Skript zur Vorlesung Algebra

Basierend auf der Vorlesung von
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 : Beachte beim Ziehen der 3. Wurzel in der Formel von Cardano explizit, dass eq. (5) erfüllt bleibt.

  Formel von Cardano

- 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 $\{e\} \neq N \triangleleft G$ 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.$\sigma = (1\ 2\ \dots\ r)\rho, \forall i \in \{1,2,3\} : \rho(i) = i$. 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 $N \ni \sigma^{-1}(2\ 3\ 4)\sigma(2\ 4\ 3) = (1\ 2\ 4\ 3\ \dots)$ ($\Rightarrow$ 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

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

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

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

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

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

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

$$\mathscr{G} : \{1\} = G_0 \lhd G_1 \lhd \dots \lhd G_i \lhd \dots \lhd G$$

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 $(\{G_{i-1}\} =)\{1_{G_i/G_{i-1}}\} \neq N \lhd G_i/G_{i-1}$. Dann ist mit lemma 0.10 (beachte, dass die kanon. Projektion surjektiv ist und $\pi^{-1}(\{G_{i-1}\}) = G_{i-1}$, $\pi^{-1}(G_i/G_{i-1}) = G_i$)

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

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

$\Leftarrow$ Sei $\mathscr{G}$ eine Normalreihe mit einfachen Faktoren und $\mathscr{H}$ eine Verfeinerung. Z.z. $\mathscr{H} = \mathscr{G}$, 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 $H_i = G_{i+1}$. $G_i \subseteq H_{j-1} \lhd H_j = G_{i+1} \overset{\rightarrow}{\pi_i} G_{i+1}/ = G_i$ 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 $\mathscr{G}$, $\mathscr{H}$ Normalreihen von G, dann gibt es Verfeinerung $\tilde{\mathscr{G}}$, $\tilde{\mathscr{H}}$ von $\mathscr{G}$, $\mathscr{H}$, 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 $\notin$ 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 $\mathscr{H} : \{0\} \lhd \mathbb{Z}/3\mathbb{Z} \lhd H$ die gleichen Faktoren (zweimal $\mathbb{Z}/3\mathbb{Z}$ 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

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

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

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

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)

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

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. "$\Rightarrow$: 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 $\{1\} \triangleleft G_i/_{G_{i-1}}$ 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).
"$\Leftarrow$: 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 $g^{-1}D(G)g = \langle [g^{-1}xg, g^{-1}yg] \mid x, g \in G \rangle = D(G)$.

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

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

(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

$$\{1\} = G_0 \lhd \dots \lhd G_n = G$$

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 $f = \sum_{0 \le i \le n} a_i X^i$ mit drei Eigenschaften:*

1) $a_n \notin P$

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

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. $f = g_0h_0$ mit $g_0, h_0 \in K[X]$. Setze

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

und

$$h := \tilde{c}(g_0)\tilde{c}(h_0)\tilde{c}(h_0)^{-1}h_0 = \tilde{c}(g_0h_0)a\tilde{c}(h_0)^{-1}h_0$$

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

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

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: $L|K$, $(L-K)^T$ $\begin{matrix} L \\ | \\ K \end{matrix}$

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 $i \in I ist \sum_j c_{ij} e_j = 0$. (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.

[3] irreduzible Polynome sind per Definition nicht-konstant

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).

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 $f = f_1 \dots f_r$ 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

$$K \subseteq L_1 \subseteq L_2 \subseteq \dots$$

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

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

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

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

$(\mathcal{U}, \leq)$ ist induktiv, d.h jede Kette in $(\mathcal{U}, \leq)$ (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 $(F_1, \tau_1) \in \mathcal{U}$. 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 $\overline{K}$.

$$\begin{tikzcd}
\overline{K'} \arrow[d, dash, "\text{alg.}"] & \text{alg. abgeschlossen} \\
\phi(\overline{K}) \arrow[d, dash] & \text{alg. abgeschlossen} \\
K' \arrow[uu, dash, bend left, "\text{alg.}"] &
\end{tikzcd}$$

Wegen remark 2.22 und der Algebraizität von $\overline{K'}|\phi(\overline{K})$ folgt $\phi(\overline{K}) = \overline{K'}$. $\square$

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).

$$\begin{array}{l}
L = K(\alpha_1, \ldots, \alpha_r) \\
\quad | \\
K(\alpha_1, \ldots, \alpha_{r-1}) \\
\quad \vdots \\
K
\end{array}$$

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 $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$

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

$$\shortparallel$$

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

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 $\forall x \in \mathbb{F}_5 \setminus \{0\}\colon f(x) = X^4 - 2 = 1 - 2 = 4 \neq 0$. 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.

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:

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

§2.6 Serperable Erweiterungen

Definition 2.38. Ein irreduzibles Polynom in $K[X]$ heißt *separabel*, wenn es im $\overline{K}$ nur einfache Nullstellen hat. (allgemein heißt ein 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 mehrfachen Nullstellen eines beliebigen 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.

Bemerkung. Schreibe $f = c\Pi_{j=1}^{d}(X - a_j) \in \overline{K}[X]$ mit $0 \neq c, a_1, \dots, a_d \in \overline{K}$. 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

$$1 = g(a_k)\underbrace{f(a_k)}_{= 0} + h(a_k)\underbrace{D(f)(a_k)}_{\neq 0}$$

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 algebraische 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.

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

[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.

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.

$\square$

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 $[L:K]_S \leq [L:K]$

Beweis.

$$\begin{tikzcd}
\overline{K} \arrow[dr, bend left, "\overline{\sigma}_i\ K\text{-Hom}"] \arrow[d, dash] & \\
M \arrow[r, "\tau_j", "L\text{-Hom}"'] \arrow[d, dash] & \overline{K} \\
L \arrow[ur, bend right, "\sigma_i K\text{-Hom}"'] \arrow[d, dash] & \\
K &
\end{tikzcd}$$

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 $L = K(a_1, \dots, a_n)$ 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 $[K(a):K]_S = \left|\{b \in \overline{K} \mid m_{a,k}(b) = 0\}\right| \leq \deg(m_{a,K}) = [K(a):K]$ $\square$

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

(i) $L|K$ separabel

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

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

[7] Nach theorem 2.35 b)

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

Beweis.

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

(ii) $\rightarrow$ (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) $\rightarrow$ (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:

§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 $\mathbb{F}|\mathbb{F}_p$ 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 $\mathbb{F}^\times$ 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 $\mathbb{F}_q$.*

[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 $char(K) > 0$.

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. $\square$

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 $p^{n'} = |\mathbb{F}_{q'}| = |\mathbb{F}_q|^m = (p^n)^m = p^{n \cdot m}$, 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 in $\overline{\mathbb{F}}_p$ realisiert werden. Die Eindeutigkeit folgt dann mit dem schon Gezeigten and dem vorherigen Satz. $\square$

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

$$\begin{tikzcd}
\mathbb{F}_5(t^{\frac{1}{15}}) \arrow[d, dash] \arrow[dd, bend right, dash, "\substack{\text{nicht normal}\\ \text{nicht separabel}}"'] & \cong \mathbb{F}_5(t^{\frac{1}{5}})/(X^3 - t^{\frac{1}{5}}) \\
\mathbb{F}_5(t^{\frac{1}{5}}) \arrow[d, dash, "\text{nicht separabel}"] & \cong \mathbb{F}_5(t)/(X^5 - t) \\
\mathbb{F}_5(t) &
\end{tikzcd}$$

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

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

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 $\mathbb{F}_p$ für 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 $1 \le m < n$. 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: $|\mathbb{F}_{p^n}|\mathbb{F}_p| = [\mathbb{F}_{p^n}:\mathbb{F}_p]_s = [\mathbb{F}_{p^n}:\mathbb{F}_p]=n$ □

VL vom 24.11.2023:

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

Beweis. Sei $H \le K^*$ 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 $|H_m| \le m$. 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 $ord(ab) = kgV(ord(b),m) > m$. ↯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. $L^* = \langle a \rangle$. 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 $L = K(a_1, a_2)$ und $\phi_1, \ldots, \phi_m : L \to \overline{K}$ seien die verschiedenen K-Einbettungen $L \to \overline{K}$, wobei $m = [L : K]_S = [L : K]$ weil separabel. Das Polynom

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

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 $g(c) \neq 0$. Also $(\phi_i(a_1) - \phi_j(a_1)) \cdot c + (\phi_i(a_2) - \phi_j(a_2)) \neq 0$ für alle $i < j$. Das ist $\phi_i(a_1 \cdot c + a_2) - \phi_j(a_1 \cdot c + a_2) \neq 0$ und $\phi_i(a) \neq \phi_j(a)$ mit $a := a_1 c + a_2 \in L$ 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.

$$\begin{array}{c} K(\sqrt[p]{s}, \sqrt[p]{t}) \\ \big\downarrow p \\ K(\sqrt[p]{s}) \\ \big\downarrow p \\ K \end{array}$$

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 $[L : K] = p^2$.
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.

"⊇" klar

"⊆" (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. *$Gal(L|L^H) = H$*

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

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

Betrachte Polynom $f_a = \prod_{i=1}^n (X - a_i)$. Für $\sigma \in H$ ist $\sigma_*(f) = \prod_{i=1}^n (X - \sigma(a_i)) = \prod_{i=1}^n (X - a_i)$.[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 $[L : L^H] = |H| = \left|Gal(L|L^H)\right|$ => $H = Gal(L|L^H)$. □

VL vom 30.11.2023:

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

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

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

[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

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:

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

Fix und Γ sind enthaltungsumkehrend:

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

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 $\forall \sigma \in H_2\colon \sigma(x) = x$, 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 $x \in L^{\sigma H \sigma^{-1}} \Leftrightarrow \forall \tau \in H\colon \sigma\tau\sigma^{-1}(x) = x \Leftrightarrow \forall \tau \in H\colon \tau\sigma^{-1}(x) = \sigma^{-1}(x) \Leftrightarrow \sigma^{-1}x \in L^H \Leftrightarrow x \in \sigma(L^H)$

Zu b)

“$\Rightarrow$“ 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 $Gal(L|E) \trianglelefteq Gal(L|K)$.

“$\Leftarrow$“ $Gal(L|E) \trianglelefteq Gal(L|K)$, 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:

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 für $\sigma \in \ker(\Phi)$ gilt $\sigma_{|L_1} = id$,$\sigma_{|L_2} = id$ und damit $\sigma = id$, da L_1L_2 erzeugt wird von $L_1 \cup L_2$.

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 für $\sigma \in \ker(\Phi_1)$ gilt $\sigma_{|L_1} = id$. Außerdem ist $\sigma_{|L_2} = id$, da σ L_2-Homomorphismus. $\Rightarrow \sigma = id$

Φ_1 ist surjektiv (falls $K = L_1 \cap L_2$): Sei $H = Bild(\Phi_1) \leq Gal(L_1|K)$.

$$\begin{aligned} L_1^H &= \{x \in L_1 \mid \forall \sigma \in Gal(L_1L_2|L_2) : \sigma_{|L_1}(x) = x\} \\ &= L_1 \cap (L_1L_2)^{Gal(L_1L_2|L_2)} \\ &= L_1 \cap L_2 \\ &= L_1^{Gal(L_1|L_1 \cap L_2)} \end{aligned}$$

$\Rightarrow H = Gal(L_1|L_1 \cap L_2)$

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 $\xi \in K^\times$ mit $\xi^n = 1$ heißt *n-te Einheitswulzel (EW)*. Hat ξ die Ordnung n, so nennt man ξ *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. $\mu_n(\mathbb{C}) = \{exp(2\pi i \frac{k}{n}) \mid k = 0, \dots, n-1\}$ $exp(2\pi i \frac{2}{4} = exp(2\pi i \frac{1}{2})$ $\xi \in \mu_n(\mathbb{C})$ ist primitiv $\Leftrightarrow ggT(k,n) = 1$

$theta \in \mu_n(K) \setminus \{1\} \Rightarrow (X^n - 1)/(X - 1) = X^{n-1} + X^{n-2} + \dots + X + 1$ hat ξ 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, $n \in \mathbb{N}$, $char(K) \nmid n$*

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

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) $\sigma \in Gal(K_n|K), theta \in \mu_n^*(K_n)$ $\sigma(\xi) = \xi^m$ 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 $\mathbb{Q}(\xi_n)$ für $\xi_n \in \mu_n^*(\mathbb{C})$ heißt n-ter *Kreisteilungskörper*. Das Polynom $\phi_n = \prod_{\xi \in \mu_n^*(\mathbb{C})}(X-\xi)$ 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). $X^n - 1 = \prod_{\xi \in \mu_n(\mathbb{C})}(X-\xi) = \prod_{d|n} \underbrace{\prod_{\xi \in \mu_d^*(\mathbb{C})} (X-\xi)}_{=\phi_d}$ Setze $f = \prod_{d|n, d<n} \phi_d \overset{(IV)}{\in} \mathbb{Z}[X]$, 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 $X^n - 1 = \prod_{d|n} \phi_d$. 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

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

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

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

IS $n \geq 2$ 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

[13] Erweiterung mit abelscher Galoisgruppe

$\mu \in \Gamma$ mit $\chi_1(\mu) \neq \chi_2(\mu)$. Dann gilt für alle $\gamma \in \Gamma$:

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

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

□

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 $\langle\{v_1,\ldots,v_n\}\rangle = L$, 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.

□

VL vom 8.12.2023:

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 $\underset{\substack{\| \\ id}}{\sigma_1}(a),\ldots,\sigma_n(a)$ eine K-Basis von L bilden. Eine solche Basis nennen wir* Normalbasis *von $L|K$.*

Beweis für unendliche Körper. Gemäß 3.19 reicht es ein Element $a \in L$ zu finden, mit $\det(\sigma_i(\sigma_j(a)))_{ij} \neq 0$. Nach dem Satz vom primitiven Element (2.56) gibt es ein $b \in L$ mit $K(b) = L$. Dann sind $b_i := \sigma_i(b)$ die paarweise verschiedenen Nullstellen von $f := m_{b,K} = \prod_{i=1}^n (X - \sigma_i(b)) \in K[X]$. Es ist $b_1 := b$ und $b_i := \sigma_i(b)$. Setze

$$g_j = \prod_{i \neq j} \frac{X - b_i}{b_j - b_i} \in L[X] \quad \text{womit } g_j(b_k) = \delta_{jk} = \begin{cases} 1 & \text{, wenn } j = k \\ 0 & \text{, wenn } j \neq k \end{cases}$$

Weiter ist

$$(1) \quad g_1 + \cdots + g_n = 1$$

, weil die linke Seite Grad $\leq n-1$ hat und beide Seiten für $b_1, \ldots, b_n$ übereinstimmen.

$$(2) \quad \sigma_{j_*}(g_1) = \sigma_{j_*}\left(\prod_{i \neq 1} \frac{X - b_i}{b_1 - b_i}\right) = \prod_{i \neq 1} \frac{X - \sigma_{j_*}(b_i)}{b_j - \sigma_{j_*}(b_i)} = \prod_{i \neq j} \frac{X - b_i}{b_j - b_i} = g_j$$

Betrachte die Matrix

$$A = (\sigma_{i*}(g_j))_{ij} \in M_n(L[X])$$

Beh: $\det(A) \neq 0 \in L[X]$

- Für jedes b_k ist $(g_i \cdot g_j)(b_k) = \delta_{ik} * \delta_{jk} = 0$ falls $i \neq j$. $\Rightarrow$ Für $i \neq j$ gilt $f = m_{b,K} | (g_i \cdot g_j)$. (smile)
- Multipliziere (1) mit g_i. Dann ergibt sich, dass $g_i^2 \equiv g_i \mod f \cdot L[X]$. (*)

Sei $B = AA^T = (\beta_{ij})_{ij} \in M_n(L[X])$. Dann gilt

$$\begin{aligned} \beta_{ij} &= \sum_{k=1}^n \sigma_{i*}(g_k)\sigma_{j_*}(g_k) \\ &\overset{(2)}{=} \sum_{k=1}^n \sigma_{i*}(\sigma_{k*}(g_1))\sigma_{j_*}(\sigma_{k*}(g_1)) \\ &= \sum_{k=1}^n \underbrace{(\sigma_i \circ \sigma_k)}_{=\sigma_{m(i,k)}}{}_*(g_1) \cdot \underbrace{(\sigma_j \circ \sigma_k)}_{\sigma_{m(j,k)}}{}_*(g_1) \end{aligned}$$

mit einer passenden Abbildung $m \colon [n] \times [n] \to [n]$.

