalteiler von G.*

Beweis. Sei $H \subseteq G$ und $g \in G$. Dann ist wegen der Kommutativität $gHg^{-1} = gg^{-1}H = H$, also ist H konjugationsinvariant. Gilt zudem $H \leq G$, so folgt die Behauptung. □

Lemma 0.9. *Sei $(G,*)$ eine Gruppe, $N \trianglelefteq G$ und $U \leq G$. Dann ist $U*N := \{u*n \mid u \in U, n \in N\} = N*U$ eine Untergruppe von G.*

Beweis. **TODO** □

Lemma 0.10. *Seien $(G,*),(H,\cdot)$ Gruppen, $U \leq H$, $N \trianglelefteq U$ und $\phi : G \to H$ ein Gruppenhomomorphismus. Dann ist $\phi^{-1}(N) \trianglelefteq \phi^{-1}(U)$. Ist ϕ zusätzlich surjektiv, so gilt Gleichheit gdw. $U = N$.*

Beweis. Die Untergruppenrelation ist klar. Wir zeigen also noch, dass das Urbild $\phi^{-1}(N)$ konjugationsinvariant ist. Sei dafür $g \in G$. Dann ist $\phi(g\phi^{-1}(N)g^{-1}) = \phi(g)\phi^{-1}(N)\phi(g)^{-1} = N$, also $g\phi^{-1}(N)g^{-1} \subseteq \phi^{-1}(N)$. Außerdem ist für $a \in \phi^{-1}(N)$: $\phi(g^{-1}ag) = \phi(g)^{-1}\phi(a)\phi(g) \in \phi(g)^{-1}N\phi(g) = N$, also $g^{-1}ag \in \phi^{-1}(N)$ und damit $a = gg^{-1}agg^{-1} \in g\phi^{-1}(N)g^{-1}$, was die andere Inklusionsrichtung und damit die Konjugationsinvarianz zeigt. Ist zudem ϕ surjektiv, so gilt $N \neq U \Rightarrow \exists\, u \in U.\ u \notin N$. Ein solches $u \in U$ besitzt also kein Urbild in $\phi^{-1}(N)$, jedoch ein Urbild in $\phi^{-1}(U)$, da ϕ ja surjektiv ist. Damit muss dann also gelten $\phi^{-1}(N) \subseteq \phi^{-1}(U) \setminus \{\phi^{-1}(u))\}$ und die Mengen sind nicht gleich. □

Lemma 0.11. *Seien $(G,*),(H,\cdot)$ Gruppen, $N \trianglelefteq G$ und $\phi : G \to H$ ein surjektiver Gruppenhomomorphismus. Dann ist auch $\phi(N) \trianglelefteq H$.*

Beweis. **TODO** □

1 Einfache & Auflösbare Gruppen

VL vom 26.10.2023:

Erinnerung 1.0. Ein *Normalteiler* N einer Gruppe $(G,*)$ ist eine Untergruppe mit der Eigenschaft $\forall g \in G : gNg^{-1} = N$. Man definiert auf den Nebenklassen $G/N = \{gN \mid g \in G\}$ eine Verknüpfung $g_1N \cdot g_2N = g_1g_2N$, die aus G/N eine Gruppe macht. Weiter ist $G \to G/N, g \mapsto gN$ ein Homomorphismus. Notation $N \trianglelefteq G$.

Z.B. Die alternierende Grruppe A_n ist ein Normalteiler der symmetrischen Gruppe S_3.

Ansatz: Verstehe eine Gruppe G, indem man Normalteiler $\{e\} \neq N \lhd G$ und dann G/N studiert.

§1.1 Einfache Gruppen

Definition 1.1 (Einfache Gruppe)**.** Eine Gruppe $(G,*)$ heißt *einfach*, wenn $G \neq \{1\}$ und die trivialen Normalteiler $\{1\}, G$ die einzigen Normalteiler von G sind.

Beispiel 1.2. $\mathbb{Z}/n\mathbb{Z}$ ist einfach gdw. n prim ist. Andernfalls folgt mit dem chinesischen Restsatz für alle $d \mid n$, dass $\mathbb{Z}/d\mathbb{Z} \trianglelefteq \mathbb{Z}/n\mathbb{Z}$.

Wir verfolgen das Ziel, Gruppen zu verstehen, indem wir sie in einfache Normalteiler zerlegen und diese sowie deren Quotientengruppen separat untersuchen, welche hoffentlich eine simplere Struktur haben. Für endliche Gruppen haben die nichttrivialen Normalteiler bspw. echt kleinere Kardinalität.

Satz 1.3 (A_5)**.** *Die alternierende Gruppe A_n ist einfach für $n \geq 5$.*

Beweis. Wir wissen, dass A_n von 3-Zykeln erzeugt wird (lemma 0.7). Weiterhin sind alle 3-Zykel in A_n konjugiert zueinander, d.h. für jeden 3-Zykel $\sigma \in A_n$ existiert $\tau \in A_n$ (nicht unbedingt ein 3-Zykel) mit $\tau\sigma\tau^{-1} = (1\ 2\ 3)$[1]. Sei $N \trianglelefteq A_n$ ein Normalteiler mit $N \neq \{1\}$. z.z. $N = A$. Das erreichen wir indem wir zeigen, dass N enthält einen 3-Zykel, da alle 3-Zyklen zueinander konjugiert sind und A_n erzeugen, wodurch $N = A_n$ gelten müsste. Wähle $\sigma \in N \setminus \{1\}$:

Fall 1: σ enthält einen Zyklus der Länge ≥ 4 O.B.d.A.$\sigma = (1\ 2\ \ldots\ r)\rho, \forall i \in \{1,2,3\}$: $\rho(i) = i$. Dann $\sigma^{-1}(1\ 3\ 2)\sigma(1\ 2\ 3) = (2\ 3\ r) \in N$.

Fall 2: σ hat als längsten Zykel einen 3-Zykel (aber ist keiner) O.B.d.A.$\sigma = (1\ 2\ 3)\rho$ mit $\forall i \in \{1,2,3\} : \rho(i) = i$ und $\rho(4) \neq 4$. dann besitzt $N \ni \sigma^{-1}(2\ 3\ 4)\sigma(2\ 4\ 3) = (1\ 2\ 4\ 3\ \ldots)$ ($\Rightarrow$ Fall 1)

[1] Es gibt $\tau_0 \in S_n$ mit $\tau_0\sigma\tau_0^{-1} = (1\ 2\ 3)$. Falls $\tau_0 \in A_n$ ✓, sonst betrachte $\tau = (4\ 5)\tau$: $\tau\sigma\tau^{-1} = (4\ 5)\tau_0\sigma\tau_0^{-1} = (4\ 5)(1\ 2\ 3)(5\ 4) = (4\ 5)(5\ 4)(1\ 2\ 3) = (1\ 2\ 3)$

Fall 3: σ besteht nur aus Transpositonen(aber gerade Anzahl) O.B.d.A.$\sigma = (1\,2)(3\,4)\rho$, $\forall i \in \{1,2,34,\} : \rho(i) = i$. Dann ist $\sigma^{-1}(1\ 3\ 2)\sigma(1\ 2\ 3) = (1\ 4)(2\ 3) \in N$. Weiter gilt: Alle Elemente in A_n von diesen Zykeltyp sind in A_n zueinander konjugiert (vgl. oben mit $\tau = (1\ 2)\tau_0$). Also liegt auch $(1\ 2)(3\ 4)(2\ 5)(3\ 4) = (1\ 2\ 5) \in N$ ($\Rightarrow$ Fall 2)

□

§1.2 Normal- und Kompositionsreihen

Definition 1.4 (Normalreihe, Kompositionsreihe)**.** Sei G eine Gruppe. Eine *Normalreihe* ist eine aufsteigende Folge von Untergruppen $\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ sodass G_i normal in G_{i+1} ist. Die Quotienten G_{i+1}/G_i heißen *Faktoren* der Reihe $\mathscr{G}$.

Man sagt, dass eine Normalreihe $\mathscr{H}$ von G eine Normalreihe $\mathscr{G}$ *verfeinert*, wenn $\mathscr{H}$ aus $\mathscr{G}$ durch hinzufügen von Termen hervorgeht.

Man sagt, dass $\mathscr{G}$ und $\mathscr{H}$ äquivalent sind, wenn sie die gleiche Länge haben und es eine Permutation $\sigma \in S_n$ gibt mit $H_{i+1}/H_i \cong G_{\sigma(i)+1}/G_{\sigma(i)}$.

Eine Normalreihe, die keine echte Verfeinerung besitzt, heißt Kompositionsreihe.

VL vom 27.10.2023:

Beispiel 1.5 (Kompositionsreihen von $(G := (\mathbb{Z},+))$. Alle Untergruppen von G sind Normalteiler, da es sich um eine abelsche Gruppe handelt (lemma 0.8). Weiterhin haben alle Untergruppen von G die Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$. Sei nun $n \in \mathbb{N}$. Dann ist

$$\mathscr{G} : \{0\} = G_0 \underset{\neq}{\lhd} n\mathbb{Z} \underset{\neq}{\lhd} \mathbb{Z} = G$$

eine Normalreihe in G mit den Faktoren

$$G_1/G_0 = \{\{k\} \mid k \in n\mathbb{Z}\} \ \cong\ n\mathbb{Z} \ \cong\ \mathbb{Z},\ G/G_1 = \mathbb{Z}/n\mathbb{Z}$$

G besitzt allerdings keine Kompositionsreihe, denn für jede Normalreihe

$$\{0\} \underset{\neq}{\lhd} n\mathbb{Z} \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} \mathbb{Z} = G$$

ist für alle $1 < k \in \mathbb{N}$ eine echte Verfeinerung gegeben durch

$$\{0\} \underset{\neq}{\lhd} (kn)\mathbb{Z} \underset{\neq}{\lhd} n\mathbb{Z} \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} \mathbb{Z} = G$$

wobei $n\mathbb{Z}/(kn)\mathbb{Z} \cong k\mathbb{Z}$ **TODO** .

Satz 1.6. *Es gelten die folgenden Charakterisierungen von Kompositionsreihen:*

(a) Eine Normalreihe ist genau dann eine Kompositionsreihe, wenn alle Faktoren einfach sind.

(b) Jede endliche Gruppe besitzt eine Kompositionsreihe.

Beweis. Zu (a):

$\Rightarrow$ Der Beweis erfolgt durch Kontraposition. Sei dazu

$$\mathcal{G} : \{1\} = G_0 \underset{\neq}{\lhd} G_1 \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} G_i \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} G$$

so dass G_i/G_{i-1} nicht einfach ist. Sei weiterhin $\pi_i : G_i \to G_i/G_{i-1}$ die kanonische Projektion. Per Definition existiert dann ein nichttrivialer Normalteiler N von G_i/G_{i-1}, also $(\{G_{i-1}\} =)\{1_{G_i/G_{i-1}}\} \neq N \underset{\neq}{\lhd} G_i/G_{i-1}$. Dann ist mit lemma 0.10 (beachte, dass die kanon. Projektion surjektiv ist und $\pi^{-1}(\{G_{i-1}\}) = G_{i-1},\ \pi^{-1}(G_i/G_{i-1}) = G_i$)

$$\{1\} = G_0 \underset{\neq}{\lhd} G_1 \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} G_{i-1} \underset{\neq}{\lhd} \pi_i^{-1}(N) \underset{\neq}{\lhd} G_i \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} G$$

eine echte Verfeinerung von $\mathcal{G}$, also ist $\mathcal{G}$ keine Kompositionsreihe.

$\Leftarrow$ Sei $\mathcal{G}$ eine Normalreihe mit einfachen Faktoren und $\mathcal{H}$ eine Verfeinerung. Z.z. $\mathcal{H} = \mathcal{G}$, d.h. $G_i = H_i$ für alle i. Beiweis durch Induktion.

IA $i = 0$: $G_0 = \{e\} = H_0$ ✓

IS: Es existiert $j > i$ mit $H_i = G_{i+1}$. $G_i \subseteq H_{j-1} \lhd H_j = G_{i+1}\vec{\pi_i}G_{i+1}/ = G_i$ einfach. Da surjektive Homomorphismen Normalteiler erhalten gilt $\pi_i(H_{j-1}) \subseteq G_{i+1}/G_i$. Wegen Ëinfachheit"$\pi_i(H_j) = \{e\}$. $\Rightarrow H_{j-1} = G_i = H_i$.

Zu (b): Induktion über die Mächtigkeit dei Gruppe $|G|$. IA $|G| = 1$: $G = \{e\}$ ✓. IS: Wähle maximalen Normalteiler $N \lhd G$. Dann ist G/N einfach. Wende nun IA auf N (um die Kette weiter aufzubauen) an.$\Rightarrow$ Es entsteht eine Reihe mit einfachen Faktoren, also eine Kompositionsreihe. □

Erinnerung: Sei G Gruppe, $N \trianglelefteq G$ und $U \leq G$, dann ist $UN = NU$ Untergruppe von G.

Lemma 1.7 (Schmetterlingslemma von Zassenhaus)**.** *Sei G Gruppe, $A, B < G$ Untergruppen und $A_0 \trianglelefteq A$, $B_0 \trianglelefteq B$. Dann*

(a) $A_0(A \cap B_0) \trianglelefteq A_0(A \cap B)$ *und* $B_0(A_0 \cap B) \trianglelefteq B_0(A \cap B)$

(b) $\frac{A_0(A\cap B)}{A_0(A\cap B_0)} \cong \frac{(A\cap B)}{(A_0\cap B)(A\cap B_0)} \cong \frac{B_0(A\cap B)}{B_0(A_0\cap B)}$

Beweis. **TODO** □

Satz 1.8. *Sind $\mathcal{G}$, $\mathcal{H}$ Normalreihen von G, dann gibt es Verfeinerung $\tilde{\mathcal{G}}$, $\tilde{\mathcal{H}}$ von $\mathcal{G}$, $\mathcal{H}$, sodass sie äquivalent sind.*

Beweis. **TODO** □

Satz 1.9 (Jordan Hölder)**.** *Je zwei Kompositionsreihen einer Gruppe sind äquivalent.*

Beweis. Kompositionsreihen haben keine Verfeinerung & 1.8 □

Bemerkung. Gleiche Kompositionsreihen $\not\in$ gleiche Gruppe.

Beispiel.
- $\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ hat Kompositionsreihen $\{0\} \lhd (\mathbb{Z}/2\mathbb{Z} \times \{0\}) \lhd \mathbb{Z}/14\mathbb{Z}$ und $\{0\} \lhd (\{0\} \times \mathbb{Z}/2\mathbb{Z}) \lhd \mathbb{Z}/14\mathbb{Z}$, aber immer die gleichen Faktoren in unterschiedlicher Reihenfolge.
- Zu $G = \mathbb{Z}/9\mathbb{Z}$ und $H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ haben die Kompositionsreihen $\mathscr{G} : \{0\} \lhd 3\mathbb{Z}/9\mathbb{Z} \lhd G$ und $\mathscr{H} : \{0\} \lhd Z/3\mathbb{Z} \lhd H$ die gleichen Faktoren (zweimal $Z/3\mathbb{Z}$ und damit äquivalent, aber $G \neq H$).

§1.3 Auflösbare Gruppen

Definition 1.10. Eine Gruppe $(G, *)$ heißt auflösbar, wenn sie eine Normalreihe besitzt, deren Faktoren alle abelsch sind.

VL vom 02.11.2023:

Beispiel 1.11. a) Insbesondere ist jede abelsche Gruppe auflösbar: Für die triviale Gruppe $\{1\}$ existieren keine Faktoren, ansonsten setze

$$G_0 := \{1\} \underset{\neq}{\lhd} G_1 := G$$

b) Sei weiterhin $\mathbb{K}$ ein Körper. Die Matrixgruppe

$$(B = \{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \in GL_2(\mathbb{K}) \mid a,b,c \in \mathbb{K}\}, \cdot)$$

ist nicht abelsch, aber dennoch auflösbar. Sei dafür

$$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$$

und

$$\phi : B \to \mathbb{K}^* \times \mathbb{K}^*, \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \mapsto (a,b)$$

Dann ist $N = ker(\phi) = \{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{K}\} \cong (\mathbb{K}, +)$ Somit ist

$$\{id\} \underset{\neq}{\lhd} N \underset{\neq}{\lhd} B$$

eine Normalreihe mit abelschen Faktoren. (Geht auch für $GL_n(K)$, Beweis komplizierter)

c) (Semidirektes Produkt von Gruppen) **TODO**

Satz 1.12 (Untergruppen und Faktorgruppen auflösbarer Gruppen)**.** *Untergruppen und Faktorgruppen auflösbarer Gruppen sind auflösbar.*

Beweis. Sei G auflösbar mit abelscher Normalreihe (abelsche Faktoren)

$$G_0 := \{1\} \underset{\neq}{\triangleleft} ... \underset{\neq}{\triangleleft} G_n := G$$

Sei $H < G$ Untergruppe. Dann ist

$$H_0 := \{1\} \triangleleft ... \triangleleft H_n := H$$

mit $H_i := G_i \cap H$ eine abelsche Normalreihe von H (nach Streichen gleicher Elemente):

$$H_{i+1}/_{H_i} < G_{i+1}/_{G_i}$$

□

Satz 1.13. *Sei G eine endliche Gruppe und $\mathcal{G}$ eine Kompositionsreihe von G. Dann ist G auflösbar gdw. jeder Faktor von $\mathcal{G}$ zyklisch von Primzahlordnung ist.*

Beweis. "⇒": Sei G auflösbar. Nach Def. von Kompositionsreihen sind dann die $G_i/_{G_{i-1}}$ einfach und nach theorem 1.12 auflösbar. Insbesondere existiert also eine Normalreihe von $G_i/_{G_{i-1}}$. Dies impliziert, dass $G_i/_{G_{i-1}}$ abelsch ist, da $G_i/_{G_{i-1}}$ in einer solchen Normalreihe vorkommt (Begründung aus VL: da $\{1\} \underset{\neq}{\triangleleft} G_i/_{G_{i-1}}$ die einzige Normalreihe ist - wird aber nicht benötigt?) $G_i/_{G_{i-1}}$ ist als endliche abelsche Gruppe isomorph zu

$$\mathbb{Z}/_{p_1^{\alpha_1}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p_m^{\alpha_m}\mathbb{Z}}, \alpha_t \geq 1$$

Wegen Einfachheit gilt $m = 1$ (ansonsten $\mathbb{Z}/_{p_1^{\alpha_1}\mathbb{Z}} \times \{0\} \times ... \times \{0\}$ nichttrivialer NT). Also $G_i/_{G_{i-1}} \cong \mathbb{Z}/_{p^\alpha\mathbb{Z}}$. Wieder wegen Einfachheit ist $\alpha = 1$ (ansonsten $p\mathbb{Z}/_{p^\alpha\mathbb{Z}}$ nichttrivialer NT).
"⇐": Offensichtlich. □

Definition 1.14 (Kommutator)**.** Sei G eine Gruppe. Für $x, y \in G$ heißt $x^{-1}y^{-1}xy = [x,y]$ *Kommutator* von x und y. Die Kommutatoruntergruppe von G ist

$$D(G) =< [x,y] \mid x,y \in G >$$

Alternativnotation: $[G,G] := D(G)$.

Lemma 1.15. *Die Kommutatoruntergruppe D(G) einer Gruppe G ist ein NT von G. Die Faktorgruppe $G^m = G/_{D(G)}$ ist abelsch und heißt* Abelisierung *von G. Ist $N \trianglelefteq G$ und $G/_N$ abelsch, dann ist $D(G) \subseteq N$ (d.h. $G/_{D(G)} - >> G/_N$ ist surjektiv)*

Beweis. Es ist $g^{-1}[x,y]g = g^{-1}x^{-1}y^{-1}xyg = (g^{-1}x^{-1}g)(g^{-1}yg)(g^{-1}xg)(g^{-1}yg) = [g^{-1}xg, g^{-1}yg]$. Somit ist $g^{-1}D(G)g =< [g^{-1}xg, g^{-1}yg] \mid x,g \in G >= D(G)$.

Seien $xD(F), yD(G) \in G/D(G)$. Es ist dann $xyD(G) = xy[y,x]D(G) = xyy^{-1}x^{-1}yxD(G) = yxD(G)$.

Betrachte die kanonische Projektion $\pi : G - >> G/N$. Dann ist $\pi([x,y]) = \pi(x^{-1}y^{-1}xy) = \pi(x)^{-1}\pi(y)^{-1}\pi(x)\pi(y) = [\pi(x),\pi(y)] = N =\in G/N$ abelsch. Also $D(G) \subseteq N$. □

Definition 1.16. Setze $D^0(G) = G$ und dann induktiv $D^{i+1}(G) := D(D^i(G))$. Die Reihe

$$\ldots \triangleleft D^2(G) \triangleleft D^1(G) \triangleleft D^0(G) = G$$

(mit abelschen Faktoren nach dem vorhergehenden Lemma) heißt *abgeleitete Reihe* von G.

Satz 1.17. *Eine Gruppe G ist auflösbar gdw. es ein $m \in \mathbb{N}$ gibt mit $D^m(G) = \{1\}$. (Dies ist nicht immer erfüllt, da es Gruppen gibt mit $D(G) = G$, so dass die abgeleitete Reihe konstant G ist.)*

Beweis. "$\Leftarrow$": ist klar (good one).

"$\Rightarrow$": Sei G auflösbar. Dann gibt es eine abelsche Normalreihe

$$\{1\} = G_0 \underset{\neq}{\triangleleft} \ldots \underset{\neq}{\triangleleft} G_n = G$$

Wir zeigen induktiv über die Länge n der Normalreihe: $D^j(G) \subseteq G_{n-j}, j \in [n]_0$. IA: $n = 0$. Klar: $D^0(G) = G = G_0 = G_n$ ISt: Angenommen $D^j(G) \subseteq G_{n-j}$. Dann $D^{j+1}(G) = D(D^j(G)) \subseteq D(G_{n-j}) \subseteq G_{n-j-1}$. Die letzte Inklusion folgt aus TODO □

Beispiel 1.18. Sei G eine Gruppe und p eine Primzahl. Ist $|G| = p^n$, dann ist G auflösbar (und sogar nilpotent).

2 Körpererweiterungen

§2.1 Irreduzible Polynome

Definition 2.1 (Wiederholung aus EAZ)**.** Sei K im Folgenden ein Körper. Der Polynomring $K[X]$ ist ein Hauptidealring[2]. Das Ideal (f) ist Primideal gdw. $f = 0$ oder f irreduzibles Polynom ist, d.h. $f = gh \Rightarrow g \in K^* \vee h \in K^*$.

Lemma 2.2. *Ist f irreduzibel, dann ist (f) ein maximales Ideal.*

Beweis. Angenommen $(f) \subseteq (g)$. Dann $f = hg$ für ein $h \in K[X]$ nach Def. von (g). Dann gilt

$$\begin{cases} g \in K^* \Rightarrow (g) = K[X] \\ oder \\ h \in K^* \Rightarrow (f) = (g) \end{cases}$$

□

Satz 2.3 (Eisensteinkriterium)**.** *Sei A ein kommutativer Ring und $P \subseteq A$ ein Primideal (e.g. $A = \mathbb{Z}$, $P = \{pn \mid n \in \mathbb{N}\}$, p prim). Sei $f \in A[X]$ mit $f = \sum_{0 \leq i \leq n} a_i X^i$ mit drei Eigenschaften:*

1) $a_n \notin P$

2) $a_i \in P \; \forall 0 \leq i \leq n-1$

3) a_0 ist kein Produkt von zwei Elementen in P.

Dann lässt sich f nicht als Produkt zweier Polynome in $A[X]$ vom Grad $< n$ schreiben.

[2] nullteilerfrei, kommutativ und jedes Ideal ist Hauptideal

Beweis. EAZ Kühnlein □

Definition 2.4 (Inhalt)**.** Sei A ein Hauptidealring und $K = Quot(A)$. Sei $f = \sum_{0 \leq i \leq n} a_i X^i \in A[X]$. Definiere $\tilde{c}(f) \in A$ als einen Erzeuger des Ideals $(a_0, ..., a_n) \subset A$ (eindeutig bis auf Multiplikation mit Einheiten/inv. Elemente in A). Die Assoziiertenklasse $c(f) = \tilde{c}(f)A^* \subset A/A^*$ [A^* invertierbare Elemente in A] heißt *Inhalt* von f. Sei $f \in K[X]$. Wähle $a \in A \setminus \{0\}$ mit $af \in A[X]$. Definiere $\tilde{c}(f) = c(af)a^{-1} \in K$ und $c(f) = \tilde{c}(f)A^* \in K/A^*$ (Übung: Def. unabh. von der Wahl von a).

Beispiel. $A = \mathbb{Z}, K = \mathbb{Q}$. Dann

$$f(x) := \frac{2}{5}x^7 - 2x^3 + \frac{8}{3} = \frac{1}{15}(6x^7 - 30x^3 + 40)$$

also $\tilde{c}(f) = \frac{ggT(6,30,49)}{15} = \frac{2}{15}$.