$i = j$ $\beta_{ii} = \sum_{k=1}^n \left(\sigma_{m(i,k)}(g_1)\right)^2 = \sum_{k=1}^n g_k^2 \overset{(*)}{\equiv} \sum_{k=1}^n g_k \overset{(1)}{=} 1 \mod f \cdot L[X]$

$i \neq j$ $m(i,k) \neq m(j,k)$ für alle k. Wegen (smile) also $\beta_{ij} \equiv 0 \mod f \cdot L[X]$.

$\Rightarrow B \equiv I_n \mod f \cdot L[X] \Rightarrow \det(A)^2 = \det(B) \equiv 1 \mod f \cdot L[X]$. Insbesondere ist $\det(A) \neq 0$.

Weil K unendlich ist existiert ein $u \in K$ so, dass $p(u) \neq 0$, wobei $p := \det(A) \in L[X]$. Definiere $a := g_1(u)$.

Dann folgt:

$$\begin{aligned}
0 \neq p(u) &= \det\Big(\big(\sigma_{i*}(g_j)(u)\big)_{ij}\Big) \\
&= \det\Big(\big((\sigma_i \circ \sigma_j)_* g_j(u)\big)_{ij}\Big) \\
&= \det\Big(\big((\sigma_i \circ \sigma_j)(a)\big)_{ij}\Big) \\
&= \det\Big(\big(\sigma_i(\sigma_j(a))\big)_{ij}\Big)
\end{aligned}$$

□

§3.4 Auflösbarkeit von Gleichungen

Definition 3.21. Sei K eine Körper, $a \in K$. Eine Nullstelle von $X^n - a$ nennt man *Radikal* von a.

Die Nullstellen von $X^n - a$ in $\overline{K}$ sind

$$\{\xi \cdot \sqrt[n]{a} \mid \xi \in \mu_n(\overline{K})\}$$

. Der Zerfällungskörper ist $K(\xi, \sqrt[n]{a})$, wobei ξ eine primitive n-te EW ist.

Satz 3.22. *Sei K ein Körper, $n \in \mathbb{N}$ mit $char(K) \nmid n$.*[14] *Es enthalte K eine primitive n-te EW ξ*

(a) $K(\sqrt[n]{a})|K$ eine endliche Galois-Erweiterung. Die Galoisgruppe $Gal(K(\sqrt[n]{a})|K)$ ist zyklisch und ihre Ordnung teit n.

(b) Ist $L|K$ eine endliche Galois-Erweiterung mit $[L:K] = n$ und zyklischer Galoisgruppe, dann ist $L = K(\sqrt[n]{a})$ für ein $a \in K$.

Beweis.

a) $K(\sqrt[n]{a})|K$ ist galois'sch, weil $K(\sqrt[n]{a})$ Zerfällungskörper des separablen Polynoms $X^n - a$ ist. Sei $\sigma \in Gal(K(\sqrt[n]{a})|K)$. Dann ist $\sigma(\sqrt[n]{a}) = w_\sigma \cdot \sqrt[n]{a}$, wobei $\omega_\sigma = \xi^{m_\sigma}$ eine n-te EW ist. Die Abbildung $\psi : Gal(K(\sqrt[n]{a})|K) \to \mu_n(K), \sigma \mapsto \omega_\sigma = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ ist eine injektiver Gruppenhomomorphismus:

Gruppenhomomorphismus

$$\psi(\sigma\tau) = \frac{\sigma(\tau(\sqrt[n]{a}))}{\sqrt[n]{a}} = \frac{\sigma(\omega_\tau \cdot \sqrt[n]{a})}{\sqrt[n]{a}} = \omega_\tau \cdot \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \omega_\tau \cdot \omega_\sigma = \psi(\tau)\psi(\sigma)$$

injektiv , weil σ durch ω_σ eindeutig feistgelegt wird, da $\sqrt[n]{a}$ prim Element von $K(\sqrt[n]{a})$.

Wegen $\mu_n(K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ nach 3.10 a) ist $Gal(K(\sqrt[n]{a}|K))$ auch zyklisch

[14] 0 teilt keine Zahl

b) $L|K$ Galois mit $Gal(L|K) = \langle\sigma\rangle$. Langrange-Resolvente: $\phi = \sum_{i=0}^{n-1} \xi^{-i} \cdot \sigma^i \in Abb(L,L)$ Nach 3.18 sind $\sigma^0, ..., \sigma^{n-1}$ linear unabhängig in $Abb(L,L)$. Somit ist $\phi \neq 0$. Also existiert ein $c \in L$ mit $b := \phi(c) \neq 0$. Es gilt $\sigma(b) = \sum_{i=0}^{n-1} \xi^{-i} \cdot \sigma^{i+1}(c) = \xi \sum_{i=0}^{n-1} \xi^{-(i+1)} \cdot \sigma^{i+1} = \xi \cdot b$, weil $\xi^{-((n-1)+1)} = \xi^{-n} = \xi^0$ und $\sigma^{(n-1)+1} = \sigma^0$. Das Minimalpolynom von b hat die Nullstellen $b, \xi \cdot b, \xi^2 \cdot b, \ldots, \xi^{n-1} \cdot b$ und Grad $\leq n$. Also $m_{b,K} = \prod_{i=0}^{n-1}(X - \xi^i \cdot b) = X^n - b^n \in K[X]$. Wähle $a = b^n$.

$\square$

Definition 3.23.

(i) man sagt eine K-Erweiterung $L|K$ sei *durch Radikale auflösbar*, wenn ein Turm von endlichen K-Erweiterungen gibt $K = K_0 \subseteq K_1 \subseteq K_2 \cdots \subseteq K_r$, sodass

- Für alle i ist $K_i = K_{i-1}(u_i)$ mit $u_i^{m_i} \in K_{i-1}$ für $m_i \in \mathbb{N}$
- $L \subseteq K_r$

(ii) Wir nennen ein Polynom $f \in K[X] \setminus K$ durch Radikale auflösbar, wenn der Zerfällungskörper von f über K durch Radikale auflösbar ist.

Bedeutung: Die Nullstellen von f lassen sich mittels Körperoperationen (+ and *) und (iterierte) Wurzeln schreiben.

VL vom 15.12.2023:

Lemma 3.24. *K Körper mit $char(K) = 0$*

a) Wenn $L|K$ durch Radikale auflösbar, dann existiert ein Radikalturm $K \subseteq K_1 \subseteq \cdots \subseteq K_r$ mit $L \subseteq K_r$ und $K_r|K$ galois'sch.

b) Sei $\xi \in \overline{K}$ eine EW, dann ist $L|K$ durch Radikale auflösbar g.d.w. $L(\xi)|K(\xi)$ durch Radikale auflösbar ist.

Beweis. a) Induktion über die Länge des Turms: Der Induktionsanfang mit Länge 0 ist gegeben ✓. Für den Induktionsschritt betrachte einen Turm $K \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n$, wobei $K_n = K_{n-1}(u)$ mit $u^m \in K_{n-1}$ und $K_{n-1}|K$ galoisch ist. Nach Induktionsvorraussetzung muss ein solcher Turm existieren. Betrachte

$$f = \prod_{\sigma \in Gal(K_{n-1}|K)} (X^m - \sigma(u^m)) \in K[X]$$

. $f \in K[X]$, weil $\sigma \circ f = f$ (die Linearfaktoren werden nur permutiert) und somit alle Koeffizienten in $K_{n-1}^{Gal(K_{n-1}|K)} = K$ liegen müssen. Seien $u_1, \ldots, u_t$ die Nullstellen von f in M, dem Zerfällungskörper von f:[15]

$$K \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_{n-1}(u_1) \subseteq K_{n-1}(u_1,u_2) \subseteq \cdots \subseteq K_{n-1}(u_1,\ldots,u_t) = M$$

[15] Wenn K_{n-1} Zerfällungskörper von $W \subseteq K[X]$, dann ist M Zerfällungskörper von $W \cup \{f\}$

Die zu beweisende Aussage gilt mit $K_r := M$: $M|K$ ist normal (weil Zerfällungskörper) und separarabel (da $char(K) = 0$) und damit galois'sch. Offensichtlich ist auch $L \subseteq M$ und M lässt sich durch einen Radikalturm darstellen.

b)

$\Leftarrow$ Sei $K(\xi) \subseteq K_1 \subseteq K_r \supseteq L(\xi)$ ein Radikalturm für $L(\xi)|K(\xi)$. Erhalte neuen Turm mit $K \subseteq K(\xi) \subseteq K_1 \subseteq \cdots \subseteq K_r \supseteq L(\xi) \supseteq L$ einen neuen Radikalturm für $L|K$.

$\Rightarrow$ Sei $K \subseteq K_1 \subseteq \cdots \subseteq K_r \supset L$ ein Radikalturm für $L|K$. Dann ist $K(\xi) \subseteq K_1(\xi) \subseteq \cdots \subseteq K_r(\xi) \supseteq L(\xi)$.

□

Satz 3.25. *K Körper, $char(K) = 0$, $L|K$ endliche Erweiterung. Dann sind äquivalent:*

(i) $L|K$ ist durch Radikale auflösbar

(ii) Es existiert eine endliche galois'sche Erweiterung $M|K$ mit $L \subseteq M$ und $Gal(M|K)$ auflösbar.

Erinnerung. Gruppe G auflösbar, wenn eine Normalreihe $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = G$ und G_{i+1}/G_i abelsch existiert bzw. $G' = [G,G]$ terminiert in $\{1\}$ nach endlich vielen Schritten.

Beweis.

(ii) $\Rightarrow$ (i) Sei $n = [M : K]$ und $\xi \in \overline{K}$ eine primitive n-te Einheitswurzel. Nach 3.24 genügt es zu zeigen, dass $M(\xi)|K(\xi)$ durch Radikale auflösbar ist. Bemerke $M(\xi)|K(\xi)$ galois'sch, da $M|K$ bereits galois'sch nach Vorraussetzung.

$$Gal(M(\xi)|K(\xi)) \leq Gal(M|K)$$

gilt, da sich Automorphismen aus $G(M(\xi)|K(\xi))$ auf $Gal(M|K)$ eingeschränkt werden kann. Die ist möglich, da die evtl.[16] zusätzliche Nullstellen ξ^i (als Elemente in $K(\xi)$) fix gehalten werden und die Automorphismen in $Gal(M(\xi)|K(\xi))$ höchstens auf den verbleibenden Nullstellen/Elementen in M nicht-fix agieren können.

Nach theorem 1.12 sind die Untergruppen auflösbarer Gruppen auflösbar. Damit ist auch $Gal(M(\xi)|K(\xi))$ auflösbar, da $Gal(M|K)$ nach Vorraussetzung auflösbar.

Sei $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = Gal(M(\xi)|K(\xi))$ mit G_i/G_{i-1} abelsch, nach 1.13 sogar zyklisch. Definiere $K_i = M(\xi)^{G_{r-i}}$.

$$K(\xi) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = M(\xi)$$

Nach Haupsatz der Galoistheorie ist $M(\xi)|K_i$ galois'sch mit $Gal(M(\xi)|K_i) = G_{r-i}$. Nach 3.4 und wegen $G_{i-1} \trianglelefteq G_i$ folgt $Gal(K_{i+1}|K_i) = G_{r-i}/G_{r-i-1}$, was zyklisch ist

[16] ξ könnte bereits in M sein. In dem Fall ist $Gal(M(\xi)|K(\xi))$ die Menge der Automorphismen in $Gal(M|K)$ ist, die *xi* fix halten.

(siehe oben). Sei $m = [K_{i+1} : K_i] | n$ und K enthält eine primitive n-te EW. Dann gilt nach 3.22b) $K_{i+1} = K_i(\sqrt[n]{a})$ für ein $a \in K_{i-1}$

(i) $\Rightarrow$ (ii) Beweisidee: Gruppenturm aus Körperturm umsetzen. Mit lemma 3.24 finde Radikalturm $K = K_0 \subseteq \cdots \subseteq K_r$ mit $K_r|K$ galios'sch und $K_i = K_{i-1}(u_i)$ wobei $u_i^{m_i} \in K_{i-1}$ für geeignete $m_i \in \mathbb{N}$. Sei n eine Vielfaches von $m_1, \dots, m_r$ und ξ eine primitive n-te EW und $M = K_r(\xi)|K$ galois'sch. Setze $G_i = Gal(M|K_{r-i}(\xi)) \leq Gal(M|K)$. $K_{r-i}(\xi)$ ist Radikalerweiterung von K_{r-i-1}. Nach 3.22 gilt/gibt es? $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = Gal(M|K(\xi)) \leq Gal(M|K)$ Nach 3.22a) ist G_i/G_{i-1} für alle i zyklisch. Da $K(\xi)|K$ galois'sch, folg aus 3.4, dass normal Untergruppe und nach 3.10 ist die Faktorgruppe ablsch.

□

Korollar 3.26. *K Körper mit $char(K) = 0$. Dann $f \in K[X] \setminus K$ auflösbar durch Radikale gdw. Galoisgruppe des Zerfällungskörper auflösbar ist.*

Beweis.

$\Leftarrow$ L Zerfällungskörper, $Gal(L|K)$ auflösbar, setze $M = L$ in 3.25

$\Rightarrow$ Sei $L|K$ durch Radikale auflösbar. Nach 3.25 ist $K \subseteq L \subseteq M$. Da $L|K$ galois'sch, ist $Gal(M|L) \trianglelefteq Gal(M|K)$ und $Gal(M|K)/Gal(M|K) = Gal(L|K)$. Nach 3.25 ist $Gal(M|K)$ auflösbar und damit ist $Gal(L|K)$ als dessen Faktor auch auflösbar (nach 1.12).

□

Beispiel 3.27.

1. S_5 nicht auflösbar ($A_5 \leq S_5$ einfach, also nicht auflösbar). Wenn Polynom f so geartet ist, dass für dessen Zerfällungskörper M gilt $Gal(M|K) \cong S_5$, dann lassen sich die Nullstellen von f nicht durch iterierte Wurzeln sind. Z.B $f = X^5 - 25X + 5 \in \mathbb{Q}[X]$.