Lemma 2.5. *Seien A, K wie oben und $f, g \in K[X]$. Dann gilt*
a) Für $f \neq 0$ gilt $\tilde{c}(f)^{-1} f \in A[X]$.
b) $c(fg) = c(f)c(g)$ (Gauß)

Beweis. Kühnlein EAZ □

Lemma 2.6. *A Hauptidealring, $K = Quot(A)$, $f \in A[X]$ nicht-konstantes Polynom. Falls f sich nicht als Produkt $f = gh$ mit $g, h \in A[X], \deg(g), \deg(h) < \deg(f)$ schreiben lässen, dann ist auch $f \in K[X]$ irreduzibel.*

Beweis. Ang. $f = g_0 h_0$ mit $g_0, h_0 \in K[X]$. Setze

$$g = \tilde{c}(g_0)^{-1} g_0 \in A[X]$$

und

$$h := \tilde{c}(g_0)\tilde{c}(h_0)\tilde{c}(h_0)^{-1} h_0 = \tilde{c}(g_0 h_0) a \tilde{c}(h_0)^{-1} h_0$$

für geeignetes $a \in A^*$. Somit ist auch $h \in A[X]$. Weiter ist $f = gh$. Dann ist $degg_0 = degg = degf$ oder $degh_0 = degh = degf$. □

Satz 2.7 (Eisensteinkriterium für Irreduzibilität)**.** *Sei A ein Hauptidealring, $P \subset A$ Primideal und $f \in A[X]$. Erfüllt f die Bedingungen i), ii), iii) des Eisensteinkriteriums, dann ist f irreduzibel in K[X] ($K = Quot(A)$).*

Beispiel 2.8. $A = \mathbb{Z}, K = \mathbb{Q}$.

1. $f = X^m - a, a \in \mathbb{Z}$. Falls $a = \prod_{1 \leq i \leq r} p_i^{\alpha_i}$ mit verschiedenen Primzahlen p_i und es ein $j \in \{1, ..., r\}$ mit $\alpha_i = 1$ gibt, dann ist f irreduzibel in K[X].

2. Sei p eine Primzahl. Das Polynom $\Phi_p = X^{p-1} + X^{p-2} + ... + X + 1$ heißt das p-te Kreisteilungspolynom. Setze $g(X) := \Phi_p(X+1)$ (dann impliziert insb. Irreduzibilität von g auch Irreduzibilität von Φ_p; SSubstitutionstrickfalls Eisensteinkriterium für Irreduzibilität nicht direkt anwendbar). Es ist $(X-1)\Phi_p(X) = X^p - 1$ und daher

$$g(X) = \frac{(X+1)^p - 1}{X} = \sum_{1 \le j \le p} \binom{p}{j} X^{j-1}$$

Eisenstein für p liefert nun Irreduzibilität von g (beachte $p \mid \binom{p}{j}$ für $j = 1, ..., p-1$). Dann Φ_p irreduzibel. Die Nullstellen von Φ_p sind gerade die primitiven p-ten Einheitswurzeln.

§2.2 Körpererweiterungen

Definition 2.9 (Körpererweiterung)**.** Sei $(L, +, \cdot)$ ein Körper. Sei K ein Teilkörper von L, d.h. $K \subseteq L$ und $(K, +|_K, \cdot|_K)$ ist selbst Körper. Dann bezeichnet man L als Erweiterungskörper von K. Man sagt, dass L über K eine Körpererweiterung (oder auch "K-Erweiterung") ist.

Notation: $L|K$, $(L-K)^T$ (**TODO Graphic with tikz?**)

Beispiel. $\mathbb{R}|\mathbb{Q}, \mathbb{C}|\mathbb{R}, \mathbb{C}|\mathbb{Q}, \mathbb{Q}(\sqrt{2})|\mathbb{Q}, \mathbb{C}(\mathbb{Z})|\mathbb{C}$

Definition 2.10 (Endliche Erweiterung)**.** Sei $L|K$ eine Erweiterung. Dann ist L insb. ein $K-VR$. Die Dimension über K von L $dim_K(L) =: [L:K]$ heißt der *Grad der Körpererweiterung* $L|K$. Die Erweiterung heißt *endlich*, wenn $[L:K] < \infty$.

Lemma 2.11 (Grad ist multiplikativ)**.** *Sei $L|K$ eine K-Erweiterung und sei V ein L-Vektorraum mit L-Basis $(v_i)_{i\in I} \subset V$. Sei $(e_j)_{j\in J} \subset L$ eine K-Basis von L. Dann ist $(e_j \cdot v_i)_{i\in I, j\in J}$ (VR-Multiplikation von Skalaren aus L mit Vektoren aus V) eine K-Basis von V.*

Beweis. (v_i) L-Basis $\Rightarrow$ für jedes $i \in Iist \sum_j c_{ij} e_j = 0$. (c_j) K-Basis $\Rightarrow c_{ij} = 0$ für alle $i \in I, j \in J$ Erzeugendensystem: Sei $v \in V$. Dann ist $v = \sum_{i\in I} \lambda_i v_i$ mit gewissen $\lambda_i \in L$. Für jedes $i \in I$ ist $\lambda_i = \sum_{j\in J} b_i j e_j$ mit gewissen $b_i j \in K$. Also $v = \sum_{i,j} b_{ij}(e_j \cdot v_i)$. □

Lemma 2.12 (Korollar)**.** *Sind $M|L, L|K$ Körpererweiterungen, dann gilt $[M:K] = [M:L] \cdot [L:K]$ (mit den üblichen Konventionen $\infty \cdot \infty = \infty$).*

Definition 2.13 (Adjungieren)**.** Sei $L|K$ eine Körpererweiterung. Sei $S \subset L$ eine Teilmenge. Dann bezeichnet $K(S)$ den kleinsten Teilkörper von L, der K und S enthält. Für $S = \{\alpha\}$ schreibt man $K(\alpha) = K(\{\alpha\})$ (gesprochen "K adjungiert α"). Man nennt eine Körpererweiterung $K(\alpha)|K$ *einfach*.

Definition 2.14 (Algebraisch vs. Transzendent)**.** Sei $L|K$ eine Körpererweiterung. Sei $\alpha \in L$. Betrachte die Evaluationsabbildung $ev_\alpha : K[X] \to L, f \mapsto f(\alpha)$.

Falls ev_α injektiv ist, so nennt man α *transzendent* (dann ist $f(\alpha) \equiv 0 \Rightarrow f \equiv 0$, also ist α nicht Nullstelle eines nichttrivialen Polynoms). Es gilt $Bild(ev_\alpha) \cong K[X]$ und $K(X) \cong K(\alpha)$. Insb. $[K(\alpha):K] = \infty$.

Falls dagegen ev_α nicht injektiv ist, nennt man α *algebraisch*. Dann ist $ker(ev_\alpha) = (m_{\alpha,K})$ Hauptideal. O.B.d.A. sei $m_{\alpha,K}$ normiert (Leitkoeffizient = 1). Wir nennen $m_{\alpha,K}$ das *Minimalpolynom* von α über K. Dann $L \supset Bild(ev_\alpha) \cong K[X]/(m_{\alpha,K})$ nullteilerfrei. Folglich ist $m_{\alpha,K}$ irreduzibel. Damit ist $(m_{\alpha,K})$ sogar ein maximales Ideal in K[X], also ist $Bild(ev_\alpha) \cong K[X]/(m_{\alpha,K})$ sogar ein Körper, also $Bild(ev_\alpha) = K(\alpha)$. (Schreibe auch $K[\alpha] := Bild(ev_\alpha)$.) Es ist $[K(\alpha) : K] = deg\, m_{\alpha,K} < \infty$.

Beispiel 2.15. $\pi \in \mathbb{C}$ ist transzendent über $\mathbb{Q}$ (Lindemann 1882). Es gibt in $\mathbb{C}$ nur abzählbar viele algebraische Zahlen über $\mathbb{Q}$, also überabzählbar viele transzendente Zahlen.

$d \in \mathbb{Z}$ sei quadratfrei und $d \neq 1$. Die Zahl $\sqrt{d} \in \mathbb{C}$ ist algebraisch mit Minimalpolynom $m_{\sqrt{d},\mathbb{Q}} = X^2 - d \in \mathbb{Q}[X]$. Weiter ist dann $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a,b \in \mathbb{Q}\}$.

Definition 2.16 (Algebraische K-Erweiterung)**.** Eine K-Erweiterung $L \mid K$ ist algebraisch, wenn jedes $\alpha \in L$ algebraisch über K ist.

§2.3 Algebraische Körpererweiterungen

Satz 2.17. *1. Ist $L \mid K$ endlich, dann ist $L \mid K$ algebraisch.*

2. *Ist $L \mid K$ algebraisch und endlich erzeugt (d.h. $L = K(\alpha_1, ..., \alpha_n)$ für geeignete α_i), dann ist $L \mid K$ endlich.*

3. *Sind $M \mid L$ und $L \mid K$ algebraisch, so ist auch $M \mid K$ algebraisch.*

Beweis. Zu a) Sei $\alpha \in L$. Dann gilt $[K(\alpha) : K] \leq [L : K] < \infty \Rightarrow \alpha$ algebraisch.

Zu b) Betrachte die Zwischenkörper $L =: L_n - ... - L_2 := L_1(\alpha_2) = K(\alpha_1, \alpha_2) - L_1 := L_0(\alpha_1) = K(\alpha_1) - L_0 := K$ (also $L_i := L_{i-1}(\alpha_i)$). Da α_i algebraisch über K ist, ist α_i insb. algebraisch über L_{i-1}. Somit $[L_i, L_{i-1}] = [L_{i-1}(\alpha_i), L_{i-1}] < \infty \Rightarrow [L : K] = [L_n : L_{n-1}]...[L_1 : L_0] < \infty$.

Zu c) Sei $\alpha \in M$. Betrachte $m_{\alpha,L} = \sum_{i=0}^{n} c_i X^i$, $c_i \in L$, Minimalpolynom von α über L. Definiere $K_0 := K(c_0, ..., c_n) \subseteq L$. Wegen b) ist $[K_0 : K] < \infty$. Wegen $m_\alpha, L \in K_0[X]$, ist α algebraisch über K_0. Dann $[K(\alpha) : K] \leq [K_0(\alpha) : K] = [K_0(\alpha) : K_0][K_0 : K] < \infty$, also α algebraisch über K.

□

Bemerkung 2.18. Sei $L \mid K$ eine K-Erweiterung. Die Menge $L_{alg,K} := \{\alpha \in L \mid \alpha$ algebraisch über K$\}$ ist ein Zwischenkörper $L - L_{alg,K} - K$. Diesen nennt man den *algebraischen Abschluss* von K in L.

Begründung: Seien $\alpha, \beta \in L_{alg,K}$.

$$[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K] \leq [K(\beta) : K][K(\alpha) : K] < \infty$$

(Frage aus VL: Wie würde das Minimalpolynom von $\alpha + \beta$ über K aussehen?)

Wir stellen uns nun die folgenden Fragen: Sei K ein Körper und $f \in K[X]$ nicht-konstant. Gibt es einen Erweiterungskörper $L \mid K$ so, dass

- f eine Nullstelle in L hat?
- f in L[X] in Linearfaktoren zerfällt?
- jedes Polynom in L[X] in Linearfaktoren zerfällt?

Satz 2.19. *Seien K ein Körper und $f \in K[X]$ irreduzibel. Dann gibt es eine algebraische K-Erweiterung mit $[L:K] = deg(f)$, in der f eine Nullstelle besitzt.*

Beweis. Setze $L := K[X]/(f)$. Nach lemma 2.2 ist L ein Körper. Betrachte die Quotientenabbildung $\pi : K[X] \to L$ (Homomorphismus!). Setze $\alpha := \pi(X) \in L$. Dann ist

$$f(\alpha) = f(\pi(X)) = \sum_{i=0}^{n} c_i \pi(X)^i = \pi\left(\sum_{i=0}^{n} c_i X^i\right) = \pi(f) = 0 \in L$$

Also $[L:K] = [K(\alpha):K] = deg(f)$, weil f Minimalpolynom von α ist. □

Korollar 2.20. *Seien K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom*[3]*. Es gibt eine endliche K-Erweiterung $L \mid K$, so dass f über L in Linearfaktoren zerfällt.*

Beweis. Induktion über $deg(f) =: d$:

IA $d = 1$: Klar, da f selbst Linearfaktor ist.

ISchritt Sei $g \in K[X]$ ein irreduzibles Polynom, das f teilt. Nach dem vorhergehenden Satz (theorem 2.19) gibt es $L_1 \mid K$, in der g eine Nullstelle $\alpha \in L_1$ besitzt. Schreibe $f = (X - \alpha)\tilde{f}$ mit $\tilde{f} \in L_1[X]$. Nach I-Annahme existiert $L \mid L_1$ endlich, in der $\tilde{f}$ in Linearfaktoren zerfällt. Weiter $[L:K] = [L:L_1][L_1:L] < \infty$.

□

Definition 2.21. Ein Körper K ist *algebraisch abgeschlossen*, falls jedes nicht-konstante Polynom $f \in K[X]$ eine Nullstelle in K besitzt.

Bemerkung 2.22. Ist K algebraisch abgeschlossen, dann gilt:

- Jedes $f \in K[X] \setminus K$ zerfällt in Linearfaktoren.
- Die irreduziblen Polynome über K sind von Grad 1.

Weiter gilt: Ist $L \mid K$ algebraisch, dann gilt bereits $L = K$, denn: Das Minimalpolynom m_β von $\beta \in L$ ist linear, d.h. $m_\beta = X - \alpha, \alpha \in K \Rightarrow \beta = \alpha \in K$.

Beispiel. $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra).

[3] irreduzible Polynome sind per Definition nicht-konstant

Lemma 2.23. *Sei A ein kommutativer Ring und $I \subsetneq A$ ein Ideal. Dann ex. ein maximales Ideal $m \subsetneq A$, das I enthält (Beweisidee: Lemma von Zorn).*

Satz 2.24. *Für jeden Körper gibt es einen algebraisch abgeschlossenen Erweiterungskörper.*

Auswahlaxiom in Algebra: nur hier; Funktionale Analysis: überall/Hahn-Banach; Lineare Algebra: Existenz von Basen unendlich dim VR

Beweis. 1) Konstruiere $L_1 \mid K$, so dass jedes $f \in K[X] \setminus K =: \Omega$ eine Nullstelle in L_1 hat. Definiere $A = K[(X_f)_{f\in\Omega}]$ (Polynomring in unendlich vielen Variablen). Setze $I := (\{f(X_f) \mid f \in \Omega\}) \subseteq A$. Dann ist $I \subsetneq A$. Angenommen $I = A$, also $1 \in I$. Dann $1 = \sum_{i=1}^{r} g_i f_i(X_{f_i})$ für $g_i \in A, f_i \in \Omega$. Sei $f = f_1 ... f_r$ Nach 2.20 ex. $F \mid K$, so dass f in Linearfaktoren zerfällt. Insbesondere hat jedes f_i eine Nullstelle $z_i \in F$. Definiere $\phi : A \to F$ durch $\phi|_K =$ Inklusion $K- > F$, $\phi(X_f) = 0$ für $f \in \Omega \setminus \{f_1, ..., f_r\}$, $\phi(X_{f_i}) = z_i$. Es gilt:

$$1 = \phi(1) = \sum_{i=1}^{r} \phi(g_i)\phi(f_i(X_{f_i})) = \sum_{i=1}^{r} \phi(g_i) f_i(\phi(X_{f_i})) = 0 \in F$$

Nach 2.24 ex. ein max. Ideal $m \subsetneq A$ mit $I \subseteq m$. Setze $L_1 := A/m$. Dann ist $K- > A- >> A/m = L_1$ eine Einbettung (setze $\pi : A \to A/m$). Sei $f \in K[X] \setminus K$. Setze $\gamma_f = \pi(X_f) \subseteq L_!$. Dann $f(\gamma_f) = f(\pi(X_f)) = \pi(f(X_f)) = 0$ da $f(X_f) \in I \subseteq m$.

2) Mit Schritt 1) erhalten wir eine Folge von Körpererweiterungen

$$K \subseteq L_1 \subseteq L_2 \subseteq ...$$

mit der Eigenschaft, dass jedes $f \in L_j[X] \setminus L_j$ eine Nullstelle in L_{j+1} hat. Definiere $L = \bigcup_{j\geq 1} L_j$. Sei $g \in L[X] \setminus L$. Dann hat g endlich viele Koeffizienten, die alle in einem L_m (m groß genug) liegen. Damit hat g eine Nullstelle in $L_{m+1} \subseteq L$. [Frage aus VL: Warum existiert $L = \bigcup_{j\geq 1} L_j$?] □

Definition 2.25. Sei K ein Körper. Es gibt einen algebraisch abgeschlossenen Körper $\overline{K}$ so, dass $K \subseteq \overline{K}$ und $\overline{K} \setminus K$ algebraisch ist. Man nennt $\overline{K}$ einen *algebraischen Abschluss*.

Beweis. Sei $L|K$ eine alg. abgeschlossene Erweiterung. Sei $\overline{K} = L_{alg,K} = \{\alpha \in L \mid \alpha$ algebraisch über K$\}$. Z.z. $\overline{K}$ ist alg. abgeschlossen. Sei dafür $f \in \overline{K}[X] \setminus \overline{K}$. Es gibt eine Nullstelle $\alpha \in L$ von f. Dann ist α algebraisch über $\overline{K}$. Da $\overline{K}$ alg. über K, ist α alg. über K, also $\alpha \in \overline{K}$. □

§2.4 $\overline{K}$-Homomorphismen

Definition 2.26. Seien $L_1|K$ und $L_2|K$ K-Erweiterungen. Ein Homomorphismus $f : L_1 \to L_2$ heißt *K-Homomorphismus*, falls $f(k) = k$ für alle $k \in K$. Ein K-Isomorphismus ist ein bijektiver K-Homomorphismus. Definiere $Aut(L_1|K) = \{f : L_1 \to L_2 \mid f\ K-Isom.\}$ (Gruppe der K-Automorphismen mit Verknüpfung als Operation).

Bemerkung 2.27 (Beobachtung). Sei $\phi : L_1 \to L_2$ K-Hom. Sei $f \in K[X]$, $\alpha \in L_1$ mit $f(\alpha) = 0$. Dann ist $f(\phi(\alpha)) = \phi(f(\alpha)) = \phi(0) = 0$. Folgerungen: α transzendent, ϕ K-Isom. $\Rightarrow \phi(\alpha)$ transzendent; für algebraisches α ist $m_{\alpha,K} = m_{\phi(\alpha),K}$.

Beispiel. $Aut(\mathbb{C} \mid \mathbb{R}) = \{id, \tau\}$ mit τ komplexe Konjugation. Denn: $\mathbb{C} = \mathbb{R}[i], m_{i,\mathbb{R}} = X^2 + 1$ mit Nullstellen i, $-i$. Jeder $\mathbb{R} - Aut.$ bildet i auf i (id) oder $-i$ (τ) ab.

Lemma 2.28. *Seien K, K' zwei Körper und $\sigma : K \to K'$ ein Isomorphismus. Sei $K(\alpha) \mid K$ eine einfache algebraische K-Erweiterung. Sei $L' \mid K'$ eine K'-Erweiterung. Für jede Nullstelle $\alpha' \in L'$ von $\sigma_*(m_{\alpha,K}) \in K'[X]$ (σ_* wendet σ auf die Koeffizienten an) gibt es genau einen Homomorphismus $\phi : K(\alpha) \to L'$ mit $\phi_{|K} = \sigma$ und $\phi(\alpha) = \alpha'$. Dann ist ϕ Isomorphismus zwischen $K(\alpha)$ und $K'(\alpha')$.*

Beweis. Kommutatives Diagramm □

Bemerkung 2.29. Die Anzahl der Homomorphismen ϕ wie im vorherigen Lemma ist genau die Anzahl der Nullstellen von $\sigma_*(m_{\alpha,K})$ in L'.

Beispiel 2.30. Sei $d \neq 1$ eine quadratfreie ganze Zahl. $Aut(\mathbb{Q}(\sqrt{d}) \mid \mathbb{Q}) = \{id, \sigma\}$, $m_{\sqrt{d},\mathbb{Q}} = X^2 - d$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$.

Satz 2.31 (Fortsetzungssatz)**.** *(a) Sei $L \mid K$ eine alg. K-Erweiterung, M ein alg. abgeschlossener Körper und $\sigma : K \to M$ ein Homomorphismus Dann existiert $\phi : L \to M$ mit $\phi_{|K} = \sigma$.*

(b) Sei $\sigma : K \to K'$ ein Isomorphismus von Körpern. Seien $\overline{K}, \overline{K'}$ alg. Abschlüsse von K bzw. K'. Dann ex. ein Isomorphismus $\phi : \overline{K} \to \overline{K'}$ mit $\phi_{|K} = \sigma$. (Je zwei algebraische Abschlüsse eines Körpers K sind isomorph.)

Beweis. a) Sei

$$\mathscr{U} = \{(F, \tau) \mid K \subseteq F \subseteq L \text{ Zwischenkörper und } \tau : F \to M \text{ Hom. mit } \tau|_K = \sigma\}$$

Die Menge $\mathscr{U}$ ist partiell geordnet via

$$(F_1, \tau_1) \leq (F_2, \tau_2) :\Leftrightarrow F_1 \subseteq F_2 \text{ und } \tau_2|_{F_1} = \tau_1$$

$(\mathscr{U}, \leq)$ ist induktiv, d.h jede Kette in $(\mathscr{U}, \leq)$ (total geordnete Teilmenge) besitzt eine obere Schranke. Sei C eine Kette. Setze $F_0 := \bigcup_{(F,\tau)\in C} F \subseteq L$. Für $x \in F_0$ definiere man $\tau_0(x) := \tau_F(x)$, falls $x \in F$. Da C eine Kette ist, ist die Definition von $\tau_0(x)$ unabhängig von der konkreten Wahl von F, also wohldefiniert. Dann ist (F_0, τ_0) eine obere Schranke von C. Lemma von Zorn impliziert die Existenz eines max. Elementes $(F_1, \tau_1) \in \mathscr{U}$. Wir behaupten nun, dass $F_1 = L$. Falls nicht, also $F_1 \subsetneq L$, sei $\alpha \in L \setminus F_1$. Dann ist α algebraisch über K, insb. algebraisch über F_1. Definiere $F_2 := F_1(\alpha)$. Nach 2.28 ex. $\tau_2 : F_2 \to M$ mit $\tau_2|_{F_1} = \tau_1$, also $(F_2, \tau_2) > (F_1, \tau_1)$ - Widerspruch.

b) Nach a) gibt es $\phi : \overline{K} \to \overline{K'}$ mit $\phi_{|K} = \sigma$. Z.z. $\phi(\overline{K}) = K'$.

Das Bild $\phi(\overline{K}$ ist ein alg. abgeschlossener Körper, da ϕ injektiv und damit $\phi(\overline{K})$ isomorph zu $\overline{K}$. **TODO Abbildung** Wegen remark 2.22 und der Algebraizität von $\overline{K'}|\phi(\overline{K})$ folgt $\phi(\overline{K}) = \overline{K'}$. □

VL vom 13.11.2023:

§2.5 Zerfallskörper

Definition 2.32. Sei K ein Körper und $\Omega \subseteq K[X]$ ene Teilmenge von nicht konstanten Polynomen. Ein Erweiterungskörper L von K heißt *Zerfällungskörper* von Ω, falls gilt

1. Jedes $f \in \Omega$ zerfällt in $L[X]$ in Linearfaktoren
2. $L = K(S)$, wobei $S = \{x \in L \mid \exists f \in \Omega : f(x) = 0\}$

Eine Körpererweiterung $L|K$ heißt *normal*, falls sie ein Zerfällungskörper für eine Menge $\Omega \subseteq K[X] \setminus K$ ist.

Bemerkung 2.33. Ist L ein Zerfällungskörper von $f \in K[X] \setminus K$ mit $\deg(f) = m$. Dann ist $L = K(\alpha_1, \ldots, \alpha_r)$, wobei $\alpha_1, \ldots, \alpha_r$ Nullstellen von f in L sind ($r \leq m$). Es gilt $[L : K] < m^r$. Tatsächlich gilt $[L : K] \leq m!$ (Übung). Natürlich **TODO graphik** und $[K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})] \leq [K(\alpha_i) : K] \leq m$.

Beispiel 2.34. a) $f = X^4 - 2 \in \mathbb{Q}[X]$ irreduzibel nach Eisensteinkriterium mit $p = 2$ und Nullstellen $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$

$$L = \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[X]/(f) \text{hat Grad 4 über } \mathbb{Q}$$

$$\mathbb{C} \supseteq \mathbb{Q}[\sqrt[4]{2}] = \{\sum_{j=0}^{3} a_j (\sqrt[4]{2})^j \mid a_j \in \mathbb{Q}\} \not\ni \pm i\sqrt[4]{2}$$

daher ist L kein Zerfällungskörper von f.

Dagegen ist $\mathbb{Q}(\sqrt{2})$ ein Zerfällungskörper von $X^2 \in \mathbb{Q}[X]$.

b) $f = X^4 - 2 \in \mathbb{F}_5[X]$ irreduzibel.