2. Alle Untergruppen von S_4, S_3 sind auflösbar.

VL vom 21.12.2023:

§3.5 Spur und Norm

Definition 3.28. Sei $L|K$ endlich. Sei $a \in L$. Die *Spur* $Sp_{L|K}(a) \in K$ ist die Spur des K-lin. Endomorphismus $\phi_a : L \to L, \phi_a(x) = a \cdot x$. Ähnlich definiert man die *Norm* $N_{L|K}(a) \in K$ als $\det(\phi_a)$. Das char. Polynom von ϕ_a bezeichnen wir mit $\chi_{a,L|K} \in K[X]$.

Offensichtlich ist $Sp_{L|K} : L \to K$ K-linear. Weiter ist $N_{L|K}(a \cdot b) = N_{L|K}(a) \cdot N_{L|K}(b)$.

Beispiel 3.29. $L = \mathbb{Q}(\sqrt{3})$, $K = \mathbb{Q}$. Sei $a = a_1 + \sqrt{3}a_2 \in L$, $a_i \in \mathbb{Q}$. Die darstellende Matrix von ϕ_a bez. der $\mathbb{Q}$-Basis $1, \sqrt{3}$ ist.

$$\begin{pmatrix} a_1 & 3a_2 \\ a_2 & a_1 \end{pmatrix}$$

Also gilt $Sp_{L|K}(a) = 2a_1$ und $N_{L|K}(a) = a_1^2 - 3a_2^2$

Lemma 3.30. *Sei M ein Zwischenkörper der endlichen Körpererweiterung $L|K$. Dann ist $\chi_{a,L|K} = \chi_{a,M|K}^{[L:M]}$ für $a \in M$.*

Beweis. Wähle VR-Basen $v_1, \dots, v_n$ von M über K, $w_1, \dots, w_m$ von L über M. Dann bilden die Produkte $w_k \cdot v_i$ eine VR-Basis von L über K. Sei A die darstellende Matrix von ϕ_a bezüglich $(v_1, \dots, v_n)$. Dann gilt

$$\chi_{a,M|L} = \det(X \cdot I_n - A)$$

Die darstellende Martix von $\phi_a : L \to L$ bezüglich der Basis $w_k \cdot v_i$ $(k = 1, \dots, m,\ i = 1, \dots, n)$ ist.

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & A \end{pmatrix}$$

$\Rightarrow \chi_{a,L|K} = \chi_{a,M|L}^m$, $m = [L : M]$ $\square$

Bemerkung 3.31. Unter der Vorraussetzung von 3.30 erhält man für $a \in M$, dass

$$Sp_{L|K}(a) = [L : M] \cdot Sp_{M|K}(a)$$
$$N_{L|K}(a) = N_{M|K}(a)$$

Satz 3.32. *Sei $L|K$ endlich und $a \in L$. Es sei $m_{a,K} = X^n + \alpha_{n-1}X^{n-1} + \dots + \alpha_0$. Dann gelten*

$$Sp_{L|K}(a) = -[L : K(a)]\alpha_{n-1}$$
$$N_{L|K}(a) = ((-1)^n \cdot \alpha_0)^{[L:K(a)]}$$

Beweis. Nach Lemma 3.30/3.31 reicht es den Fall $L = K(a)$ zu betrachten. In diesem Fall hat L die Basis $1, a, \dots, a^{n-1}$ über K. Die dazugehörige Matrix von ϕ_a lautet

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & -\alpha_0 \\ 1 & 0 & & & \vdots & -\alpha_1 \\ 0 & 1 & \ddots & & \vdots & -\alpha_2 \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 0 & -\alpha_{n-2} \\ 0 & 0 & \dots & \dots & 1 & -\alpha_{n-1} \end{pmatrix}$$

$\Rightarrow Sp_{L|K}(a) = -\alpha_{n-1} \quad \Rightarrow N_{L|K}(a) = (-1)^n \alpha_0$ $\square$

Bemerkung 3.33. Es gilt sogar $\chi_{a,K(a)|K} = m_{a,K}$. Cayley Hamilton: $\chi_{a,K(a)|K}(\phi_a) = 0$. Andererseits ist $0 = \chi_{a,K(a)|K}(\phi_a)(1) = \chi_{a,K(a)|K}(\underbrace{\phi_a(1)}_{=a})$. Da $\deg(\chi_{a,K(a)|K}) = \deg(m_{a,K})$ ist $m_{a,K} = \chi_{a,K(a)|K}$.

Satz 3.34. *Sei $L|K$ endlich und separabel. Sei $n = [L:K]$ und $\{\sigma_1, \dots, \sigma_n\} = Hom_K(L, \overline{K})$. Dann gilt*

$$Sp_{L|K}(a) = \sum_{i=1}^{n} \sigma_i(a)$$
$$N_{L|K}(a) = \prod_{i=1}^{n} \sigma_i(a)$$

TODO All contents from this lecture are in dire need of formating! Proceed with caution

Beweis. $m_{a,K} = X^r + \alpha_{r-1}X^{r-1} + \dots + \alpha_0$ das Minimalpolynom. Nach Lemma 2.44 ist $K(a)|K$ ist auch separabel. Folglich gibt es r verschiedene K-Homomorphismen $\tau_1, \dots, \tau_r$ von $K(a)$ nach $\overline{K}$. Weiter ist $m_{a,K} = \prod_{i=1}^{r}(X - \tau_i(a))$. => $\sum_{i=1}^{r} \tau_i(a) = -\alpha_{r-1}$ (**TODO why?**), $\prod_{i=1}^{r} \tau_i(a) = (-1)^r \cdot \alpha_0$.

Es ist $\{\sigma_{1|K(a)}, \dots, \sigma_{n|K(a)}\} = \{\tau_1, \dots, \tau_r\}$. Für jedes i ist die Anzahl der j's mit $\sigma_{j|K(a)} = \tau_i$ gleich $[L:K(a)]_S = [L:K(a)]$ Daher folgt $\sum_{j=1}^{n} \sigma_j(a) = [L:K(a)] \cdot \sum_{i=1}^{r} \tau_i(a) = -[L:K(a)]\alpha_{r-1} \overset{\text{Satz 3.32}}{=} Sp_{L|K}(a)$. □

Satz 3.35. *Sei M ein Zwischenkörper der endlichen Erweiterung $L|K$. Dann gelten $Sp_{L|K} = Sp_{M|K} \circ Sp_{L|M}$ und $N_{L|K} = N_{M|K} \circ N_{L|M}$*

Beweis. nur für separable Erweiterungen: Seien $hom_M(L, \overline{K}) = \{\tau_1, \dots, \tau_m\}$, $m = [L:M]$ $hom_K(M, \overline{K}) = \{\sigma_1, \dots, \sigma_l\}$, $l = [M:K]$. Dann ist $\{\overline{\sigma}_j \circ \tau_i \mid i \in \{1, \dots, m\}, j \in \{1, \dots, l\}\} = hom_K(L, \overline{K})$, wobei $\overline{\sigma}_j$ Erweiterung vorn σ_j zu $\overline{K} \to \overline{K}$ (siehe Beweis von 2.46)

$$\begin{aligned} Sp_{L|K}(a) &= \sum_{i,j} \overline{\sigma}_j(\tau_i(a)) \\ &= \sum_j \overline{\sigma}_j(\underbrace{\sum_i \tau_i(a)}_{Sp_{L|M}(a) \in M}) \\ &= \sum_j \sigma_j(Sp_{L|M}(a)) // \qquad = Sp_{M|K}(Sp_{L|M}(a)) \end{aligned}$$

□

Satz 3.36. *Sei $L|K$ endlich und separabel.*

1. *Es gibt ein $a \in L$ mit $Sp_{L|K}(a) \neq 0$*
2. *Durch $(v, w) := Sp_{L|K}(v \cdot w)$ wird eine symmetirsche Bilienarform des K-VR L definiert, die nicht ausgeartet ist.*

Beweis. Zu a) Die Homom. $\{\tau_1,\dots,\tau_n\} = hom_K(L|\overline{K})$ sind lin. unabhöngig als Elemente von $Abb(L^\times,\overline{K})$ und somit von $Hom_K(L,\overline{K})$. Da $Sp_{L|K} = \sum_{i=1}^n \tau_i$ kann $Sp_{L|K}$ nicht die Nullabbildung sein.

zu b) Sei $a \in L$ mit $Sp_{L|K}(a) \neq 0$. Dann gilt $(v, av^{-1}) = Sp_{L|K}(a) \neq 0$ => nicht ausgeartet $\square$

§3.6 Anwendungen der Galoistheorie

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

Beweis. Sei $\mathbb{R} \subseteq \mathbb{C} \subseteq L$ eine Kette von endlichen Erweiterungen. Zu zeigen: $L = \mathbb{C}$. Durch Vergrößern von L können wir annehmen, dass $L|\mathbb{R}$ eine Galoiserweiterung ist. Sei $G := Gal(L|\mathbb{R})$. Es ist $[L:\mathbb{R}] = |G| = 2^k \cdot m$ mit $2 \nmid m$. Es sei $H \leq G$ eine 2-Sylowuntergruppe von G.

$$\begin{tikzcd}
 & L \arrow[dl, dash, "2^k"'] \arrow[dr, dash] & \\
L^H \arrow[dr, dash, "m"'] & & \mathbb{C} \arrow[dl, dash] \\
 & \mathbb{R} &
\end{tikzcd}$$

Satz vom primitiven Element: $L^H = \mathbb{R}(\alpha)$. Da $m_{\alpha,\mathbb{R}}$ eine Nullstelle in $\mathbb{R}$ besitzt (Zwischenwertsatz!), ist $m_{\alpha,\mathbb{R}}$ linear, also $m = 1$ und $L^H = \mathbb{R}$. $\Rightarrow [L:\mathbb{R}] = 2^k$, $[L:\mathbb{C}] = 2^{k-1}$

Ang. $k \geq 2$. Dann existiert $H' \leq G' = Gal(L|\mathbb{C})$ mit $|H'| = 2^{k-2}$ (allg. Aussage über p-Gruppen)

$$\begin{tikzcd}
 & L \arrow[dl, dash, "2^{k-2}"'] \\
L^H \arrow[dr, dash, "2"'] & \\
 & \mathbb{C} \arrow[d, dash] \\
 & \mathbb{R}
\end{tikzcd}$$

Da jedes quadratische Polynom in $C[X]$ zerfällt in $\mathbb{C}$, folgt ähnlich wie oben ein Widerspruch (bet $m_{a,\mathbb{C}}$ für die $L^H = \mathbb{C}(a)$) $\square$

VL vom 22.12.2023: (Weihnachtsvorlesung)

§3.7 Transzendenz von e und π

Satz 3.37. *e ist transzendent (über $\mathbb{Q}$)*

Lemma 3.38. *Ist $F \in \mathbb{Z}[X]$ ein Polynom, das bei Stelle $s \in \mathbb{N}$ eine k-fache Nullstelle hat, so ist*

$$T := e^s \cdot \int_s^\infty F(x) e^{-x} dx$$

eine durch $k!$ teilbare ganze Zahl. Weiter gilt: $\frac{T}{k!} \equiv \frac{F}{(x-s)^k}_{|x=s} \mod k+1$

Beweis. Zunächst sei $s=0$. Der allgemeine Fall folgt dann duch Substitution $x=x'+s$. man hat $\int_0^\infty x^n e^{-x}dx = n!$. Da F eine Z-Linearkombination von Polynomen x^{k+j} ist, folgt daraus die erste Aussage.

$$\frac{1}{k!}\int_0^\infty x^{k+j}e^{-x}dx = \frac{(k+j)!}{k!} = \begin{cases} 1 & j=0 \\ (k+1)\dots(k+j) & j\geq 1 \end{cases}$$

$$\frac{x^{k+j}}{x^k}_{|x=0} = \begin{cases} 1 & j=0 \\ 0 & j\geq 1 \end{cases}$$

Beide sind kongruent $\mod k+1$ □

Beweis. Angenommen e wäre algebraisch über $\mathbb{Q}$. Dann gilt $a_0,\dots,a_n\in\mathbb{Z}$ mit $a_0+a_1\cdot e+\dots+a_n e^n=0$, $a_0\neq 0$. Für ein noch festzulegendes $F\in\mathbb{Z}[X]$ multipliziert mit $\int_0^\infty F(x)e^{-x}dx$:
->

$$0 \overset{(*)}{=} \sum_{s=0}^n a_s e^s \int_0^\infty F(x)e^{-x}dx = \underbrace{\sum_{s=0}^n a_s e^s \int_0^s F(x)e^{-x}dx}_{P_2:=} + \underbrace{\sum_{s=0}^n a_s e^s \int_s^\infty F(x)e^{-x}dx}_{P_1:=}$$

Besitzt F in 0 eine k-fache Nullstelle und in den Stellen $1,2,\dots,n$ eine $(k+1)$-fache Nullstelle besitzt, dann $\mathbb{Z}\ni P_1\equiv 0 \mod k!$[17] und $\frac{P_1}{k!}\equiv a_0\cdot\frac{F}{x^k}_{|x=0} \mod k+1$.[18] Für eine geeignete Wahl von F erhalten wir $\frac{P_1}{k!}\not\equiv 0 \mod k$ und somit $\frac{P_1}{k!}\neq 0$. Wähle $F(x)=x^k(x-1)^{k+1}\dots(x-n)^{k+1}$ für ein k, das ein Vielfaches von $a_0\cdot n!$. Für diese Wahl ist $a_0\frac{F}{x^k}_{|x=0}\not\equiv 0 \mod k+1$. Somit $P_1\neq 0$, also $|P_1|\geq 1$.

Für den gewünschten Wiederspruch zeigen wir nun $\left|\frac{P_2}{k!}\right|<1$ für $k\gg 1$. Beh: Für die obrige Wahl von F gibt es von k unabhängig Konstanten $C,M\geq 0$ mit $|P_2|\leq C\cdot M^k$.

My notes: P_2 lässt sich durch $n\cdot n^{n\cdot(k+1)+k}$, weil $s\leq n$, $e^{-x}\leq 1$. Dann ist $M=n^{n+1}$, $C=n^{n+1}$.

=>$\frac{P_2}{k!}\to 0$ für $k\to\infty$ (Stirling)↯. □

Ähnlich aber kompilizierter beweist man: Satz(Hilbert): Ist $P\in\mathbb{Q}[X]$ von Grad n und sind $s_1,\dots,s_n\in\mathbb{C}$ seine Nullstellen, dann $a+e^{s_1}+\dots+e^{s_n}\neq 0$ für alle natürlichen Zahlen a. [mult. die angenommene Gleichung mit $\int_0^\infty F(x)e^{-x}dx$ für ein geeignetes $F\in\mathbb{Z}[X]$]

Transzendenz von π. Ang. π wäre algrbaisch über $\mathbb{Q}$. Dann ist auch $x_1 := i\cdot\pi$ algebraische. Sei $0\neq Q\in\mathbb{Z}[X]$ sodass $Q(x_1)=0$. Es seien $x_2,\dots,x_n$ die anderen Nullstellen von Q. Wegen $e^{x_1}=-1$ ist dann

$$0=\prod_{i=1}^n(1+e^{x_i}) = 1+e^{s_1}+e^{s_2}+\dots+e^{s_m}$$

wobei jedes s_i genau die Summe einer bestimmten Anzahl von x_i's ist und $m=2^n-1$. Betrachte nun das Polynom $P=(X-s_1)\cdot\dots\cdot(X-s_m)\in\mathbb{C}[X]$. Da $s_i\in\mathbb{Q}(x_1,\dots,x_n)$, ist

[17] Richtig, weil richtig in jedem summanden??

[18] Lemma -> erster Summand in P_1. Die anderen summanden sind $0 \mod k+1$

$P \in \mathbb{Q}(x_1,\ldots,x_n)[X]$ und $G = Gal(\mathbb{Q}(x_1,\ldots,x_n)|\mathbb{Q})$. Jeges $\sigma \in G$ permutiert die x_i und somit die s_j. Daher gilt $P \in \mathbb{Q}(x_1,\ldots,x_n)^G[X] = \mathbb{Q}[x]$. Fun fact: P ist nicht irreduzibel.

Daher ergibt sich ein Widerspruch zum Satz von Hilbert □

4 Bewertungstheorie

VL vom 11.1.2024:

§4.1 Beträge

Definition 4.1. Ein *Betrag* auf einem Körper K ist eine $|\cdot| : K \to \mathbb{R}_{\geq 0}$ mit den Eigenschaften

i) $|x| = 0 \Leftrightarrow x = 0$

ii) $|x \cdot y| = |x| \cdot |y|$

iii) $|x + y| \leq |x| + |y|$

Aus ii) folgt $|1| \cdot |1| = |1| = 1$.

Beispiel 4.2.

i) $\mathbb{R}$ mit dem gewöhnlichen Absolutbetrag

ii) K beliebig. Dann definiert

$$|x|_{trivial} = \begin{cases} 1 & falls x \neq 0 \\ 0 & falls x = 0 \end{cases}$$

ein Betrag (genannt: *trivialer Betrag*)

iii) $\mathbb{C}$ mit dem komplexen Betrag

iv) Ist $|\cdot|$ ein Betrag auf L und K ein Teilkörper von L, so ist $|\cdot|_{|K}$ ein Betrag auf K.

Definition 4.3 (p-adischer Betrag). Sei $a \in \mathbb{Z}$ und p prim. Dann ist $\nu_p(a) = \sup\{e \in \mathbb{N} \mid p^e|a\} \in \mathbb{N}_0 \cup \{\infty\}$ die *p-adische Betrag*. Beachte $\nu_p(0) = \infty$.

Damit gilt:

$$a = \pm \prod_{p \text{ prim}} p^{\nu_p(a)}$$

Die Funktion $\nu_p : \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ heißt *p-adische Bewertung*. Sie hat die folgenden Eigenschaften

i) $\nu_p(a) = \infty \Leftrightarrow a = 0$

ii) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

iii) $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$

Sei nun $x \in \mathbb{Q}^\times$. Schreibe

$$x = p^m \cdot \frac{a}{b}$$

mit $m \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$. Definiere $\nu_p(x) = m$ und $\nu_p(0) = \infty$. Dies setzt die p-adische Bewertung von $\mathbb{Z}$ auf $\mathbb{Q}$ fort mit den gleichen Eigenschaften. Setze $|x|_p := p^{-\nu_p(x)}$ mit der Konvention $|0|_p = p^{-\infty} = 0$. Dann definiert $|\cdot|_p$ einen Betrag auf $\mathbb{Q}$, den *p-adischen Betrag*[19]. Die Eigenschaften i), ii) sind offensichtlich. Zu iii):

$$\begin{aligned} |x+y|_p &= p^{-\nu_p(x+y)} \\ &\leq p^{-\min\{\nu_p(x),\nu_p(y)\}} \\ &= \max\{p^{-\nu_p(x)}, p^{-\nu_p(y)}\} \\ &= \max\{|x|_p, |y_p|\} \end{aligned}$$

Dies wird *ultrametrische Dreiecksungleichung* genannt.

Definition 4.4. Eine Bewertung ν auf einem Körper K ist eine Funktion

$$\nu : K \to \mathbb{R} \cup \{\infty\}$$

mit folgenden Eigenschaften

i) $\nu(x) = \infty \Leftrightarrow x = 0$

ii) $\nu(x \times y) = \nu(x) + \nu(y)$

iii) $\nu(x+y) \geq \min\{\mu(x), \nu(y)\}$

Lemma 4.5. *Seien K ein Körper, ν eine Bewertung auf K und $a \in \mathbb{R}_{>1}$. Dann definiert $|x| = a^{-\nu(x)}$ einen Betrag auf dem die ultimetrische Dreiecksungleichung $|x+y| \leq \max\{|x|, |y|\}$ erfüllt.*

Beweis. analog zu p-adischen Betrag □

Beispiel 4.6. Sei K ein Körper. Sei $K(T) = Quot(K[T])$. Sei $K(T) \setminus \{0\} \ni x = \frac{f}{q}$, $f, g \in K[T]$. Setze $\nu_{deg}(x) = -\deg(f) + \deg(g)$ und $\nu_{deg}(0) = \infty$. Dies definiert eine Bewertung auf $K(T)$

Definition 4.7 (Metrik und Topologie)**.** Sei K ein Körper mit Betrag $|\cdot|$. Dann definiert $d(x,y) = |x-y|$ eine Metrik auf K. Insbesondere erhalten wir eine Topologie auf K vermöge

$$U \text{ offen } :\Leftrightarrow \forall u \in U \exists \varepsilon > 0 : B_\varepsilon^{|\cdot|} = \{v \in K \mid |u-v| < \varepsilon\} \subseteq U$$

Bemerkung 4.8. Die Addition und Multiplikation definieren stetige Abbildungen $K \times K \to K$.

Definition 4.9. Zwei Bewertungen $|\cdot|_1$, $|\cdot|_2$ sind *äquivalent*, wenn sie diesselbe Topologie auf K induzieren.

[19] Zum 2ten mal

Lemma 4.10. *Für zwei Beträge $|\cdot|_1$, $|\cdot|_2$ auf K sind folgende Aussagen äquivalent (schreibe $|\cdot|_1 \sim |\cdot|_2$):*

a) $|\cdot|_1 \sim |\cdot|_2$

b) $\forall x \in K : |x|_1 < 1 \Leftrightarrow |x|_2 < 1$

c) $\exists s \in \mathbb{R}_{>0} : |x|_1 = |x|_2^s$ *für alle* $x \in K$

Beweis.

a) $\Rightarrow$ b) Sei $x \in K$. Dann gilt

$$\begin{aligned} |x|_1 < 1 &\Leftrightarrow |x|_1^n \xrightarrow[n\to\infty]{} 0 \\ &\Leftrightarrow |x^n|_1 \xrightarrow[n\to\infty]{} 0 \\ &\Leftrightarrow |x^n|_2 \xrightarrow[n\to\infty]{} 0 \\ &\Leftrightarrow |x|_2^n \xrightarrow[n\to\infty]{} 0 \\ &\Leftrightarrow |x|_2 < 1 \end{aligned}$$

TODO Wieso folgt das in der Mitte aus äquivalenz?

b) $\Rightarrow$ c) Falls $|\cdot|_1$ nicht trivial ist, dann gilt es ein $y \in K^\times$ mit $|y|_1 < 1$. Somit ist $|\cdot|_1$ trivial gdw $|\cdot|_2$ trivial ist.

Wir nehmen nun an, dass $|\cdot|_1$ nicht trivial ist. Sei $x \in K^\times$. Schreibe $|x|_1 = |y|_1^\alpha$ für eine $\alpha \in \mathbb{R}$. Beh: $|x|_2 = |y|_2^\alpha$. Sei $(\frac{m_i}{n_i})_i$ eine Folge rationaler Zahlen, die von oben gegen α konvergiert.

$$|x|_1 \leq |y|_1^{\frac{m_i}{n_i}} \Rightarrow |x^{n_i}|_1 < |y^{m_i}|_1 \Leftrightarrow |x^{n_i}y^{-m_i}|_1 < 1$$

Damit folgt mit b), dass $|x^{n_i}y^{-m_i}|_2 < 1$ und somit (ähnlich wie für $|\cdot|_1$) $|x|_2 \leq |y|_2^{\frac{m_i}{n_i}}$.[20] Limes $i \to \infty$ ergibt, dass $|x|_2 \leq |y|_2^\alpha$. Das selbe Argument mit von unten gegen α konvergierende $\frac{m_i}{n_i}$ liefert $|x|_2 \geq |y|_2^\alpha$. Sei $s \in \mathbb{R}_{>0}$ mit $|y|_2 = |y|_1^s$. Dann folgt:

$$|x|_2 = |y|_2^\alpha = |y|_1^{s\cdot\alpha} = |x|_1^s$$

.

c) $\Rightarrow$ a) Sei $\varepsilon > 0$ und $u \in K$.

$$B_\varepsilon^{|\cdot|_1}(u) = \{u \in K \mid |x-u|_1 < \varepsilon\} = \{x \in K \mid |x-u| < \varepsilon^{-s}\} = B_{\varepsilon^{-s}}^{|\cdot|_2}(u)$$

$\Longrightarrow |\cdot|_1 \sim |\cdot|_2$

□

[20] **TODO Wieso gilt die Rückrichtung?**

Korollar 4.11. *Seien $|\cdot|_1, |\cdot|_2$ zwei nicht triviale, nicht äquivalente Beträge auf K. Dann gibt es ein $u \in K$ mit $|u|_1 < 1$ und $|u|_2 > 1$.*

Beweis. nach 4.10 b) finden wir $y \in K$ mit $|y|_1 < 1$ und $|y|_2 \geq 1$.[21] Falls $|y|_2 = 1$, wähle $w \in K$ mit $|w|_2 > 1$. Setze $u = y^m \cdot w$ für hinreichend großes m eine geeignete Wahl. □

Satz 4.12 (Approximationssatz)**.** *Seien $|\cdot|_1, \dots, |\cdot|_n$ nicht trivial, paarweise inäquivalente Beträge auf K. Für alle $a_1, \dots, a_n \in K$ und $\varepsilon > 0$ existiert ein $x \in K$ mit*

$$|a_i - x|_i < \varepsilon \textit{ für alle } i \in \{1, \dots, n\}$$

VL vom 11.1.2024:

Beweis. Behauptung: $\exists z \in K : |z|_1 > 1$ und $|z|_j < 1$ für $j \in \{2, ..., n\}$ Durch Induktion: Der Induktionsanfang $n = 2$ ist nach 4.11✓.

Angenommen es gibt $\tilde{z} \in K$ mit $|\tilde{z}|_1 > 1$ und $|\tilde{z}|_j < 1$ für $j \in \{2, ..., n-1\}$. Wähle $u \in K$ mit $|u|_1 > 1$ und $|u|_n < 1$ nach 4.11. Falls $|\tilde{z}|_n < 1$, dann ist $z = \tilde{z}$ das gesuchte Element. Falls $|\tilde{z}|_n = 1$, dann ist $z = u\tilde{z}^m$ für hinreichend großes m das gesuchte Element. <Argumentation, dass z gewünschte Eigenschaften hat...> Falls $|\tilde{z}|_n > 1$, dann betrachtet man die Folge $t_m := \frac{\tilde{z}^m}{1+\tilde{z}^m}$., für die die

$$\begin{aligned} t_m &\to 1 \quad \text{bez. } |\cdot|_1 \text{ und } |\cdot|_n \\ t_m &\to 0 \quad \text{bez. } |\cdot|_2, \dots, |\cdot|_{n-1} \end{aligned}$$

gelten. Dann ist $z = u \cdot t_m$ für hinreihend großes m das gesuchte Element. <Argumentation, dass z gewünschte Eigenschaften hat...>

Für ein $z \in K$ wie in der obigen beh. konvergiert die Folge $(\frac{z^m}{1+z^m})_m$ gegen 1 bez $|\cdot|_1$ und gegen 0 bez $|\cdot|_2, \dots, |\cdot|_n$.

Für jedes $i \in \{1, \dots, n\}$ können wir somit ein $z_i \in K$ konstrieren, das sehr nahe bei 1 bez $|\cdot|_i$ und sehr nahe 0 bez der restlichen Beträge. Das Element $x = a_1 \cdot z_1 + \dots + a_n \cdot z_n$ erfüllt die Anforderungen des Approximationssatzes. □

Definition 4.13. Ein Betrag $|\cdot|$ auf K heißt *archimedisch*, wenn

$$\{|n \cdot 1_K| \mid n \in \mathbb{N}\}$$

nicht beschränkt ist.[22]

Satz 4.14. *Ein Betrag ist genau dann nicht-archimedisch, wenn er die ultrametrische Dreiecksungleichung erfüllt.*

Beweis. $\Leftarrow$ $|n \cdot 1_K| = |1_K + \dots + 1_K| \leq |1_K| = 1$ also ist $|\cdot|$ nicht -archimedisch

[21] Sollten die Ungleichheiten vertauscht sind, kann das Inverse betrachtet werden.

[22] Nach Übung: Wenn ein Betrag $|\cdot|$ nicht-archimedisch, gilt $\sup\{|n \cdot 1_K| \mid n \in \mathbb{N}\} = 1$, wegen $|1| = 1$ und der ultrametrischen Dreiecksungleichung nach 4.14

$\Rightarrow$ Seien $x, y \in K$ mit O.B.d.A.$|x| \geq |y|$. Sei $B > 0$ eine obere Schranke für $\{|n \cdot 1_K| \mid n \in \mathbb{N}\}$.

$$\begin{aligned}
|x+y|^n = |(x+y)^n| &= |\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}| \\
&\leq \sum_{k=0}^{n} |\binom{n}{k} \cdot 1_K| \cdot |x|^k \cdot |y|^{n-k} \leq \sum_{k=0}^{n} |\binom{n}{k} \cdot 1_K| \cdot |x|^n \\
&\leq (n+1) \cdot B \cdot |x|^n
\end{aligned}$$

$$\Longrightarrow \quad |x+y| \leq \sqrt[n]{(n+1)B} \cdot |x| \overset{n \to \infty}{\Rightarrow} |x+y| \leq |x|$$

$\square$

Der Trick am Ende für 'schlechte'/ungenaue Ungleichungen: Betrachte Potenzen und ziehe von dem dort gezeigen die Wurzel. Das kann bessere Ungleichungen bringen.

Bemerkung 4.15.

a) Ist $|\cdot|$ ein nicht-archimedischer Betrag, dann ist $\nu(x) = -\log(|x|)$ eine Bewertung auf Körper K

b) Ist $|\cdot|$ nicht-archimedisch, $|x| > |y|$, dann folgt

$$|x| \leq |x-y+y| \leq \max\{|x-y|, |y|\} = |x-y| \leq |x|$$

und somit Gleichheit.

Satz 4.16 (Satz von Ostrowski). *Jeder nicht-triviale Betrag auf $\mathbb{Q}$ ist äquivalent zu $|\cdot|_p$ für eine Primzahl p oder zum Absolutbetrag $|\cdot|_\infty$.*

Beweis. Sei $\|.\|$ ein nicht-trivialer Betrag auf $\mathbb{Q}$.