Beweis. Angenommen $f = gh$: Wenn $\deg(g) = 1$, hat f eine Nullstelle in $\mathbb{F}_5$, aber $X^4 \equiv 1 \mod 5$ nach Satz von Euler[4] und damit $\forall x \in \mathbb{F}_5 \setminus \{0\}: f(x) = X^4 - 2 = 1 - 2 = 4 \neq 0$. Wenn $\deg(g) = 2 = \deg(f)$ **TODO was soll das für eine begründung sein?** □

Sei $\alpha \in \overline{\mathbb{F}}_5$ eine Nullstelle von f. $\overline{\mathbb{F}}_5$ algebraischer Abschuss von $\mathbb{F}_5$. Dann ist $E = \mathbb{F}_5(\alpha) \cong \mathbb{F}_5[X]/(f)$ ein Zerfällungskörper von f, weil: f hat die Nullstellen $\alpha, 2\alpha, 3\alpha, 4\alpha \in E$, da $b^4 \equiv 1 \mod 5$ nach Euler für $b = 2, 3, 4$ und damit $(b\alpha)^4 = b^4\alpha^4 = \alpha^4$.

In $E[X]$ gilt: $f = \Pi_{i=1}^{4}(X - i\alpha) \in E[X]$.

Satz 2.35. *Sei K Körper und $\Omega \subseteq K[X] \setminus K$*

a) Jeder alg. Abschluss von K enhält genau einen Zerfällungskörper von Ω.

[4] Satz von Euler: $X^{p-1} \equiv 1 \mod p$

b) Je zwei Zerfällungskörper von Ω sind K-Isomorph

Beweis. **TODO** □

Satz 2.36 (Charackterisung von normalen Erweiterungen)**.** *Sei K Körper mit alg. Abschluss $\overline{K}$. Für einen Zwischenkörper $K \subseteq L \subseteq \overline{K}$ sind folgende Aussagen äquivalent:*

1. *$L|K$ ist normal*
2. *Ist $\phi : L \to \overline{K}$ ein K-Homomorphismus, dann ist $\phi(L) = L$*
3. *Jedes irreduzible $f \in K[X]$, dass in L eine Nullstelle besitzt, zerfällt in $L[X]$ in Linearfaktoren*

Beweis. **TODO** □

Satz 2.37. *Sei $L|K$ eine normale K-Erweiterung*

a) Für jeden Zwischenkörper M gilt $L|M$ ist normal.

b) Sind $\alpha, \beta \in L$, dann gibt es $\sigma \in Aut(L|K)$ mit $\sigma(\alpha) = \beta$ gdw $m_{\alpha,K} = m_{\beta,K}$

Beweis. **TODO** □

VL vom 13.11.2023:

§2.6 Serperable Erweiterungen

Definition 2.38. Ein irreduzibles Polynom in $K[X]$ heißt *separabel*, wenn es im $\overline{K}$ nur einfache Nullstellen hat. (allg. heizt ein allg. Polynom separabel, wenn alle irreduzieblen Faktoren separabel sind)

Definition 2.39. Die K-lineare Abbildung $D : K[X] \to K[X], \sum a_i x^i \mapsto \sum i a_i X^{i-1}$ heißt *(formal) Ableitung*. Es gilt die Leibnizregel $D(fg) = D(f)g + fD(g)$.[5]

Satz 2.40. *Ein irreduzibles Polynom f ist genau dann separabel, wenn $D(f) \neq 0$.*

(Die mehrfache Nullstellen eines bel. Polynoms f sind die gemeinsamen Nullstellen von f und $D(f)$)

Beispiel 2.41. $K = \mathbb{F}_p(T) = Quot(\mathbb{F}_p[T])$ (rationaler Funktionenkörper) Betrachte $f = X^p - T \in K[X]$. Nach Eisenstein ist f irreduzibel. Es ist $D(f) = pX^{p-1} = 0$. Also ist f nicht separabel.

Sei $a = \sqrt[p]{T} \in \overline{K}$ eine Nullstelle von f. Dann gilt $(X-a)^p = f$.

Beweis zu 2.40.

[5] Präziser $\sum a_i x^i \mapsto \sum \pi(i) a_i X^{i-1}$ mit $\pi \colon \mathbb{Z} \to K$ definiert durch $1 \mapsto 1_K$. Daher ist die $Char(K)$ auch relevant.

Bemerkung. Schreibe $f = c\Pi_{j=1}^{d}(X - a_j) \in \overline{K}[X]$ mit $0 \neq c, a_1, \ldots, a_d \in \overline{K}$. Dann ist $D(f) = c\sum_{j=1}^{d}\Pi_{i\neq j}(X - a_i)$ (Leibnizregel).

Damit folgt $D(f)(a_k) = c\Pi_{i\neq k}(a_k - a_i)$.

"$\Rightarrow$" Durch Kontraposition: Sei $D(f) = 0$. Dann $D(f)(a_1) = 0$. Dann $\exists i \neq 1 : a_i = a_1$, was $\lightning$sep.

"$\Leftarrow$" Sei $D(f) \neq 0$. Wegen $\deg(D(f)) < \deg(f)$ und f irreduzibel, sind $D(f)$ und f teilerfremd. Es gibt also $g, k \in K[X]$ mit $1 = gf + hD(f)$.

Sei a_k eine der Nullstellen von f in $\overline{K}$. Dann ist

$$\begin{array}{ccc} 1 = g(a_k)f(a_k) + h(a_k)D(f)(a_k) \\ \| \qquad\qquad \nmid \\ 0 \qquad\qquad 0 \end{array}$$

Wegen (*) muss die Nullstelle a_k einfach sein.

□

Bemerkung 2.42. Ist $Char(K) = 0$, dann ist jedes irreduzible Polynom separabel.[6]

Definition 2.43. Sei $L|K$ eine alg. K-Erweiterung. Ein Element $a \in L$ ist separabel, wenn $m_{a,K}$ separabel ist. Sind alle $a \in L$ separabel, dann nennt man $L|K$ separabel.

Lemma 2.44. *Ist $L|K$ separabel und $K \subseteq M \subseteq L$ ein Zwischenkörper, dann ist $L|M$ und $M|K$ separabel.*

Beweis. $M|K$: Sei $a \in M$. Die Minimalpolynome über K von a als Element von M und L sind gleich. Also ist a separabel.

$L|M$: Sei $a \in L$. Dann ist $m_{a,M}$ ein Teiler von $m_{a,K}$ in $\overline{K}[X]$. daher hat auch $m_{a,M}$ nur einfache Nullstellen.

□

Definition 2.45. Sei $L|K$ eine alg. K-Erweiterung. Der *Separabititätsgrad* $[L : K]_S$ über K ist definiert als $\left|Hom_K(L, \overline{K})\right|$. Ist $L|K$ normal, dann ist $[L : K]_s = |Aut(L|K)|$.[7]

Lemma 2.46.

a) Sind $M|L$ und $L|K$ alg. Erweiterungen, dann ist

$$[M : K]_S = [M : L]_S \cdot [L : K]_S$$

b) Ist $L : K$ endlich, so ist $[L : K]_S \leq [L : K]$

[6] Editor's remark: $Char(K) = 0$ verhindert, dass die Faktor i in der Ableitung 0 werden kann und damit $D(f) = 0$ werden könnte.

[7] Nach theorem 2.35 b)

Beweis. Wir betten K, M, L in einen gemeinsamen alg. Abschluss $\overline{K}$ ein. Seien $(\sigma_i)_{i\in I}$ die paarweise verschiedenen K-Homomorphismen $L \to \overline{K}$. Seien $(\tau_j)_{j\in J}$ die paarweise verschiedenen L-Homomorphismen $M \to \overline{K}$. Also $|I| = [L:K]_S$ and $|J| = [M:L]_S$. Die K-Homomorphismen $\overline{\sigma_i} \circ \tau_j = f_{ij}$ sind genau die paarweise verschiedenen K-Homom. $M \to \overline{K}$, wobei $\overline{\sigma_i}$ eine Fortsetzung von σ_i zu einem K-Homomorphismus $\overline{K} \to \overline{K}$ ist (Fortsetzungssatz theorem 2.31). Angenommen $\overline{\sigma_i} \circ \tau_j = \overline{\sigma_s} \circ \tau_r$, dann ist $\overline{\sigma_i}_{|L} = (\overline{\sigma_i} \circ \tau_j)_{|L} = (\overline{\sigma_s} \circ \tau_s)_{|L} = \sigma_s$, also $i = s$. Da $\overline{\sigma_i}, \overline{\sigma_s}$ automatisch inj. sind[8], ist $\tau_j = \tau_r$ also $j = r$. Damit ist a) bewiesen.

Zu b) Es gilt $L = K(a_1, \ldots, a_n)$ für gewisse $a_i \in L$. Wegen a) wird der Gradformel lemma 2.12 genügt es $L = K(a)$ zu betrachten. Nach lemma 2.28 ist $[K(a):K]_S = \left|\{b \in \overline{K} \mid m_{a,k}(b) = 0\}\right| \leq \deg(m_{a,K}) = [K(a):K]$ □

Satz 2.47 (Char. separabler Erweiterungen)**.** *Sei $L|K$ eine endliche Erweiterung. Dann sind äquivalent:*

(i) $L|K$ *separabel*

(ii) $L = K(a_1, \ldots, a_n)$ *für über K separable Elemente* $a_1, \ldots, a_n \in L$

(iii) $[L:K]_S = [L:K]$

Beweis.

(i) → (ii) $[L:K] < \infty$, dann gilt $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Diese Elemente sind (nach Definition separabler Körpererweiterungen definition 2.43) automatisch separabel.

(ii) → (iii) Wegen lemma 2.46 a) and lemma 2.12 reicht es (iii) für den Fall $L = K(a)$ zu zeigen.

$$[K(a):K]_S = \left|\{b \in \overline{K} \mid m_{a,K}(b) = 0\}\right| \overset{a \text{ sep.}}{=} \deg(m_{a,K}) = [K(a):K]$$

(iii) → (i) Sei $a \in L$. Dann gilt

$$\begin{aligned}[L:K] = [L:K]_S &= [L:K(a)]_S \cdot [K(a):K]_S \\ &\leq [L:K(a)] \cdot [K(a):K] \\ &= [L:K]\end{aligned}$$

Damit ist $[K(a):K]_S = [K(a):K]$ und a ist separabel.

□

Korollar 2.48. *Ist $f \in K[X] \setminus K$ ein separables Polynom, so ist der Zerällungskörper von f separabel*

VL vom 23.11.2023:

[8] Alle Körperhomomorphismen sind 0 oder injektiv. Wäre $\phi(a) = 0$, dann $0 = \phi(a) = \phi(a)\phi(a^{-1}) = \phi(1) = 1$

§2.7 Endliche Körper

Ziel: Konstruktion eines Körpers $\mathbb{F}_q$, $q = p^n$, p prim mit q Elementen. Nicht zu verwechseln mit $\mathbb{Z}/q\mathbb{Z}$, der für $n > 1$ Nullteiler besitzt.

Lemma 2.49. *Es sei $\mathbb{F}$ ein endlicher Körper. Dann gilt $p = char(\mathbb{F}) > 0$. Somit $|\mathbb{F}| = q := p^n$ für $[\mathbb{F} : \mathbb{F}_p] = n$. Es ist $\mathbb{F}$ der Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$. Insbesondere ist die Erweiterung über $\mathbb{F}/\mathbb{F}_p$ normal.*

Beweis. Mit $\mathbb{F}$ ist auch der Primkörper[9] endlich, also von der Form $\mathbb{F}_p$. Daher $|\mathbb{F}| = |\mathbb{F}_p|^{[\mathbb{F}:\mathbb{F}_p]} = p^n$.

Die multiplikative Gruppe $\mathbb{F}^*$ hat die Ordnung $q-1$, daher ist jedes Element in $\mathbb{F}^*$ Nullstelle von $X^{q-1} - 1$. Also ist jedes Element von $\mathbb{F}$ Nullstelle von $X^q - X$. Insbesondere ist $\mathbb{F}$ Zerfällungskörper von $X^q - X$. □

Satz 2.50. *Es sei p eine Primzahl. Dann existiert zu jedem $n \in \mathbb{N}$ eine Erweiterung $\mathbb{F}_q|\mathbb{F}_p$ mit $q = p^n$ Elementen. Es ist $\mathbb{F}_q$ bis auf Isomophie der eindeutige Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$. Es besteht $\mathbb{F}_q$ genau aus den Nullstellen von $X^q - X$. Jeder endliche Körper ist bis auf Isomorphie ein Körper des Typs $\mathbb{F}_q$.*

Beweis. Die Eindeutigkeitsaussagen folgen aus dem Lemma. Sie $f := X^q - X$. Wegen $D(f) = -1$ hat das Polynom nur einfache Nullstellen, also q einfache Nullstellen in einem algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$. Diese Nullstellen bilden einen Teilkörper von $\overline{\mathbb{F}}_p$:

Sei $a, b \in \overline{\mathbb{F}}_p$ Nullstellen. Dann $(a \pm b)^q = \sum_{i=0}^{q} \binom{q}{i} a^i b^{q-i} \overset{char=p}{=} a^q \pm b^q$ also ist $a \pm b$ wieder eine Nullstelle.

$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}$ also ist ab^{-1} wieder eine Nullstelle. D.h. die Nullstellen von f sind der Zerfällungskörper von f. Er hat q Elemente. □

Bemerkung 2.51. Sei K ein Körper der Charakteristik $p > 0$. Das Argument des letzten Beweises impliziert, dass

$$\{x^{p^n} \mid x \in K\}$$

ein Teilkörper von K ist.

Korollar 2.52. *Man bette die Körper $\mathbb{F}_q$, $q = p^n$ in einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ ein. Es ist $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$, $(q = p^n, q' = p^{n'})$genau dann, wenn $n|n'$. Die Erweiterung $\mathbb{F}_{q'}|\mathbb{F}_q$ sind bis auf Isomorphie die einzigen Erweiterungen zwischen endlichen Körpern der Charackteristik p.*

Beweis. Es gelte $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$. Sei $m := [\mathbb{F}_{q'} : \mathbb{F}_q]$. Dann $p^{n'} = \left|\mathbb{F}_{q'}\right| = \left|\mathbb{F}_q\right|^m = (p^n)^m = p^{n \cdot m}$, also $n|n'$. Gilt umgekehrt $n' = n \cdot m$, so folgt für $a \in \overline{\mathbb{F}}_p$ aus $a^q = a$ stets $a^{q'} = a^{q^m} = a$. Wegen des Fortsetzungssatzes kann man jede Erweiterung $L|\mathbb{F}$ von endlichen Köpern der Char. p

[9] Kleinster Teilkörper eines Körpers. Er wird von 0 und 1 durch Abschluss von Multiplikation, Addition und der Inversen erzeugt. Er ist isomorph zu $\mathbb{Q}$, wenn $char(K) = 0$, oder zu $\mathbb{F}_{char(K)}$, wenn $char(K) > 0$.

in $\overline{\mathbb{F}}_p$ realisiert werden. Die Eindeutigkeit folgt dann mit dem schon Gezeigten and dem vorherigen Satz. □

Ein Körper K ist *perfekt*, wenn jede alg. Erweiterung von K separabel ist.

1. $char(K) = 0$, d.h. $\mathbb{Q} \subseteq K$. Dann ist K perfekt, weil jedes irreduzible Polynom f über K separabel ist. (denn $D(f) = 0$) Es gibt aber alg., nicht normale Erweiterungen von $\mathbb{Q}$ (Bsp. theorem 2.36 **TODO does this reference make sense???**)

2. $\mathbb{F}_p(t)$ ist nicht perfekt. Die Erweiterung $\mathbb{F}_p(t)[t^{\frac{1}{p}}] = \mathbb{F}_p(t^{\frac{1}{p}})$ ist normal aber nicht separabel. (Bsp. 2.41) Sei $p = 5$. Betrachte die alg. Erweiterung **TODO bild** Warum ist $\mathbb{F}_5(t^{1/15})|\mathbb{F}(t)$ nicht normal? Ansonsten wären alle Nullstellen von $X^3 - t^{1/5}$ in $\mathbb{F}_5(t^{1/15})$.[10] Somit auch alle Nullstellen von $X^3 - 1 = (X-1)(X^2+X+1)$. Jedes Element von $\mathbb{F}_p(t^{1/15})$ ist von der Form $\frac{p(t^{1/15})}{q(t^{1/15})}$ mit $p, q \in \mathbb{F}_5[X]$ teilerfremde Polynome. Da $t^{1/15}$ transzendent über $\mathbb{F}$, ist die Evaluationsabbildung

$$\mathbb{F}_5[Y] \xrightarrow{ev} \mathbb{F}_5(t^{1/15})$$

injektiv, erwertert sich also auf den Quotientenkörper

$$\mathbb{F}_5(Y) \to \mathbb{F}_5(t^{F/15})$$

injektiv. Also muss es ein $f \in \mathbb{F}_5(Y)$ geben mit $f^2 + f + 1 = 0$. Sei $g = f - 2 \in \mathbb{F}_5(Y)$. Dann $0 = (g+2)^2 + (g+2) + 1 = g^2 + 4g + 4 + g + 2 + 1 = g^2 + 2$ also $g^2 = -2 = 3$ undn $g \in \mathbb{F}_5$. Das ist ein Wiederspruch: 3 ist kein Quadrat mod 5.

Korollar 2.53. *Jede algebraische Erweiterung eines endlichen Körpers ist normal und separabel. Insbesondere ist jeder endliche Körper perfekt.*

Beweis. Sei $K|\mathbb{F}$ eine alg. Erweiterung von $\mathbb{F}$ endlicher Körper mit Char $p > 0$. Sei zunächst $K|\mathbb{F}$ endlich. Da $f = X^q - X$ seprabel und K Zerfällungskörper von f über $\mathbb{F}_p$ füre ein $q = p^n$ ist, ist $K|\mathbb{F}_p$, insb auch $K|\mathbb{F}$, normal und separabel.

Allgemein lässt sich K durch endliche Erweiterungen ausschöpfen. □

Satz 2.54. *Aut*$(\mathbb{F}_{p^n}|\mathbb{F}_p)$ *ist zyklisch von Ordung n. Sie wird erzeugt vom* Frobenius-Automorphismus*:*

$$\begin{aligned} Fr : \mathbb{F}_{p^n} &\xrightarrow{\cong} \mathbb{F}_{p^n} \\ x &\mapsto x^p \end{aligned}$$

Beweis. Fr ist Homomorphismus Fr injektiv, also bijektiv, weil $\mathbb{F}_{p^n}$ endlich ist. Fr Erzeuger: Angenommen $Fr^m = id$ für $1 \leq m < n$. Dann $X^{p^m} = X$ für alle $X \in \mathbb{F}_{p^n}$. Dann hätte $X^{p^m} - X$ mehr als p^m Nullstellen. (Wiederspruch) Fr hat Ordnung n: $|\mathbb{F}_{p^n}|\mathbb{F}_p| = [\mathbb{F}_{p^n} : \mathbb{F}_p]_s = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ □

[10] man bekommt die dritten Einheitswurzeln aus den nullstellen raus

Satz 2.55. *Eine endliche Untergruppe der multiplikativen Gruppe eines beliebigen Körpers ist zyklisch.*

Beweis. Sei $H \leq K^*$ eine endliche Untergruppe. Sei $a \in H$ ein Element maximaler Ordnung m in H. Sei $H_m := \{b \in H \mid ord(b) | m\} \subseteq H$. Die Elemente von H_m sind Nullstellen des Polynoms $X^m - 1 \in K[X]$. Somit $|H_m| \leq m$. Wegen $a \in H_m$, somit $\langle a \rangle \subseteq H_m$, ist $|H_m| = m$. Ang. es gibt $b \in H \setminus H_m$. D.h. $ord(b) \nmid m$. Dann gilt $ord(ab) = kgV(ord(b), m) > m$. $\lightning$ zur Maximalität von a. □

Satz 2.56 (Satz vom primitiven Element)**.** *Sei $L|K$ eine endliche und separabel Körpererweiterung. Dann existiert ein $a \in L$ mit $L = K(a)$.*

Beweis.

1.Fall: K ist ein Endlicher Körper Dann ist auch L endlich. Nach theorem 2.55 ist L^* zyklisch, d.h. $L^* =< a >$. Somit $L = K(a)$.

2. Fall K ist unendlich Schreibe $L = K(a_1, \ldots, a_n)$. Durch eine Induktion über n reicht es den Fall $n = 2$ zu zeigen. Sei $L = K(a_1, a_2)$Seien $\phi_1, \ldots, \phi_m : L \to \overline{K}$ seien die verschiedenen K-Einbettungen $L \to \overline{K}$, wobei $m = [L : K]_S = [L : K]$ weil separabel. Das Polynom

$$g = \Pi_{i<j} ((\phi_i(a_1) - \phi_j(a_1)) \cdot X + (\phi_i(a_2) - \phi_j(a_2))) \in \overline{K}[X]$$

Für $i < j$ ist $\phi_i(a_1) \neq \phi_j(a_1)$ oder $\phi_i(a_2) \neq \phi_j(a_2)$. Somit $g \neq 0$. Da K unendlich, gibt es ein $c \in K$ mit $g(c) \neq 0$. Aslo $(\phi_i(a_1) - \phi_j(a_1)) \cdot c + (\phi_i(a_2) - \phi_j(a_2)) \neq= 0$ für alle $i < j$. Das ist $\phi_i(a_1 \cdot c + a_2) - \phi_i(a_1 \cdot c + a_2)$ und $\phi_i(a) \neq \phi_j(a)$ mit $a := a_1 c + a_l \in L$ für $i < j$. Damit sind $\phi_1(a), \ldots, \phi_m(a)$ sind verschiedene Nullstellen von $m_{a,k}$. Damit $[L : K] \geq [K(a) : K] = \deg(m_{a,K}) \geq= m = [L : K]$, also $[L : K] = [K(a) : K]$ und $L = K(a)$

□

Beispiel 2.57. Die Separabilität im Satz theorem 2.56 ist essenziell. $K = \mathbb{F}_p(s,t)$ rationaler Funktionenkörper in zwei Variablen. $L = K(\sqrt[p]{s}, \sqrt[p]{t})$ und damit $[L : K] = p^2$. **TODO Graphik**

Sei $a \in L$. Schreibe $a = \sum_{l,k} = a_{l,k} (\sqrt[p]{s})^l (\sqrt[p]{t})^k$ mit $a_{l,k} \in K$. Dann ist $a^p = \sum_{l,k} a_{l,k}^p s^l t^k =: c \in K$, da $(*)^p$ eine Homomorphismus ist. Somit ist a Nullstelle von $X^p - c \in K[X]$ und $\deg(m_{a,K}) leq p$. Damit ist $K(a) \subset L$.

3 Galoistheorie

Definition 3.1. Eine algebraische Körpererweiterung $L|K$ heißt *Galoiserweiterung* (oder galois'sch), wenn $L|K$ normal und separabel ist. Man nennt dann $Gal(L|K) = Aut_K(L)$ die *Galoisgruppe* von $L|K$.

Sei F ein Körper und $H \leq Aut(F)$ eine Untergruppe. dann ist $F^H = \{x \in F \mid \forall \sigma \in H : \sigma(x) = x\}$ ein Teilkörper von F, genannt *Fixkörper* von H.

§3.1 Hauptsatz der Galoistheorie

Lemma 3.2. *Sei $L|K$ Galoiserweiterung. Dann ist $L^{Gal(L|K)} = K$.*

Beweis.

"$\supseteq$" klar

"$\subseteq$" (Durch Kontraposition) Sei $a \in L \setminus K$. Das Minimalpolynom $m_{a,K}$ hat Grad ≥ 2.

- $L|k$ normal => $m_{a,K}$ zerfällt in $L[X]$ in Linearfaktoren.
- $L|K$ separabel => $m_{a,k}$ hat keine mehrfach Nullstelle.

Also gibt es eine weitere Nullstelle b von $m_{a,K}$ mit $b \neq a$. Nach Satz theorem 2.37 existiert eine $\sigma \in Gal(L|K)$ mit $\sigma(a) = b$. => $a \notin L^{Gal(L|K)}$

□

Satz 3.3. *Seien L ein Körper und $H \leq Aut(L)$ eine endliche Untergruppe. Dann ist*

1. *$L|L^H$ galois'sch*
2. *$[L : L^H] = |H|$*
3. *$Gal(L|L^H) \cong H$*

Beweis. Sei $a \in L$. Betrachte die H-Bahn von a.

$$H \cdot a = \{\sigma(a) \mid \sigma \in H\} = \{a_1, \ldots, a_n\} \subseteq L$$

Betrachte Polynom $f_a = \Pi_{i=1}^n (X - a_i)$. Für $\sigma \in H$ ist $\sigma_*(f) = \Pi_{i=1}^n (X - \sigma(a_i)) = \Pi_{i=1}^n (X - a_i)$.[11] Da f_a also fix unter $\sigma \in H$ ist, müssen die Koeffizienten von f_a in L^H liegen und damit $f_a \in L^H[X]$. Weil alle Nullstellen von f_a auch Nullstelle von m_{a,L^H} sind, muss schon $f_a = m_{a,L^H}$ sein.[12] Nach Konstruktion hat f_a nur einfache Nullstellen, ist also separabel. $\Rightarrow$ a separabel. $\overset{a \text{ beliebig}}{\Rightarrow} L|L^H$ separabel. Weiter zerfällt $f_a = m_{a,L^H}$ in Linearfaktoren $\Rightarrow L|L^H$ normal and damit galois'sch.