1.Fall Sei $\|.\|$ nicht-archimedisch, d.h. $\|n\| \leq 1$ für alle $n \in \mathbb{N}$. Sei $\mathscr{A} := \{n \in \mathbb{Z} \mid \|n\| < 1\}$. Dann ist $\mathscr{A}$ ein Ideal in $\mathbb{Z}$. Es gibt eine Primzahl p mit $p \in \mathscr{A}$, ansonsten würe $\|.\|$ trivial wegen Primfaktorenzerlegung. Also

$$p\mathbb{Z} \subseteq \mathscr{A} \subset \mathbb{Z}$$

(da $1 \notin \mathscr{A}$). Da $p\mathbb{Z}$ maximales Ideal ist, ist $p\mathbb{Z} = \mathscr{A}$. Sei $q \in \mathbb{Q}^\times$ und schreibe $q = p^m \cdot \frac{a}{b}$ mit $p \nmid a$, $p \nmid b$. Dann gilt $\|q\| = \|p\|^m$ wegen $\|a\| = \|b\| = 1$. Sei $s > 0$ so, dass $p^{-s} = \|p\|$. Dann folgt $\|p\| = p^{-s} = (p^{-1})^s = |p|_p^s$
$\Longrightarrow \|q\| = \|p^m\| = |q|_p^s$.
$\Longrightarrow \|.\| \sim |.|_p$

2.Fall Sei $\|.\|$ archimedisch. Beh.: Für alle natürlichen $n, m \in \mathbb{N}_{>1}$ gilt

$$\|n\|^{\frac{1}{\log(n)}} = \|m\|^{\frac{1}{\log(m)}} \quad (*)$$

Somit $c := \|n\|^{\frac{1}{\log(n)}}$ unabhängig von $n > 1$. => $\|m\| = c^{\log(m)}$ für jedes $m \in \mathbb{N} \setminus \{1\}$. Wenn wir $c = e^s$, $s > 0$, schreibe, dann ergibt sich für jedes positive rationale Zahl $x = \frac{a}{b}$

$$\|x\| = e^{s\log(x)} = |x|_\infty^s$$

Damit folgt $\|.\| \sim |\cdot|_\infty$.

Zu $(*)$:
Schreibe $m \in \mathbb{N}$ zur Basis $n \in \mathbb{N}$ (O.B.d.A. $n < m$):

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

mit $a_i \in \{0, \ldots, n-1\}$, $a_r \neq 0$. Somit $n^r \leq m$, also $r \leq \frac{\log(m)}{\log(n)}$. Weiter $\|a_i\| \leq a_i \|1\| = a_i < n$. Es folgt

$$\|m\| \leq \sum_{i=0}^{r} \|a_i\| \cdot \|n\|^i \leq \sum_{i=0}^{r} n \cdot \|n\|^r \leq \left(1 + \frac{\log(m)}{\log(n)}\right) \cdot n \cdot \|n\|^{\frac{\log(m)}{\log(n)}}$$

Wir ersetzen in dieser Ungleichung m durch m^k und ziehen die k-te Wurzel:

$$\|m\| \leq \sqrt[k]{\left(1 + \frac{k \cdot \log(m)}{\log(n)}\right)} \cdot n^{1/k} \cdot \|n\|^{\frac{\log(m)}{\log(n)}}$$

$\Longrightarrow \|m\|^{\frac{1}{\log(m)}} \leq \|n\|^{\frac{1}{\log(n)}}$
Da die Rollen von m und n vertauschbar sind, folgt Gleichheit. $\square$

§4.2 Vervollständigungen

Definition 4.17. Ein Körper mit Betrag ist *vollständig*, wenn jede Cauchyfolge[23] in K konvergiert.

Beispiel 4.18.

- $(R, |\cdot|_\infty)$, $(\mathbb{C}, |\cdot|_\mathbb{C})$ sind vollständig
- $(\mathbb{Q}, |\cdot|_5)$ nicht vollständig[24] Sei $a_k + 5^k\mathbb{Z}$ ein Element in $(\mathbb{Z}/5^k\mathbb{Z})^\times$ der Ordnung 4.[25] Wir können erreichen, dass $a_k \equiv a_{k+1} \mod 5^k$ => $|a_k - a_{k+1}|_5 < \frac{1}{5^k}$, also ist $(a_k)_k$ eine Cauchyfolge bezüglich $|\cdot|_5$.

  $a_k + 5^k\mathbb{Z}$ hat Ordnung[26] 4, also $a_k^2 \equiv -1 \mod 5^k \Longrightarrow \lim_{k\to\infty} a_k^2 = -1$ bez $|\cdot|_5$. Also müsste ein Grenzwert $a = \lim_{k\to\infty} a_k$ in $\mathbb{Q}$ die Gleichung $a^2 = -1$ erfüllen $\lightning$**TODO Check for corectness**

VL vom 18.1.2024:

[23]Eine Folge $(a_n)_{n\in\mathbb{N}}$ ist eine *Cauchy-Folge*, wenn $\forall \varepsilon > 0\ \exists N \in \mathbb{N}\ \forall m,n \geq N\colon |a_m - a_n| < \varepsilon$
[24]Das Argument gilt für alle Primzahlen $p \equiv 1 \mod 4$
[25]Wegen $\phi(5^k) = 5^k - 5^{k-1} = 5^{k-1} \cdot 4$ $(k \geq 2)$ und der Tatsache, dass $(\mathbb{Z}/5^k\mathbb{Z})^\times$ yzklisch ist gilt, dass $(\mathbb{Z}/5^k\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5^{k-1}\mathbb{Z}$. Bei Hartnick gab es mehr dazu.
[26]Ordnung $ord_G(a) = \min\{i \in \mathbb{N} \mid a^i = 1\}$

Definition 4.19. Sei $(K,|\cdot|)$ ein Körper mit Betrag. Eine *Vervollständigung* von $(K,|\cdot|)$ ist ein Tripel $(\hat{K},\|\cdot\|,i)$ bestehend aus:

- einem vollständigen Körper $\hat{K}$ mit Betrag $\|\cdot\|$
- einem Homomorphismus $i : K \hookrightarrow \hat{K}$ so, dass
    1. $\|i(x)\| = |x|$ für alle $x \in K$ ("betragserhaltend")
    2. $i(K) \subseteq \hat{K}$ ist dicht[27]

Satz 4.20. *Jeder Körper mit Betrag $(K,|\cdot|)$ besitzt eine Vervollständigung $(\hat{K},\|\cdot\|,i)$, die bis auf kanonische Isomorphie eindeutig ist.*

Letzteres bedeutet: Ist $(\hat{K}_2,\|\cdot\|_2,i_2)$ eine andere Vervollständigung von $(K,|\cdot|)$, dann existiert ein Isomorphismus $\phi : \hat{K} \overset{\cong}{\to} \hat{K}_2$ so, dass

1. $$\begin{tikzcd} \hat{K} \arrow[rr, "\cong", "\phi"'] & & \hat{K}_2 \\ & K \arrow[ul, hook, "i"] \arrow[ur, hook, "i_2"'] & \end{tikzcd}$$ kommutiert und
2. ϕ ist betragserhaltend.

Für den Beweis im Falle der p-adischen Betrags siehe Goueva: p-adic numbersSS. 64-68. Der Beweis von 4.20 verläuft genauso wie die Konstruktion von $\mathbb{R}$ durch Cauchyfolgen in der Analysis.

Beweisskizze.
Zur Eindeutigkeit:
Für $x \in \hat{K}$ wähle $(x_n)_n$ in K mit $\lim_{n\to\infty} i(x_n) = x$ (Dichtheit). Setze $\phi(x) := \lim_{n\to\infty} i_2(x_n) \in \hat{K}_2$. Grenzwert ex., da $(i(x_n))_n$ genau dann eine Cauchyfolge ist, wenn $(i_2(x))_n$ eine ist, weil i, i_2 betragserhaltend sind. Zu zeigen:

- ϕ Homomorphismus
- ϕ betragserhaltend
- die Umkehrabbildung wird ähnlich konstruiert

Zur Existenz:
Sei $\mathscr{R} := \{\text{Cauchyfolgen in } K\}$ Durch punktweise Addition und Multiplikation wird $\mathscr{R}$ ein Ring mit Null $(0)_n$ und Eins $(1)_n$. Sei $I = \{(x_n)_n \in \mathscr{R} \mid \lim_{n\to\infty} x_n = 0\}$. Dann ist I ein Ideal. Setze $\hat{K} := \mathscr{R}/I$. $\hat{K}$ ist ein Körper: Sei $x + I \in \hat{K} \setminus \{0\}$ d.h. $x = (x_n)_n$ mit $(x_n)_n \notin I$. Insbesondere existiert $n_0 \in \mathbb{N}$ mit $x_n \neq 0$ für $x_n > n_0$. Setze $y_n \begin{cases} 1 & n \leq n_0 \\ x_n^{-1} & n > n_0 \end{cases}$. Dann ist

[27] Eine Menge $M \subseteq X$ ist dicht in X, wenn eine der folgenden äquivalenten Aussagen zutrifft:

- Zu jedem $x \in X$ und jedem $r > 0$ existiert ein Punkt $y \in M$, sodass $|x - y| < r$
- Zu jedem $x \in X$ existiert eine Folge $(x_n)_{n\in\mathbb{N}}$ von Punkten aus M, sodass $\lim_{n\to\infty} x_n = x$.

$(y_n)_n$ eine Cauchyfolge. Also $(y_n)_n \in \mathbb{R}$. Weiter gilt $(x_n)_n \cdot (y_n)_n = (x_n \cdot y_n)_n = (1)_n + (u_n)_n$ mit $u_n = 0$ für $n > n_0$, $(u_n)_n \in I$. $\Longrightarrow (y_n)_n + I$ Inverses von $(x_n)_n + I$ in $\hat{K}$. Der Betrag auf $\hat{K}$ ist definiert durch $\|(x_n)_n + I\| := \lim_{n\to\infty} |x_n|$ (wohldefiniert).

Definiere $i(x) = (x)_n + I \in \hat{K}$.

- i offensichtlich betragserhaltend
- $i(K) \subseteq \hat{K}$ dicht: Ist $(x_n)_n$ eine Cauchyfolge in K, dann

$$\lim_{n\to\infty} i(x_n) = (x_n)_n + I$$

.

- $\hat{K}$ ist vollständig: Ist $(y_n)_n$ eine Cauchyfolge in $\hat{K}$, dann wählen wir $x_n \in K$ mit $\|y_n - i(x_n)\| < \frac{1}{n}$. Dann gilt

$$\lim_{n\to\infty} y_n = \lim_{n\to\infty} i(x_n) = (x_n)_n + I$$

.

□

Definition 4.21. Die Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Betrags $|\cdot|_p$ nennt man den *Körper der p-adischen Zahlen* $\mathbb{Q}_p$

Bemerkung 4.22. Es gilt folgender Satz:
Ein Körper, der vollständig bez. eines archimdischen Betrags ist, ist isomorph zu $\mathbb{R}$ oder $\mathbb{C}$. Der Betrag ist äquivalent zum gewöhnlichen Betrag.

§4.3 Bewertungen und Bewertungsringe

Satz 4.23. *Sei K ein Körper mit Bewertung* $\nu : K \to \mathbb{R} \cup \{\infty\}$. *Dann ist*

$$\mathscr{O}_\nu = \{x \in K \mid \nu(x) \geq 0\}$$

[$\mathscr{O}_\nu = \{x \in K \mid \|x\|_\nu \leq 1\}$ *für* $\|x\|_\nu = a^{-\nu(x)}$*] ein Ring (genannt* Bewertungsring*). Der Ring* $\mathscr{O}_\nu$ *hat genau ein Maximales Ideal*

$$\mathscr{m}_\nu = \{x \in K \mid \nu(x) > 0\}$$

[$\mathscr{m}_\nu = \{x \in K \mid \|x\|_\nu < 1\}$*] und die Einheitengruppe*

$$\mathscr{O}_\nu^\times = \{x \in K \mid \nu(x) = 0\}$$

[$\mathscr{O}_\nu^\times = \{x \in K \mid \|x\|_\nu = 1\}$*]*

Beweis. $\mathscr{O}_\nu$ ist ein Ring wegen der ultrametrischen Dreicksungleichung. Die Aussage über $\mathscr{O}_\nu^\times$ folgt aus $\|x^{-1}\|_\nu = \|x\|_\nu^{-1}$. $\mathscr{m}_\nu$ ist ein Ideal: Für $a \in \mathscr{O}_\nu$ und $x \in \mathscr{m}_\nu$ ist $\|ax\|_\nu = \|a\|_\nu \cdot \|x\|_\nu < 1$ Für $x, y \in \mathscr{m}_\nu$ ist $\|x+y\|_\nu \leq \max\{\|x\|_\nu, \|y\|_\nu\} < 1$.

Sei $\emptyset \neq I \subset \mathscr{O}_\nu$. Dann $I \cap \mathscr{O}_\nu^\times = \emptyset$, sonst $1 \in I$ und $I = \mathscr{O}_\nu$. $\Longrightarrow I \subseteq \mathscr{m}_\nu$. Somit ist $\mathscr{m}_\nu$ das eindeutige maximale Ideal. □

Definition 4.24. Ein kommultiver Ring R mit genau einem maximalen Ideal $\mathfrak{m}$ heißt *lokaler Ring*. Der Körper $R/\mathfrak{m}$ ist der *Restklassenkörper* vorn R.

Beispiel 4.25. Betrachet $\mathbb{Q}$ mit der p-adischen Bewertung v_p.

$$\mathscr{O}_{v_p} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, a, b \in \mathbb{Z}, p \nmid b \right\} = \mathbb{Z}_{(p)}{}^{28}$$

$$\mathfrak{m}_{v_p} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, p|a, p \nmid b \right\} = p \cdot \mathscr{O}_{v_p} = p\mathbb{Z}_{(p)}$$

Weiter ist $\mathscr{O}_{v_p}/\mathfrak{m}_{v_p} \xrightarrow{\cong} \mathbb{F}_p$

$$\left[\frac{a}{b}\right] \mapsto \overline{a} \cdot \overline{b}^{-1}$$

Lemma 4.26. *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Dann gilt $R^\times = R \setminus \mathfrak{m}$.*

Beweis.

- $\subseteq$ $x \in R^\times \Rightarrow xR = R \Rightarrow x \notin \mathfrak{m}$
- $\supseteq$ $x \in R \setminus \mathfrak{m}$. Dann ist das Ideal xR nicht in $\mathfrak{m}$ enhalten. Da $\mathfrak{m}$ das einzige maximale Ideal und jedes Ideal $\neq R$ in einem maximalen Ideal enthalten ist, ist $xR = R \implies x \in R^\times$

□

VL vom 19.1.2024:

Definition 4.27. Man nennt eine Bewertung *diskret*, wenn sie Werte in $\mathbb{Z} \cup \{\infty\}$ annimmt. Ein Element π mit Bewertung $v(\pi) = 1$ heißt *uniformisierndes Element*.

Bemerkung 4.28. Sei π uniformisierendes Element von K mit Bewertung v. Dann kann man jedes $x \in K^\times$ schreiben als $x = \pi^m \cdot u$ mit $m = v(x)$, $u \in \mathscr{O}_v^\times$, denn $v(\pi^m x^{-1}) = 0$ also $\pi^m x^{-1} \in \mathscr{O}_v^\times$ und damit existiert $\mathscr{O}_v^\times \ni (\pi^m x^{-1})^{-1} = x\pi^{-m} =: u$.

Satz 4.29. *Für einen Kommutativen Ring A sind folgende Aussagen äquivalent:*

(a) A ist Bewertungsring einer diskreten (nicht-trivialen??) Bewertung auf einem Körper.

(b) A ist ein lokaler Hauptidealring, aber kein Körper

Jeder Ring, der diese Bedingungen erfüllt, heißt diskreter Bewertungsring.

Beweis.

(a) $\Rightarrow$ (b) Sei $A = \mathscr{O}_v$ für eine diskrete Bewertung v auf K. Nach 4.23 ist A lokaler Ring A ist kein Körper, weil ein uniformisierendes Element nicht invertierbar ist.**TODO Wieso muss ein solches Element existieren? Jeder nicht-triviale Betrag lässt sich zu einem äquivalenten Betrag machen, der ein uniformisierendes Element hat (mit ggt der möglichen Werte 1 oder nicht ein und dann einfach durch den**

[28] Siehe A3 auf Blatt 10

ggt Teilt) Sei $I \subseteq$ ein Ideal mit $I \neq (0)$. Beh: $I = \pi^n \cdot A$ für ein $n \in \mathbb{N}$, wobei π uniformisierend. Sei $y \in A \setminus \{0\}$. Schreibe $y = \pi^m \cdot u$ mit $m = \nu(y)$, $u \in A^\times = \mathcal{O}_\nu^\times$. Daher gilt $y \in I \Leftrightarrow u^{-1} y \in I \Leftrightarrow \pi^m = \pi^{\nu(y)} \in I$. Sei $n \in \mathbb{N}_0$ minimal mit $\pi^n \in I$. Dann $I = \pi^n \cdot A = \{x \in A \mid \nu(x) \geq n\}$.

(b) $\Rightarrow$ (a) Setze $K := Quot(A)$. Sei $\mathfrak{m} \subseteq A$ das (eindeutige) maximale Ideal. Sei $\pi \in \mathfrak{m}$ ein Erzeuger, d.h. $\pi A = \mathfrak{m}$. A ist kein Körper $\Longrightarrow \mathfrak{m} \neq (0) \Longrightarrow \pi \neq 0$. $\mathfrak{m}$ ist auch das einzige Primideal, da in Hauptidealringen Primideale maximal sind.
Eindeutige Primfaktorzerlegung und 4.26[29]:

$$A \setminus \{0\} \ni a = \pi^n \cdot u \text{ mit } n \in \mathbb{N}_0,\, u \in A^\times$$

Jedes $x \in K \setminus \{0\}$ schreibt sich eindeutig als

$$x = \pi^m \cdot u, m \in \mathbb{Z}, u \in A^\times$$

Definiere $\nu(x) := m = \max\{k \in \mathbb{Z} \mid x \in \pi^k A\}$ und $\nu(0) = \infty$. ν ist eine Bewertung auf K (A3 auf Blatt 10). Es ist dann $A = \mathcal{O}_\nu$.

□

Bemerkung 4.30. Sei K ein Körper mit diskreter Bewertung ν. Sei $|x| = a^{-\nu(x)}$ ein Betrag mit $a > 1$. Eine Folge $(x_n)_n$ in K ist eine Cauchy bezüglich $|\cdot|$ gdw.

$$\forall B > 0\ \exists N \in \mathbb{N}\ \forall n, m > N : \nu(x_n - x_m) > B$$

Ist K vollständig bezüglich $|\cdot|$, dann ist K vollständig bezüglich aller von ν induzierten Beträge, und wir sagen, dass K *vollständig bez.* ν ist.

Satz 4.31 (Satz über Reihendarstellung). *Sei K vollständig mit disketer Bewertung ν. Seien $\pi \in \mathcal{O}_\nu$ ein uniformisierendes Element und $\Omega \subseteq \mathcal{O}_\nu$ ein Repräsentantensystem für $\mathcal{O}_\nu / \mathfrak{m} = \mathcal{O}_\nu / \pi \mathcal{O}_\nu$.*

(a) Jede Laurentreihe $\sum_{n=m}^{\infty} a_n \cdot \pi^n$ mit $m \in \mathbb{Z}, a_n \in \Omega$, konvergiert in K.

(b) Jedes $x \in K^\times$ lässt sich eindeutig schreiben als $x = \sum_{n=\nu(x)}^{\infty} a_n \cdot \pi^n$ mit $a_n \in \Omega$.

Beweis. (a) Betrachte die Partialsumme $S_k = \sum_{n=m}^{k} a_n \cdot \pi^n$. Z.z. $(S_k)_{k \in \mathbb{N}}$ ist eine Cauchyfolge bezüglich ν.

$$\begin{aligned} \nu(S_k - S_l) =& \nu\left(\sum_{n=l+1}^{k} a_n \cdot \pi^n\right) \geq \min\{\nu(a_n \pi^n) \mid l+1 \leq n \leq k\} \\ =& \min\{n \cdot \underbrace{\nu(\pi)}_{=1} + \underbrace{\nu(a_n)}_{\geq 0} \mid l+1 \leq n \leq k\} \geq \min\{n \mid l+1 \leq n \leq k\} > l \end{aligned}$$

impliziert Cauchy.

[29] **TODO Wieso gibt es eine solche Primfaktorzerlegung?** Gegeben eine Primfaktorzerlegung $a = \varepsilon \cdot q_1 \cdot \ldots q_n$ mit $\varepsilon \in A^\times$ und $q_i \in A \setminus A^\times$ irreduzibel, ist nach 4.26 $q_i \in \mathfrak{m} \Rightarrow q_i = a_i \cdot \pi$. Wenn $a_i \notin A^\times$, wäre $q_i = \underbrace{a_i}_{\notin A^\times} \cdot \underbrace{\pi}_{\notin A^\times}$ nicht irreduzibel $\not\Rightarrow$ $a_i \in A^\times$. Damit ergibt sich $a = \underbrace{\varepsilon \cdot a_1 \cdot \dots \cdot a_n}_{=:u \in A^\times} \cdot \pi^n$

(b) Wir zeigen per Induktion zunächst Existenz: Es gibt $a_{\nu(x)}, \dots, a_k \in \Omega$ mit $\nu\left(x - \sum_{n=\nu(x)}^{k} a_n \pi^n\right) \geq k+1$.

Induktionsanfang $k < \nu(x)$: $\nu(x-0) \geq k+1 \checkmark$.

Induktionsschritt: Seien $a_{\nu(x)}, \dots, a_k$ wie oben bekannt. Es gibt ein eindeutiges $a_{k+1} \in \Omega$ mit $\underbrace{(x - \sum_{n=\nu(x)}^{k} a_n \pi^n)}_{\in \pi^{k+1}\mathcal{O}_\nu \text{ nach 4.28}} \pi^{-(k+1)} - a_{k+1} \in \pi \mathcal{O}_\nu$.[30]

$\Longrightarrow x - \sum_{n=\nu(x)}^{k+1} a_n \pi^n \in \pi^{k+2}\mathcal{O}_\nu \Longrightarrow \nu(x - \sum_{n=\nu(x)}^{k+1} a_n \pi^n) \geq k+2$

Zur Eindeutigkeit: Sei $x = \sum_{n=\nu(x)}^{\infty} b_n \pi^n$ eine andere solche Darstellung. Sei k minimal mit $a_k \neq b_k$.

$\Longrightarrow 0 = (a_k - b_k)\pi^k + r\pi^{k+1}$ für ein $r \in \mathcal{O}_\nu$.

$\Longrightarrow a_k \equiv b_k \mod \pi\mathcal{O}_\nu$.

$\Longrightarrow a_k = b_k$, weil Ω ein Repräsentantensystem von $\mathcal{O}_\nu/\pi\mathcal{O}_\nu$ ist.

□

Lemma 4.32 (Henselsches Lemma)**.** *Sei K ein vollständiger Körper mit diskreter Bewertung ν. Sei $q : \mathcal{O}_\nu \to \mathcal{O}_\nu/\mathfrak{m}_\nu$ die Projektion. Sei $f \in \mathcal{O}_\nu[X]$. Hat $q_*(f) \in \mathcal{O}_\nu/\mathfrak{m}_\nu[X]$ eine einfache Nullstelle in $\mathcal{O}_\nu/\mathfrak{m}_\nu$, dann hat f eine Nullstelle in $\mathcal{O}_\nu$.*

Beispiel. Betrachte $f(x) = x^2+1 \in \mathbb{Q}_5[X]$ (siehe 4.18). $q_*(f)(x) = x^2+1 \in \mathbb{F}_5[X]$ hat Nullstelle $\overline{2} \in \mathbb{F}_5$. Diese ist einfach, weil $D_{q_*}(f)(\overline{2}) = 2 \cdot \overline{2} \neq 0$ in $\mathbb{F}_5$. Nach Hensel hat f eine Nullstelle in $\mathbb{Z}_5$.

Beweis. Wir zeigen induktiv: Für alle $n \in \mathbb{N}$ gibt es $a_n \in \mathcal{O}_\nu$ gilt

(i) $f(a_n) \equiv 0 \mod \pi^n\mathcal{O}_\nu$

(ii) $a_n \equiv a_{n+1} \mod \pi^n\mathcal{O}_\nu$.

Wähle $a_1 \in \mathcal{O}_\nu$ so, dass $q_*(f)(\overline{a}_1) = 0 \in \mathcal{O}_\nu/\pi\mathcal{O}_\nu \Leftrightarrow f(a_1) \equiv 0 \mod \pi\mathcal{O}_\nu$. Angenommen wir haben $a_n \in \mathcal{O}_\nu$ wie oben.

Ansatz: $a_{n+1} = a_n + \pi^n \cdot b$ für $b \in \mathcal{O}_\nu$.

Beobachtung:

1. $(a_n + \pi^n \cdot b)^m = a_n^m + m \cdot \pi^n \cdot b \cdot a_n^{m-1} \mod \pi^{n+1}\mathcal{O}_\nu$.
   $\Longrightarrow f(a_n + \pi^n b) \equiv f(a_n) + \pi^n \cdot b \cdot D(f(a_n)) \mod \pi^{n+1}\mathcal{O}_\nu$.
2. Da $\overline{a}_1 \in \mathcal{O}_\nu/\pi\mathcal{O}_\nu$ eine einfache Nullstelle von q_*f, gilt $0 \neq q_*D(f)(\overline{a}_1) \overset{(ii)}{=} q_*D(f)(\overline{a}_n)$. Somit $D(f)(a_n) \in \mathcal{O}_\nu^\times$.

Nach (i) ist $f(a_n) = \pi^n \cdot u$ mit $u \in \mathcal{O}_\nu$. Setze $b := -u \cdot D(f)(a_n)^{-1}$. Dann $f(a_{n+1}) \equiv 0 \mod \pi^{n+1}\mathcal{O}_\nu$ □

[30]Wähle a_{k+1} sodass es die passende nebenklasse in $\pi\mathcal{O}_\nu$

Fortsetzung des Beispiels? (Lose formatiert)
$a_1 = 2$
$(2+b\cdot 5)^2 \equiv -1 \mod 5^2$
$4+4\cdot 5\cdot b \equiv -1 \mod 5^2$
=> $5^2 | 5+4\cdot 5\cdot b = 5(1+4\cdot b)$
<=> $5|1+4\cdot b$
$b = 1$ ist Lösung

$a_2 = 2\cdot 5^0 + 1\cdot 5^1$
$(2+1\cdot 5+c\cdot 5^2)^2 \equiv -1 \mod 5^3$
$7^2+2\cdot 7\cdot c\cdot 5^2 \equiv -1 \mod 5^3$
<=> $50+2\cdot 7\cdot c\cdot 5^2$
<=> $5|2+2\cdot 7\cdot c$
$c = 2$ Lösung
$a_3 = 2\cdot 5^0 + 1\cdot 5^1 + 2\cdot 5^3 + \dots$

14.1.2024

Satz 4.33. *Sei K ein vollständiger Körper bezüglich einer Bewertung ν. Dann besitzt ν eine eindeutige Bewertungsfortsetzung auf jeder endlichen Erweiterung $L|K$. Diese ist durch*

$$\nu_L(\alpha) = \sqrt[n]{\nu\left(N_{L|K}(a)\right)}$$

gegeben, wobei $n = [L:K]$. Weiter ist L bezüglich ν_L vollständig.

Bachte, dass für $\alpha \in K$: $N_{L|K}(\alpha) = \alpha^n$ und $\nu(N_{L|K}(\alpha)) = \nu(\alpha)^n$.

Bemerkung 4.34 (Die p-adischen Zahlen). $\mathbb{Q}_p$ mit ν_p bezüglich $|\cdot|_p$ p-adische (rationale) Zahlen. Einnerung: $|x|_p = p^{-\nu_p(x)}$, wobei $\nu_{p|\mathbb{Q}}$ gegeben ist durch $\nu_p(p^n \frac{a}{b}) = n$ mit $p \nmid a$, $p \nmid b$. p ist uniformisierendes Element.

Der Bewertungsring $\mathbb{Z}_p := \mathscr{O}_{\nu_p}$ heißt der *Ring der ganzen p-adischen Zahlen*. Es gilt

$$\mathbb{Z}_p \cap \mathbb{Q} = \{x \in \mathbb{Q} \mid \nu_p(x) \geq 0\} = \mathbb{Z}_{(p)}$$ [31]

Teilmenge $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ ist offen und abgeschlossen, denn:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\} = \overline{B_1(0)} \text{ und } \mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p < p\} = B_p(0)$$

Da $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ offen und $\mathbb{Q} \subseteq \mathbb{Q}_p$ dicht, ist auch $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q} \subseteq \mathbb{Z}_p$ dicht. Es ist sogar $\mathbb{Z}$ in $\mathbb{Z}_p$ dicht. Sei $x \in \mathbb{Z}_p$ und $\varepsilon > 0$. Dann gibt es $\frac{a}{b} \in \mathbb{Z}_{(p)}$ mit $\left|x - \frac{a}{b}\right| < \varepsilon$. Sei $\overline{b} \in \mathbb{Z}$ so, dass $\overline{b}\cdot b \equiv 1 \mod p^n$ für $n \in \mathbb{N}$ mit $p^{-n} < \frac{\varepsilon}{|a|_p}$. Dann $|x - \underbrace{a\overline{b}}_{\in\mathbb{Z}}|_p \leq \max\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - a\overline{b}\right|_p\}$.
Wir haben $|\frac{a}{b} - a\overline{b}|_p = |a|_p \cdot |\frac{1}{b} - \overline{b}| \leq$[32] $|a|_p \cdot |b|_p^{-1} \cdot |\frac{1}{b} - \overline{b}|_p = |a|_p \cdot |1 - b\overline{b}|_p \leq |a|_p \cdot p^{-n} < \varepsilon$
$\Longrightarrow |x - a\overline{b}|_p < \varepsilon$

[31] $A_{(p)} := \left\{x \in K \mid x = \frac{a}{b} \text{ mit } a \in A \text{ und } b \in A \setminus (p)\right\}$ nach Blatt 10 Aufgabe 3
[32] **TODO Sollte das nicht = sein? $|b|_p$ sollte ja 1 sein**

Für den Restklassenring der Körper $\mathbb{Q}, \mathbb{Q}_p$ gilt:

$$\mathbb{F}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \xrightarrow{\cong} \mathbb{Z}_p/p \cdot \mathbb{Z}_p$$

Die Surjektivität und damit Bijektivität/Isomorphie folgt aus der Tatsache, dass jede Nebenklasse $x + p\mathbb{Z}_p$ offen ist und somit Elemente aus $\mathbb{Z}_{(p)}$ enthält.**TODO Injektivität?**

Reihendarstellung(4.31): Jedes Element $x \in \mathbb{Q}_p$ lässt sich eindeutig schreiben als

$$x = \sum_{i=v_p(x)}^{\infty} a_i \cdot p^i, \, a_i \in \{0, \dots, p-1\}$$

Bsp: $-1 = (p-1) + (p-1) \cdot p + (p-1) \cdot + p^2 + \dots$ sieht man eintweder durch $\underbrace{(p-1) + \dots + (p-1)p^n}_{(p-1)(1+\dots+p^n)} = p^{n+1} - 1 \equiv -1 \mod p^{n+1}$ oder durch geometrische Reihe $\frac{-1}{p-1} = \sum_{i=0}^{\infty} p^i$.