Wegen $H \subseteq Gal(L|L^H)$ gilt $|H| \leq \left|Gal(L|L^H)\right| = [L : L^H]_S \overset{theorem\ 2.47}{=} [L : L^H]$. Angenommen $|H| < [L : L^H] \leq \infty$. Dann finden wir ein L_0 mit $L^H \subseteq L_0 \subseteq L$ mit $|H| \leq [L_0 : L^H] < \infty$. Der Satz vom primitiven Element liefert ein $a \in L_0$ mit $L_0 = L^H(a)$. Aber $f_a = m_{a,L^H}$ hat Grad $\leq |H|$. => $[L_0 : L^H] = \deg(m_{a,L^K}) \leq |H|$ ↯

Also ist $[L : L^H] = |H| = \left|Gal(L|L^H)\right|$ => $H = Gal(L|L^H)$. □

[11] Zu jedem a_i existiert ein $\tau \in H$ mit $\tau(a) = a_i$. Dann ist $\sigma(a_i) = \sigma(\tau(a)) = \underbrace{(\sigma \circ \tau)}_{\in H}(a) \in H \cdot a$. σ is bijektiv, weshalb jedes a_i auf ein anderes Element in $H \cdot a \subseteq L$ abgebildet.

[12] m_{a,L^H} teilt $f_a \in L^H[X]$, weil a Nullstelle von f_a

VL vom 30.11.2023:

Satz 3.4 (Hauptsatz)**.** *$L|K$ endliche Galoiserweiterung.*

$$U := \{H \leq Gal(L|K) \mid H \text{ Untergruppe}\}$$

$$Z := \{E \subseteq L \mid K \subseteq E \subseteq L \text{ Zwischenkörper}\}$$

a) Die Zuordnungen $Fix : U \to Z, H \mapsto L^H$ und $\Gamma : Z \to U, E \mapsto Gal(L|E)$ sind zueinander inverse Bijektionen:

$$\begin{aligned} U &\longleftrightarrow Z \\ H &\longmapsto L^H = Fix(H) \\ \Gamma(E) = Gal(L|E) &\longleftarrow\!\shortmid E \end{aligned}$$

Fix und Γ sind enthaltungsumkehrend:

$$\begin{aligned} H_1 \leq H_2 &\Rightarrow Fix(H_1) \supseteq Fix(H_2) \\ E_1 \subset E_2 &\Rightarrow \Gamma(E_1) \geq \Gamma(E_2) \end{aligned}$$

b) Sei $E \in Z$, dann ist $E|K$ normal g.d.w. $Gal(L|E)$ ein Normalteiler von $Gal(L|K)$ ist.

$$Gal(E|K) \cong Gal(L|K)/Gal(L|E)$$

Beweis.

Zu a) Beachte: $E \in Z$, dann $L|E$ nach theorem 2.37 a) normal und nach lemma 2.44 separabel und damit galoissch

Fix und Γ sind inverse Bijektionen:

$Fix \circ \Gamma = id$ Für jedes $E \in Z$ gilt $Fix(\Gamma(E)) = Fix(Gal(L|E)) = L^{Gal(L|E)} \overset{3.2}{=} E$

$\Gamma \circ Fix = id$ Für jedes $H \in U$ gilt $\Gamma(Fix(H)) = \Gamma(L^H) = Gal(L|L^H) \overset{3.3}{=} H$

Fix und Γ sind enthaltungsumkehrend

- Sei $H_1 \leq H_2$. Für jedes $x \in L^{H_2}$ gilt per Definition $\forall \sigma \in H_2 : \sigma(x) = x$, was damit auch insbesondere für jedes $\sigma \in H_1 \subseteq H_2$ gilt. $\Rightarrow x \in L^{H_1}$
  $\Rightarrow Fix(H_2) = L^{H_2} \subseteq L^{H_1} = Fix(H_1)$
- Sei $E_1 \subseteq E_2$. $\sigma \in \Gamma(E_2) = Gal(L|E_2) \leq Gal(L|E_1) = \Gamma(E_1)$

Bemerkung. Für $\sigma \in Gal(L|K)$ und $H \in U$, dann $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$, denn für $x \in L^{\sigma H \sigma^{-1}} \Leftrightarrow \forall \tau \in H : \sigma\tau\sigma^{-1}(x) = x \Leftrightarrow \forall \tau \in H : \tau\sigma^{-1}(x) = \sigma^{-1}(x) \Leftrightarrow \sigma^{-1}x \in L^H \Leftrightarrow x \in \sigma(L^H)$

Zu b)

"⇒" Ist $E|K$ normal, so gilt $\sigma(E) = E$ für alle $\sigma \in Gal(L|K)$ nach theorem 2.35 b). $E = L^{Gal(L|E)} \overset{\sigma\Gamma(\cdot)\sigma^{-1}}{\Longrightarrow} \sigma Gal(L|E)\sigma^{-1} = \sigma\Gamma(E)\sigma^{-1} = Gal(L|E)$ für alle $\sigma \in Gal(L|K)$. Damit ist $Gal(L|E) = \Gamma(E)$ normal, also $Gal(L|E) \trianglelefteq Gal(L|K)$.

"⇐" $Gal(L|E) \trianglelefteq Gal(L|K)$, d.h. $\forall \sigma \in Gal(L|K)$ gilt $\sigma(E) = \sigma(L^{Gal(L|E)}) = L^{\sigma Gal(L|E)\sigma^{-1}} = L^{Gal(L|E)} = E$. Nach theorem 2.35 (ii) ist $E|K$ normal.

Sei $E|K$ normal. Die Restriktionsabbildung $r_E : Gal(L|K) \to Gal(E|K), \sigma \mapsto \sigma_{|E}$ ist Gruppenhomomorphismus mit $\ker(r_E) = Gal(L|E)$. r_E ist surjektiv: Für $\tau \in Gal(E|K)$ findet man dank Fortsetzungssatz (2.31) ein $\sigma \in Gal(L|K)$ sodass $\sigma_{|E} = \tau$. Mit Homomorphiesatz folgt die Behauptung.

□

Bemerkung 3.5. $L|K$ endliche Galoiserweiterung $H \leq Gal(L|K)$

- $[L : L^H] = |H|$
- $[L^H : K] = [L : K]/[L : L^H] = \frac{|Gal(L|K)|}{|H|} = [Gal(L|K) : H]$

Beispiel 3.6. Wie bei (theorem 2.36 a) L Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$. $L = \mathbb{Q}(a, ia, -a, -ia) = \mathbb{Q}(a, i)$ mit $a = \sqrt[4]{2}$. Damit ist $[L : \mathbb{Q}] = 8$. $L|\mathbb{Q}$ ist Galois Gruppe. $\sigma \in Gal(L|\mathbb{Q})$ eindeutig bestimmt durch $\sigma(a) \in \{a, ia, -a, -ia\}$, $\sigma(i) \in \{i, -i\}$. Da $|Gal(L|\mathbb{Q})| = 8$ sind alle Kombinationen möglich. **TODO Graphik** $Gal(L|\mathbb{Q}) = \{id, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$ $\tau\rho^{-1} = \rho\tau = \rho\tau^3$ Isomorph zu der Diedergruppe: $D_4 =< x, y \mid x^4 = 1, y^2 = 1, xy = yx^3 >$ **TODO Andere Graphik und mehr...**

VL vom 1.12.2023:

TODO Die Stunde muss korrigiert und formatiert werden!!!

Satz 3.7 (Produktsatz)**.** *Sei K Körper $L_1, L_2 \subset \overline{K}$ zwei Teilkörper sodass $(L_1|K)$ und $(L_2|K)$ endlich und galois'sch. Dann ist das Kompositum L_1L_2 eine Galois-Erweiterung von K. Die Zuordnung*

$$\Phi\colon Gal(L_1L_2|K)) \to Gal(L_1|K) \times Gal(L_2|K)$$
$$\sigma \mapsto (\sigma_{|L_1}, \sigma_{|L_2})$$

ist ein injektiver Gruppenhomomorphismus. Falls $L_1 \cap L_2 = K$, so ist Φ ein Isomorphismus.

Beweis. Damit L_1L_2 galois ist, muss es normal und separabel sein:

normal L_i ist Zerfällungskörper von $w_i \subset K[X] \setminus K$ ($i \in \{1, 2\}$)=> L_1L_2 ist Zerfällungskörper von $w_1 \cup w_2$ => $(L_1L_2|K)$ ist normal.

separabel Nach Satz **??** gilt $L_1 = K(a_1)$, $L_2 = K(a_2)$ mit $a_i \in L_i$. Sie sind separabel über K => $L_1L_2 = K(a_1, a_2)$ ist separabel über K (nach 2.47)

Φ ist injektiv, denn $\sigma \in \ker(\Phi) \Rightarrow \sigma_{|L_1} = id, \sigma_{|L_2} = id$ => $\sigma = id$, da L_1L_2 erzeugt wird von $L_1 \cup L_2$.

Fall $K = L_1 \cap L_2$: surjektivität: * Surjektivität von Φ im Fall $K = L_1 \cap L_2$: $(L_1L_2|L_1), (L_1L_2|L_2)$ sind Galoiserweiterungen. $\Phi_1 : Gal(L_1L_2|L_2) \to Gal(L_1|K), \sigma \mapsto \sigma_{|L_1}$ ist injektiv, denn $\sigma \in \ker(\Phi_1) \Rightarrow \sigma_{|L_1} = id$. Außerdem ist $\sigma_{|L_2} = id$, da σ L_2-Homomorphismus. => $\sigma = id$

Φ_1 ist surjektiv, falls $K = L_1 \cap L_2$: Sei $H = Bild(\Phi_1) \leq Gal(L_1|K)$. $L_1^H = \{x \in L_1 \mid \forall \sigma \in Gal(L_1L_2|L_2) \colon \sigma_{|L_1}(x) = x\} = L_1 \cap \underbrace{(L_1L_2)^{Gal(L_1L_2|L_2)}}_{=L_2} L_1 \cap L_2 = L_1^{Gal(L_1|L_1 \cap L_2)}$ => $H = Gal(L_1|L_1 \cap L_2)$

Analog mit $Phi_2 : Gal(L_1L_2|L_1) \to Gal(L_2|K), \sigma \mapsto \sigma_{|L_2}$

* $Gal(L_1L_2|K) \geq Gal(L_1L_2|L_i)$ => Φ ist surjektiv □

Beispiel 3.8. $L_1 = \mathbb{Q}(\sqrt[4]{2}, i)$ $L_2 = \mathbb{Q}(\sqrt{11})$ Zerfällungskörper von $X^2 - 11$. $L_1 \cdot L_2 = \mathbb{Q}(\sqrt[4]{2}, i, \sqrt{11})$ $L_1 \cap L_2 = \mathbb{Q}$ Damit gilt $Gal(L|\mathbb{Q}) \cong \underbrace{Gal(L_1|\mathbb{Q})}_{=D_4} \times \underbrace{Gal(L_2|\mathbb{Q})}_{=\mathbb{Z}/2\mathbb{Q}}$

§3.2 Kreisteilungskörper und Einheitswurzeln

Definition 3.9. Sei K Körper und $n \in \mathbb{N}$. Ein Element $\theta \in K^\times$ mit $\theta^n = 1$ heißt *n-te Einheitswulzel (EW)*. Hat θ die Ordnung n, so nennt man θ *primitive n-te EW*. $\mu_n(K) :=$ {n-te EW in K} $\leq K^\times$ zyklische Untergruppe. $|\mu_n(K)| \leq n$ $\mu_n^*(K) :=$ {primitive n-te EW in K}

Beispiel. $\mu_n(\mathbb{C}) = \{exp(2\pi i \frac{k}{n}) \mid k = 0, \ldots, n-1\}$ $exp(2\pi i \frac{2}{4} = exp(2\pi i \frac{1}{2})$ $\theta \in \mu_n(\mathbb{C})$ ist primitiv $\Leftrightarrow ggT(k,n) = 1$

$theta \in \mu_n(K) \setminus \{1\} \Rightarrow (X^n - 1)/(X - 1) = X^{n-1} + X^{n-2} + \cdots + X + 1$ hat θ als Nullstelle

TODO bild

Definition: K Körper, $n \in \mathbb{N}$ K_n ist definiert als Zerfällungskörper von $X^n - 1$ über K.