$\mathbb{Q}_p$ enthält primitive $(p-1)$-ste Einheitswurzeln: Sei $\Phi_{p-1} \in \mathbb{Z}[x] \subset \mathbb{Z}_p[x]$ das $(p-1)$-te Kreisteilungspolynom. Da $p \nmid (p-1)$ und $\Phi_{p-1} | X^{p-1} - 1$ ist Φ_{p-1} separabel über $\mathbb{F}_p$. Weiter besitzt $\mathbb{F}_p$ eine primitive $(p-1)$-te Einheitswurzel. => Φ_{p-1} besitzt eine einfache Nullstelle über $\mathbb{F}_p$. Hensels Lemma: Φ_{p-1} hat eine Nullstelle in $\mathbb{Z}_p \subseteq \mathbb{Q}_p$.

Satz 4.35. *Sei $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$. Sei p prim. Die Kongruenz*

$$F(x_1, \dots, x_n) \equiv 0 \mod p^m$$

ist genau dann für begliebiges $m \in \mathbb{N}$ lösbar, wenn

$$F(x_1, \dots, x_n) = 0$$

in $\mathbb{Z}_p$ lösbar ist.

Beweis.

- $\Leftarrow$ Sei $(x_1, \dots, x_n) \in \mathbb{Z}_p^n$ eine Lösung. Betrachte Reihendarstellung $x_i = \sum_{\alpha=0}^{\infty} a_{i,\alpha} p^{\alpha}$. Dann ist $(\underbrace{\sum_{\alpha=0}^{m-1} a_{1,\alpha} p^{\alpha}}_{\in \mathbb{Z}}, \dots, \underbrace{\sum_{\alpha=0}^{m-1} a_{n,\alpha} p^{\alpha}}_{\in \mathbb{Z}})$ eine Lösung von F modulo p^m.

- $\Rightarrow$ Sei umgekehrt $(x_1^m, \dots, x_n^m) \in \mathbb{Z}^n$ eine Lösung modulo p^m. O.B.d.A.[33] sei $n = 1$, also $(x^m)_{m \in \mathbb{N}}$ Lösung von $F(x) \equiv 0 \mod p^m$. Wähle Teilfolge $(y_1^m)_m$ von $(x^m)_m$ und $y_1 \in \mathbb{Z}$ mit

$$y_1^m \equiv y_1 \mod p$$
$$F(y_1^m) \equiv 0 \mod p$$

  Eine solche Teilfolge muss existieren, da es nur p mögliche Reste für die x_i gibt und so mindestens einen Rest y_1 unendlich häufig volkommt und eine Teilfolge gebildet werden kann.

[33] Da Validität des O.B.d.A.zeigt sich erst im Laufe des Beweises.

Im nächsten Schritt wähle eine Teilfolge $(y_2^m)_m$ von $(y_1^m)_m$, die $\mod p^2$ konstant ist, d.h.

$$y_2^m \equiv y_2 \mod p^2$$
$$F(y_2^m) \equiv 0 \mod p^2$$

Dann konvergiert die Folge $y_1, y_2, \dots$ gegen eine Lösung von F in $\mathbb{Z}_p$.

□

5 Ringe und Moduln

VL vom 26.1.2024:

§5.1 Grundlagen der Modultheorie

Sei R ein Ring mit Eins (aber nicht zwingend kommutativ)

Definition 5.1. Ein *Linksmodul* über R ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Skalarmultiplikation

$$R \times M \to M, \quad (r,m) \mapsto r * m$$

mit den Eigenschaften

(i) $r \cdot (x+y) = r \cdot x + r \cdot y$

(ii) $(r+s) * x = r * x + s * x$

(iii) $(r \cdot s) * x = r * (s * x)$

(iv) $1_R * x = x$

für alle $r,s \in R$ und $x,y \in M$.
Analog ist ein *Rechtsmodul* definiert mit Skalarprodukt $M \times R \to M \quad (m,r) \mapsto m * r$

Bemerkung 5.2. Auf der R zugrundeliegenden abelschen Grupp erhalten wir eine neue Ringstruktur, indem wir die Multiplikation durch $r \odot s := s \cdot r$ ersetzten. Man nennt diese den entgegengesetzten Ring R^{Op}. Ist M bezüglich $M \times R \to M$ ein R-Rechtsmodul, dann ist M bezüglich $R^{Op} \times M \to M, r \odot m = m \cdot r$, ein R^{Op}-Linksmodul.

Wir betrachten in Zukunft Linksmoduln und nennen sie einfach Moduln.

Beispiel 5.3.

(1) $R = K$ Körper. Dann sind K-Moduln genau die K-Vektorräume

(2) M abelsche Gruppe

$$End(M) = \{f : M \to M \text{ Homomorphismus}\}$$

ist ein Ring bezüglich $(f+g)(x) = f(x)+g(x)$ und $(f \cdot g)(x) = f(g(x))$ mit der Skalarmultiplikation $End(M) \times M \to M \quad (f,m) \mapsto f(m)$ wird M ein $End(M)$-Modul.

(3) Abesche Gruppen sind genau die $\mathbb{Z}$-Moduln: Ist M eine abelsche Gruppe, dann ist M ein $\mathbb{Z}$-Modul vermöge

$$n \cdot x = \underbrace{x + \cdots + x}_{n\text{-fach}} \quad (-1) \cdot x = -x$$

Definition 5.4.

(a) Eine Abbildung $f : M \to N$ zwischen R-Moduln ist *R-Linear*, wenn für $x,y \in M$, $r \in R$ gilt

$$f(x+y) = f(x) + f(y) \quad f(r \cdot x) = r \cdot f(x)$$

$Hom_R(M,N) := \{R\text{-lineare Abbildung } M \to N\}$

(b) Isomorphismus

(c) Untermodul

Beispiel 5.5.

(a) Ist $f \in Hom_R(M,N)$, dann sind $\ker(f)$ und $f(M)$ Untermoduln.

(b) R ist ein Links- und Rechtsmodul bzüglich der Ringmultiplikation $R \times R \to R$. Dann (Links-) Ideale $\widehat{=}$ Untermodul (in Linksmodulstruktur). Für Rechts- analog.

Ilias (angeblich)

Definition 5.9. Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln. Das kartesische Produkt $\prod_{i\in I} M_i$ ist ein R-Modul bezüglich $(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I}$ und $r \cdot (x_i)_{i\in I} = (rx_i)_{i\in I}$. Wir sagen $\prod_{i\in I} M_i$ ist das *direkte Produkt der M_i*. Für jedes $i \in I$ ist die Projektion $pr_i : \prod_{j\in I} M_i \to M_i$ R-linear. Die Zuordnung $\phi \mapsto (pr_i \circ \phi)_{i\in I}$ definiert einen Isomorphismus abelscher Gruppen

$$Hom_R(M, \prod_{i\in I} M_i) \overset{\cong}{\to} \prod_{i\in I} Hom_R(M, M_i)$$

(Ist R kommutativ ist die Struktur wieder ein Modul)

Bemerkung. **TODO Timos remark**

Definition 5.10 (Direkte Summe von R-Modul)**.** Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln. Definiere $\bigoplus_{i\in I} M_i = \{(x_i)_{i\in I} \in \prod_{i\in I} M_i \mid x_i = 0 \text{ bis auf endlich viele } i\}$ die *direkte Summe der M_i* alse Untermodul von $\prod_{i\in I} M_i$. Für jedes $j \in I$ ist $\iota_j : M_j \to \oplus_{i\in I} M_i$, $\iota_j(x) = (0,\dots,0, \underbrace{x}_{\text{Position } j}, 0,\dots,0)$

eine injektive R-lineare Abbildung. Die Zuordnung $\phi \mapsto (\phi \circ \iota_i)_{i \in I}$ definiert einen Isomorphismus abelscher Gruppen

$$Hom_R\left(\bigoplus_{i\in I} M_i, M\right) \xrightarrow{\cong} \prod_{i\in I} Hom_R(M_i, M)$$

Die Umkehrabbildung ist

$$(f_i : M_i \to M)_{i\in I} \mapsto \begin{cases} \bigoplus_{i\in I} M_i \to M, \\ (x_i)_{i\in I} \mapsto \sum_{i\in I} f_i(x_i) \end{cases}$$

Gewöhnlich schreiben wir $(x_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ auch als $\sum_{i\in I} x_i$.
Notation: Ist $M_i = M$, dann schreiben wir $\bigoplus_{i\in I} M_i = M^{(I)}$ und $\prod_{i\in I} M_i = M^I$

Definition 5.11. Sei $S \subseteq M$ eine Teilmenge in einem R-Modul M. Dann heißt S

- *Erzeugendensystem*, wenn $M := \langle S\rangle_R = \{\sum_{s\in J} r_s \cdot s \mid J \subseteq S \text{ endlich}, r_s \in R\} = \bigcap\{N \mid N \subseteq M \text{ Untermodul mit } S \subseteq N\}$
- *R-linear unabhängig*, wenn für alle $s_1, \dots, s_m \in S$ und $r_1, \dots, r_m \in R$ die Implikation $\sum_{i=1}^m r_i \cdot s_i = 0 \Rightarrow r_1 = \dots = r_m = 0$ gilt.
- *Basis*, wenn s ein linear unabhängiges Erzeugendensystem ist
- M heißt
  - *endlich erzeugt*, wenn M ein endliches Erzeugendensystem besitzt
  - *frei*, wenn M eine Basis besitzt

Bemerkung 5.12.

a) Jeder VR hat eine Basis, ist also frei. Aber $\mathbb{Q}$, $\mathbb{Z}/n$ alse $\mathbb{Z}$-Modul ist nicht frei: Betrachte $q_1 = \frac{a_1}{b_1}, q_2 = \frac{a_2}{b_2} \in \mathbb{Q}$. Dann gilt $(b_1a_2) \cdot q_1 - (b_2a_1) \cdot q_2 = 0$ (nicht triviale linearkombination). Somit ist $S \subseteq \mathbb{Q}$ mit $|S| \geq 2$ nicht linear unabhängig. Weiter kann ein einziges Element $q = \frac{a}{b}$ nicht $\mathbb{Q}$ erzeugen als $\mathbb{Z}$-Modul, denn $\langle q\rangle_{\mathbb{Z}} = \mathbb{Z}_q = \mathbb{Z} \cdot \frac{a}{b} \subseteq \mathbb{Z} \cdot \frac{1}{b} \subset \mathbb{Q}$

b) Die Kardinalität einer Basis ist im Allgemeinen keine Invariante feier Moduln.

Lemma 5.13. *Ein R-Modul M ist frei genau dann, wenn er zu einem Modul $R^{(I)}$ für eine Menge I isomorph ist.*

Beweis.

$\Rightarrow$ Sei S eine Basis. Betrachte die Abbildung $R^{(S)} \xrightarrow{\cong} M$, $(r_s)_{s\in S} \mapsto \sum_{s\in S} r_s \cdot s$. Diese ist ein Isomorphismus.

$\Leftarrow$ $R^{(I)}$ ist frei bezüglich der Basis $\{e_i = \iota_i(1_R) \mid i \in I\}$

$\square$

01.02.2023

Definition 5.14. Ein Untermodul $N \subseteq M$ heißt *direkter Summand*, wenn es einen Untermodul $C \subseteq M$ gibt so, dass

(i) $C \cap N = \{0\}$

(ii) $C + N = M$

In diesem Fall gilt $M \cong C \oplus N$. Man schreibt dann $M = C \oplus N$.

Beispiel. $2\mathbb{Z} \subset \mathbb{Z}$ ist kein direkter Summand

Definition 5.15 (Exakte Folgen). Es seien M, M', M'' R-Moduln. Es seien $f : M' \to M, g : M \to M''$ R-lineare Abbildungen. Man sagt, dass die Folge

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

exakt ist, wenn $Bild(f) = \ker(g)$.

Eine Folge der Form

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

nennt man *kurz exakte Folge*, wenn sie exakt an jeder Stelle ist, d.h. f injektiv, g surjektiv und $Bild(f) = \ker(g)$.

Homomorphiesatz liefert[34], dass

$$M/f(M') \cong M''$$

.

Beispiel. $0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ kurz exakt.

Satz 5.16. *Für eine kurze exakte Folge* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *sind die folgeneden Aussagen äquivalent:*

(i) $f(M') \subseteq M$ *ist ein direkter Summand*

(ii) $\exists s \in Hom_R(M'', M) : g \circ s = id_{M''}$

(iii) $\exists t \in Hom_R(M, M') : t \circ f = id_{M'}$

Sind diese Bedingungen erfüllt, so sagt man, dass die Folge spaltet.

Beweis.

[34] Das sollte für alle $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ gelten. g muss surjektiv sein, damit $g(M) = M''$, aber f nicht injektiv, weil das nichts an $Bild(f) = \ker(g)$ ändert

(i)$\Rightarrow$ (ii) Angenommen $f(M') \oplus C = M$. Dann ist $g_{|C}$ ein Isomorphismus:

- $\ker(g_{|C}) = \ker(g) \cap C = f(M') \cap C = 0$
- $Bild(g_{|C}) = g(C) = g(f(M') \oplus C) = g(M) = g(M) = M''$

Definiere $s(x) = g_{|C}^{-1}(x) \in M$ für $x \in M''$. Dann ist $g \circ s = id_{M''}$.

(ii) $\Rightarrow$ (iii) Für $y \in M$ ist $y - (s \circ g)(y) \in Bild(f) = \ker(g)$, weil

$$g(y - (s \circ g)(y)) = g(y) - (\underbrace{g \circ s}_{=id_{M''}} \circ g)(y) = g(y) - g(y) = 0$$

. Definiere $t(y) = f^{-1}(y - s \circ g(y))$ wobei f als Abbildung aufs Bild batrachtet wird. Dann $t \circ f = id_{M'}$, wegen $t(f(x)) = f^{-1}(f(x) - s \circ \underbrace{g \circ f}_{=0}(x)) = x$.

(iii) $\Rightarrow$ (i) Setze $C := \ker(t)$ Dann ist $C \cap f(M') = \{0\}$: Sei $x \in C \cap f(M')$. Insbesonderer $x = f(y)$ für ein $y \in M'$. Dann $0 = t(x) = t(f(y)) = y \Longrightarrow x = f(y) = 0$.