Satz 3.10. *K Körper, $n \in \mathbb{N}$, $char(K) \not| n$*

a) $(K_n|K)$ ist Galoiserweiterung, $|\mu_n(K_n)| = n$, $\phi_n := |\mu_n^*(K_n)| = |(\mathbb{Z}/n\mathbb{Z})^\times|$ $K_n = K(\theta)$ für $\theta \in \mu_n^*(K_n)$

b) $Gal(K_n|K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$

Beweis. Zu a) $(K_n|K)$ ist normal als Zerfällungskörper. Es ist $D(X^n - 1) = nX^{n-1}$, d.h. $X^n - 1$ und $D(X^n - 1)$ haben keine gemeinsamen NS d.h. $X^n - 1$ ist separabel $\overset{2.48}{\Rightarrow}$ $K_n|K$ ist separabel. Insbesondere hat $X^n - 1$ n verschiedene NS, d.h. $|\mu_n(K_n)| = n$. Gruppe der n-ten EW ist zyklisch (mit Argument wie in 2.49), also $|\mu_n^*(K_n)| = |\mathbb{Z}/n\mathbb{Z}|$

Zu b) $\sigma \in Gal(K_n|K)$, $theta \in \mu_n^*(K_n)$ $\sigma(\theta) = \theta^m$ für m teilerfremd zu n. σ ist durch m eindeutig bestimmt. $\Phi : Gal(K_n|K) \to (\mathbb{Z}/n\mathbb{Z})^\times, \sigma \mapsto m + n\mathbb{Z}$ ist ein injektiver Gruppenhomomorphismus. □

Definition 3.11. Der Körper $\mathbb{Q}(\theta_n)$ für $\theta_n \in \mu_n^*(\mathbb{C})$ heißt *n-ter Kreisteilungskörper*. Das Polynom $\phi_n = \Pi_{\theta \in \mu_n^*(\mathbb{C})}(X - \theta)$ heißt *n-tes Kreisteilungspolynom*

Lemma 3.12. $\phi_n \in \mathbb{Z}[X]$

Beweis. Beweis mit Induktion über n: IA: $\phi_1 = X - 1$ ✓$n \geq 2$: Wir verwenden, dass für $d < n$ $\phi_d \in \mathbb{Z}[X]$. Es ist $\mu_n(\mathbb{C}) = \bigcup_{d|n} \mu_d^*(\mathbb{C})$ (disjukt). $X^n - 1 = \Pi_{\theta \in \mu_n(\mathbb{C})}(X - \theta) = \Pi_{d|n} \underbrace{\Pi_{\theta \in \mu_d^*(\mathbb{C})}(X - \theta)}_{=\phi_d}$ Setze $f = \Pi_{d|n, d<n}\phi_d \overset{(IV)}{\in} \mathbb{Z}[X]$, f ist normiert. $X^n - 1 = qf + r$ mit $q, r \in \mathbb{Z}[X]$, $\deg(r) < deg(f)$. In $\mathbb{C}[X]$ $X^n - 1 = \phi_n f$, d.h. $r = (q - \phi_n)f$. Da $\deg(r) < \deg(f)$ gilt $\phi_n = q \in \mathbb{Z}[X]$ □

Bemerkung 3.13. Rekursive Bestimmung der Kreisteilungspolynome mittels $X^n - 1 = \Pi_{d|n}\phi_d$. Wenn $n = p$ prim: $\phi_p \cdot \phi_1 = X^p - 1$ -> $\phi_p = \sum_{k=0}^{p-1} X^k$.

$\phi_2 = X + 1$, $\phi_3 = X^2 + X + 1$ $\phi_4 \cdot \phi_2 \cdot \phi_1 = X^4 - 1$ -> $\phi_4 = X^2 + 1$. $\phi_6 \cdot \phi_3 \cdot \phi_2 \cdot \phi_1$ -> $\phi_6 = X^2 - X + 1$.

Für $p \in \mathbb{N}$ Primzahl und $\alpha \in \mathbb{N}$ gilt

$$X^{p^\alpha} - 1 = \Pi_{d|p^\alpha}\phi_d = \phi_{p^\alpha} \underbrace{\Pi_{d|p^{\alpha-1}}\phi_d}_{X^{p^{\alpha-1}}-1} = \phi_{p^\alpha}(X^{p^{\alpha-1}})$$

$$\phi_{p^\alpha} = \phi_p(X^{p^{\alpha-1}}) = \sum_{k=0}^{p-1}(X^{p^{\alpha-1}})^k$$

VL vom 7.12.2023:

Satz 3.14. *Das n-te Kreisteilungspolynom ϕ_n ist irreduzibel in $\mathbb{Q}[X]$, d.h. $\phi_n = m_{\xi,\mathbb{Q}}$ für $\xi \in \mu_n^*(\mathbb{C})$*

Beweis. Sei $\xi \in \mu_n^*(\mathbb{C})$. Sei $f := m_{\xi,\mathbb{Q}} \in \mathbb{Q}[X]$. Wir zeigen, dass jede primitive n-te EW eine Nullstelle von f ist. Dies imliziert $\phi_n | f$ und somit $\phi_n = f$ irreduzibel.

Da ξ Nullstelle von $X^n - 1$ ist, existiert ein $h \in \mathbb{Q}[X]$ mit $X^n - 1 = f \cdot h$. Weiter gilt, dass $f, h \in \mathbb{Z}[X]$ aus folgendem Grund:

Erinnerung (Gauß-Lemma 2.5 b).

$$c(f) \cdot c(h) = c(f \cdot h) = c(X^n - 1) = 1$$

Weiter ist $\underbrace{c(f)}_{=\tilde{c}(a \cdot f)a^{-1}}, c(h) \in \{\frac{1}{k} \mid k \in \mathbb{N}\}$. Also folgt $c(f) = c(h) = 1$. => $f, g \in \mathbb{Z}[X]$

Sei p eine Primzahl, die n nicht teilt. Dann ist ξ^p auch eine primimtive n-te EW. Wir behaupten, dass ξ^p eine Nullstelle von f ist.

Ist das nicht der Fall, dann ist $h(\xi^p) = 0$, also ist xi eine Nullstelle von $h(X^p)$. Somit $f | h(X^p)$. Es existiert $g \in \mathbb{Q}[X]$ mit $h(X^p) = f \cdot g$. Ähnlich wie oben ist sogar $g \in \mathbb{Z}[X]$. Betrachte die Reduktion $\mod p$:

$$\mathbb{Z}[X] \to \mathbb{F}_p[X], \sum_i c_i X^i \mapsto \sum_i \overline{c}_i X^i$$

. Dann ist $\overline{h}^p = \overline{h}^p(X^p) = \overline{f} \cdot \overline{g}$, weil p-te Potenz Homomorphismus in $char = p$ und nach Euler?? $c^p \equiv c \mod p$. Somit sind f und h nicht teilerfremd $\mod p$. Dann ist $X^n - 1 = \overline{f} \cdot \overline{h} \in \mathbb{F}_p[X]$ nicht separabel im Widerspruch zu $D(X^n - 1) = nX^{n-1} \neq 0$. Somit ist ξ^p Nullstelle von f.

Ist ξ' eine andere primitive n-te EW, dann ist $\xi' = \xi^m$ mit $(m,n) = 1$ und man erhält ξ' durch wiederholtes Bilden von Primpotenzen von ξ, wobei die Primexponenten zu n teilerfremd sind. Durch Wiederholhung des obigen Alguments bekommt man $f(\xi) = 0$. □

Korollar 3.15. *Sei $\xi \in \mu_n^*(\mathbb{C})$. Dann ist $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$ und $Gal(\mathbb{Q}(\xi)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$*

Beweis. Kombination von 3.10 und 3.14 □

Bemerkung (Satz von Kronecker-Weber ('Kroneckers Jugendtraum')). Jede endliche abelsche Erweiterung[13] von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten. **TODO Optional: Ausblick über dessen Konsequenzen (inc Graphik)**

§3.3 Charaktere und Normalbasen

Definition 3.16. Sei Γ eine Gruppe, K ein Körper. Ein *Charakter* (von Γ nach K) ist ein Homomorphismus $\Gamma \to K^\times$.

Für jede Menge M ist die Menge $Abb(M,K)$ der Abbildungen von M nach K ein K-Vektorraum bezüglich punktweiser Addition und skalarer Multiplikation.

Lemma 3.17. *K, Γ wie zuvor. Paarweise verschiedene Charakterer $\chi_1, \ldots, \chi_n$ von Γ nach K sind in $Abb(\Gamma, K)$ linear unabhängig.*

Beweis. Durch Induktion über n.

IA ($n = 1$) $\chi = \chi_1 \neq 0$, da χ Werte in $K^\times$ annimmt

$n \geq 2$ Annahme: Je $n-1$ verschiedene Charaktere sind linear unabhängig. Angenommen $\sum_{i=1}^n c_i \chi_i = 0$, wobei nicht alle c_i Null sind (Sei O.B.d.A.insbesondere $c_2 \neq 0$). Sei $\mu \in \Gamma$ mit $\chi_1(\mu) \neq \chi_2(\mu)$. Dann gilt für alle $\gamma \in \Gamma$:

$$(1): \quad 0 = \sum_{i=1}^n c_i \chi_i(\mu\gamma) = \sum_{i=1}^n c_i \chi_i(\mu)\chi_i(\gamma)$$

$$(2): \quad 0 = \chi_1(\mu) \sum_{i=1}^n c_i \chi_i(\gamma) = \sum_{i=1}^n c_i \chi_1(\mu)\chi_i(\gamma)$$

$$(1)-(2): \quad 0 = \sum_{i=1}^n c_i \underbrace{(\chi_i(\mu) - \chi_1(\mu))}_{=0 \text{ für } i=1} \cdot \chi_i(\gamma)$$

$$= \sum_{i=2}^n c_i \underbrace{(\chi_i(\mu) - \chi_1(\mu))}_{\neq 0 \text{ für } i=2} \cdot \chi_i(\gamma)$$

Damit sind $\chi_2, \ldots, \chi_n$ linear abhängig. ↯Widerspruch zu I-Annahme.

[13] Erweiterung mit abelscher Galoisgruppe

□

Korollar 3.18. *Paarweise verschiedene Automorphismen eines Körpers K sind linear unabhängig in* $Abb(K,K)$

Beweis. Sei $\sigma_1,\ldots,\sigma_n \in Aut(K)$. Dann wende lemma 3.17 auf $\sigma_{1|K^\times},\ldots,\sigma_{n|K^\times}$ an. □

Lemma 3.19. *Sei $L|K$ endliche und separabel. Sei $n=[L:K]$. Seien $\sigma_1,\ldots,\sigma_n : L \to \overline{K}$ paarweise verschiedene K-Homomorphismen. Dann sind äquivalent:*

(i) $v_1,\ldots,v_n \in L$ *bilden eine K-Basis von L*

(ii) $\det((\sigma_i(v_j))_{ij}) \neq 0$

Beweis.

(ii)⇒(i) Durch Kontraposition: Sei $v_1,\ldots,v_n$ also keine Basis. Wenn sie kein Erzeugendensystem sind, ist auch die lineare Unabhängigkeit verletzt, da $n=[L:K]$. $v_1,\ldots,v_n$ ist also nicht linear unabhängig. Sei dann $\sum_{j=1}^n \lambda_i v_i = 0$, wobei nicht alle $\lambda_j \in K$ Null sind. Dann ist $0=\sigma(0)=\sigma(\sum_{j=1}^n \lambda_i v_i)=\sum_{j=1}^n \lambda_j \sigma_i(v_j)$ für alle i. D.h. die Spalte von $(\sigma_i(v_j))_{ij}$ sind linear abhängig.

(i)⇒(ii) Durch Kontraposition: Sei det $=0$. Dann gibt es $\mu_1,\ldots,\mu_n \in \overline{K}$ mit $\sum_{i=1}^n \mu_i\sigma_i(v_j)=0$ für alle j (Zeilen lin. abh). Nach lemma 3.17 sind $\sigma_{1|L^\times},\ldots,\sigma_{n|L^\times}$ linear unabhängig. Falls $<\{v_1,\ldots,v_n\}>=L$, dann gilt $\sum_{i=1}^n \mu_i\sigma_i=0$ im Widerspruch zur linearen Unabhängigkeit. Also ist $v_1,\ldots v_n$ keine Basis.

□

Satz 3.20 (Satz von der Normalbasis)**.** *Sei $L|K$ eine endliche Galois-Erweiterung. Sei $n=[L:K]$ und $Gal(L|K)=\{\sigma_1,\ldots,\sigma_n\}$. Es existiert ein $a \in L$, sodass $\sigma_1(a),\ldots,\sigma_n(a)$ eine K-Basis von L bilden.*