Weiter ist $C + f(M') = M$. Sei $m \in M$. Betrachet $t(m - f \circ t(m)) = t(m) - \underbrace{t \circ f}_{=id_{M'}} \circ t(m) = t(m) - t(m) = 0$, also $m - \underbrace{f \circ t(m)}_{\in Bild(f)} \in C$

□

Definition 5.17.

a) Ein R-Modul P heißt *projektiv*, wenn jede kurze exakte Folge von R-Moduln der Form $0 \to M' \to M \to P \to 0$ spaltet.

b) Ein R-Modul I heißt *injektiv*, wenn jede kurze exakte Folge von R-Moduln der Form $0 \to I \to M \to M'' \to 0$ spaltet.

Bemerkung 5.18. Jede kurze exakte Folge von VR über einem Körper K spaltet, weil jeder Unter-VR ein Komplement besitzt. => Alle VR sind projektiv und injektiv.

§5.2 Bilineare Abbildungen und Tensorprodukte

In diesem Abschnitt ist R ein kommutativer Ring.

Definition 5.19. Seien L, M, N drei R-Moduln. Eine Abbildung $f : M \times N \to L$ heißt R-*bilinear* wenn gelten

1. $f(rx + sy, u) = rf(x,u) + sf(y,u)$
2. $f(x, ru + sv) = rf(x,u) + sf(x,v)$

für $x, y \in M$, $u, v \in N$, $r, s \in R$.

Definition 5.20. Ein *Tensorprodukt* zweier R-Moduln M und N ist ein Paar (T, β) bestehend aus einem R-Modul T und einer R-bilinearen Abbildung $\beta : M \times N \to T$ so, dass eine *universelle* Eigenschaft erfüllt ist:

Für jeden R -Modul L und jede R-bilneare Abbildung $f : M \times N \to L$ existiert ein eindeutiger R-Homomorphismus $\phi : T \to L$ mit $\phi \circ \beta = f$

$$\begin{tikzcd}
M \times N \arrow[r, "\beta"] \arrow[d, "f"'] & T \arrow[dl, dotted, bend left, "\exists!\phi"] \\
L &
\end{tikzcd}$$

Lemma 5.21. *Sind (T, β) und (T', β') zwei Tensorprodukte von $M \times N$, dann existiert ein eindeutiger Isomorphismus $\phi : T \to T'$ mit*

$$\begin{tikzcd}
T \arrow[rr, "\phi", "\cong"'] & & T' \\
& M \times N \arrow[ul, "\beta"] \arrow[ur, "\beta'"'] &
\end{tikzcd}$$

Beweis.

- $$\begin{tikzcd}
T \arrow[rr, dotted, "\exists!\phi"] & & T' \\
& M \times N \arrow[ul, "\beta"] \arrow[ur, "\beta'"'] &
\end{tikzcd}$$ universelle Eigenschaften von (T, β)

- $$\begin{tikzcd}
T & & T' \arrow[ll, dotted, "\exists!\psi"'] \\
& M \times N \arrow[ul, "\beta"] \arrow[ur, "\beta'"'] &
\end{tikzcd}$$ universelle Eigenschaft von (T', β')

- $$\begin{tikzcd}
T \arrow[r, "\phi"] \arrow[rr, bend left, "id_T"] & T' \arrow[r, "\psi"] & T \\
& M \times N \arrow[ul, "\beta"] \arrow[ur, "\beta"'] &
\end{tikzcd}$$ univeselle Eigenschaft: (T, β) -Eindeutigkeit $\Rightarrow \psi \circ \phi = id_T$

- $$\begin{tikzcd}
T' \arrow[r, "\psi"] \arrow[rr, bend left, "id_{T'}"] & T \arrow[r, "\phi"] & T' \\
& M \times N \arrow[ul, "\beta'"] \arrow[ur, "\beta'"'] &
\end{tikzcd}$$ univeselle Eigenschaft: (T', β') -Eindeutigkeit $\Rightarrow \phi \circ \psi = id_{T'}$

□

Satz 5.22 (Satz von der Existenz des Tensorprodukts)**.** *Für je zwei R-Moduln existiert ein Tensorprodukt.*

Beweis. Sei M,N zwei R-Moduln. Sei $I = M \times N$. Betrachte den freien R-Modul $F := R^{(I)} = \bigoplus_{(x,u)\in I} R$. Für $(x,u) \in I$ sei $i_{(x,u)} : R \to F$ die jeweilige Inklusion. Schreibe $[x,u] := i_{(x,u)}(1) \in F$. Die Menge $\{[x,u] \mid x \in M, u \in N\}$ ist eine Basis von F. Sei Z der Untermodul von F, der von allen Elementen der Form $[rx+sy,u] - r[x,u] - s[y,u]$ $[x,ru+sv] - r\cdot[x,u] - s\cdot[x,v]$ mit $r,s \in R$,$x,y \in M$, $u,v \in N$ erzeugt wird. Setze $T := F/Z$.

Die Abbildung $\beta : M \times N \to T, \beta(m,n) = [m,n] + Z$ ist bilinear nach Konstruktion.

β erfüllt die Universelle Eigenschaft: Betrachte **TODO Mehr Bilder** Definiere $\overline{\phi} : F \to L$ durch $\overline{\phi}([m,n]) = f(m,n)$. Z.z. $\overline{\phi}_{|Z} \equiv 0$. Dann induziert $\overline{\phi}$ einen Homomorphismus $\phi : T \to L$. $\overline{\phi}_{|Z}$ folgt sofort aus der Bilinearität von f. □

02.02.2024

Bemerkung 5.23 (Notation). Das Tensorprodukt der R-Moduln M und N notiert man $M \otimes_R N$ ($M \otimes N$, wenn R aus dem Kontext klar ist). ´Das Bild von $(m,n) \in M \times N$ unter der Strukturabbildung $\beta : M \times N \to M \otimes N$ notiert man als $m \otimes n \in M \otimes N$. Diese Elemente $m \otimes n$, $m \in M$, $n \in N$ nennt man auch Elementartensor; diese erzeugen $M \otimes_R N$. (siehe Beweis von 5.22). Beachte: Die Bilinearität von β übersetzt sich in folgende Gleichungen für Elementartensoren: $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$ $(r \cdot m) \otimes n = r \cdot (m \otimes n) = m \otimes (r \cdot n)$

Beispiel 5.24. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$

$$\begin{aligned} x \otimes y &= x \cdot n^{-1} \cdot n \otimes y \\ &= n \cdot (xn^{-1} \otimes y) \\ &= xn^{-1} \otimes n \cdot y \\ &= xn^{-1} \cdot 0 \\ &= 0 \in M \otimes N \end{aligned}$$

Lemma 5.25. *Für alle R-Moduln L,M,N gelten:*

(i) $R \otimes_R N \cong N$

(ii) $M \otimes_R N \cong N \otimes_R M$

(iii) $M \otimes_R (N \otimes_R L) \cong (M \otimes_R N) \otimes_R L$

(iv) $(\bigotimes_{i\in I} M_i) \otimes_R N \cong \bigotimes_{i\in I} (M_i \otimes_R N)$

Beweis.

(i) $R \times N \to N, (r,n) \mapsto r \cdot n$ R-bilinear. Somit induziert sie einen R-Homomorphismus $R \otimes_R N \to N, r \otimes n \mapsto r \cdot n$. Die Umkehrabbildung ist $N \to R \otimes_R N, n \mapsto 1 \cdot n$ R-linear.

(ii) Die Abbildung $M \times N \to N \otimes_R M, (m,n) \mapsto n \otimes m$ ist bilinear.Somit erhält man die induziert Abbildung $M \otimes_R N \to N \otimes_R M, m \otimes n \mapsto n \otimes m$. Ähnlich erhält man die Umkehrabbildung $N \otimes_R M \to M \otimes_R N, n \otimes m \mapsto m \otimes n$.

(iii) Sei $z \in L$. Die Abbildung $f_z : M \times N \to M \otimes_R (N \otimes_R L), (m,n) \mapsto m \otimes (n \otimes z)$ ist bilinear. Darau lässt sich $f'_z : M \otimes_R N \to M \otimes_R (N \otimes_R L), m \otimes n \mapsto m \otimes (n \otimes z)$ Die Abbildung $g : (M \otimes_R N) \times L \to M \otimes_R (N \otimes_R L), (m \otimes n, z) \mapsto f'_z(m \otimes n)$ ist bilinear. Daraus konstruiere $(M \otimes_R N) \otimes_R L \to M \otimes_R (N \otimes_R L), (m \otimes n) \otimes z \mapsto m \otimes (n \otimes z)$. Die Wohldefiniertheit der offensichtlichen Umkehrabbildung beweist man ähnlich.

(iv) Die R-Homomorphismen $j_i : M_i \otimes_R N \to (\bigoplus_{i \in I} M_i) \otimes_R N, m \otimes n \mapsto incl_i(m) \otimes n$ sind induziert durch die bilineare Abbildung $M_i \times N \to (\bigoplus_{i \in I} M_i) \otimes_R N, (m,n) \mapsto incl_i(m) \otimes n$. Die Familie $(j_i)_i$ induziert einen R-Homomorphismus $\bigoplus_{i \in I} M_i \otimes_R N \to (\bigoplus_{i \in I} M_i) \otimes_R N$. Die dazugehörige Umkehrhabbildung wird induziert durch die bilineare Abbildung $(\bigoplus_{i \in I} M_i) \times N \to \bigoplus_{i \in I} M_i \otimes_R N, (\sum_i m_i, n) \mapsto \sum_i m_i \otimes n$

□

Beispiel. $R^2 \otimes R^3 \overset{(iv)}{\cong} R \otimes_R R^3 \oplus R \otimes R^3 \overset{(iv)+(ii)}{\cong} R \otimes_R R \oplus \cdots \oplus R \otimes_R R \overset{(i)}{\cong} R \oplus \cdots \oplus R = R^6$

Bemerkung 5.26 (Tensorprodukt als Funktor). Seien $f : M \to M'$, $g : N \to N'$ zwei R-lineare Abbildungen. Dann gibt es genau eine R-lineare Abbildung

$$\begin{aligned} M \otimes_R N &\xrightarrow{f \otimes g} M' \otimes_R N', \\ m \otimes n &\longmapsto f(m) \otimes g(n) \end{aligned}$$

Kompatibel mit Komposition: $(f \circ \tilde{f}) \otimes (g \circ \tilde{g}) = (f \otimes g) \circ (\tilde{f} \otimes \tilde{g})$

Satz 5.27 (Tensorprodukt ist rechtsexakt)**.** *Es sei M ein R-Modul and*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$$

eine exakte Folge von R-Moduln. Dann ist auch die Folge

$$M \otimes_R N' \xrightarrow{id_M \otimes f} M \otimes_R N \xrightarrow{id_M \otimes g} M \otimes_R N'' \to 0$$

exakt.

Beweis. 1. $id_M \otimes g$ ist surjektiv: Jeder Elementartensor $x \otimes y \in M \otimes_R N''$ liegt in $Bild(id_M \otimes g)$. Denn $x \otimes y = x \otimes g(\tilde{y}) = (id_M \otimes g)(x \otimes \tilde{y})$ für ein g-Urbild $\tilde{y}$ von y. Da die Elementartensoren $M \otimes_R N''$ erzeugt, ist $Bild(id_M \otimes g) = M \otimes_R N''$.

2. $Bild(id_m \otimes f) = \ker(id_M \otimes g)$: "$\subseteq$folgt aus $(id_M \otimes g) \circ (id_M \otimes f)(\underbrace{x \otimes y}_{\in M \otimes_R N'}) = x \otimes g(f(y)) = x \otimes 0 = 0$

Zu zeigen "$\supseteq$: Setze $B := Bild(id_M \otimes f)$. Definiere eine bilineare Abbildung $\beta : M \times N'' \to (M \otimes N)/B$ wie folgt: Für $x \in M, u'' \in N''$ wähle $u \in N$ mit $g(u) = u''$ und definiere $\beta(x, u'') := x \otimes u + B$. Wohldefiniertheit? Sei $g(v) = u''$. Dann ist $u - v \in \ker(g) = Bild(f)$. Sei $u' \in N'$ mit $f(u') = u - v$. Nun folgt $x \otimes v + B = x \otimes v + \underbrace{x \otimes f(u')}_{\in B} + B =$

$x\otimes v+x\otimes(u-v)+B=x\otimes v+x\otimes u-x\otimes v+B=x\otimes u+B$. Das induziret Abbildung $s:M\otimes_R N''\to(M\otimes_R N)/B$ mit der Eigenschaft $m\otimes g(u)\mapsto m\otimes u+B$. Für $w\in M\otimes N$ gilt somit $s\circ(id_M\otimes g)(w)=w+B$. Somit gilt für $w\in\ker(id_M\otimes g)\subseteq M\otimes_R N$ $w+B=0\in(M\otimes_R N)/B$. => $w\in B=Bild(id_M\otimes f)$.

□

Bemerkung 5.28. Im Allgemeinen ist der Funktor $M\otimes_R -$ nicht exakt, d.h. $M\otimes\_$ erhält im Allgemeinen nicht kurze exakte Folgen. Bsp $0\to\mathbb{Z}\xrightarrow{\cdot 5}\mathbb{Z}\to\mathbb{Z}/5\mathbb{Z}\to 0$ $\mathbb{Z}/5/Z\otimes_{\mathbb{Z}}-$ liefert: **TODO bild**

Ein R-Modul M ist *flach*, wenn $M\otimes_R -$ exakt ist. Bsp: * $\mathbb{Q}$ ist ein flacher Z-Modul. * Jeder freie R-Modul flach * Jeder projektive R-Modul ist flach.

Definition 5.29. Eine R-Algebra ist ein Ring A (mit 1, nicht unbedingt kommutativ) mit einer R-Modulstruktur $R\times A\to A$ so, dass die Ringmultiplikation $A\times A\to A$ R-bilinear ist. [d.h. $\forall a,b\in A,\ r\in R: r(a._A b)=(ra)._A b=a._A(rb)$]

08.02.2024

$(ra)\cdot b=a\cdot(rb)=r(a\cdot b)$

Beispiel 5.30.

(i) $M_n(R)$ R-Algebra

(ii) $L|K$ Körpererweiterung. Dann ist L eine K-Algebra.

(iii) R nullteierfrei. Dann ist $Quot(R)$ eine R-Algebra.

(iv) Jeder Ring ist eine $\mathbb{Z}-Algebra$

(v) $R[X_1,\dots,X_n]$ ist R-Algebra

Bemerkung 5.31. Sei A eine R-Algebra. Definiere $i:R\to A, r\mapsto r1_A$. i ist ein Ringhomomorphismus. Weiter $i(R)\subseteq Z(A):=\{a\in A\mid\forall b\in A: ab=ba\}$ (SZentrum"). Denn:
$b\cdot i(r)=b\cdot(r1_A)=rb$
$i(r)\cdot b=(r1_A)\cdot b=r(1_A\cdot b)=rb$

Umgekehrt: Ist A ein Ring und $i:R\to Z(A)\subseteq A$ ein Ringhomomorphismus, dann wird A eine R-Algebra bezüglich der Skalamultiplikation: $ra:=i(r)\cdot a$.

Satz 5.32 (Skalarerweiterung)**.** *Es seien A eine R-Algebra und M ein R-Modul. Es gibt genau eine Skalarmultiplikation von A auf $A\otimes_R M$ mit $a(b\otimes x)=ab\otimes x$ für $a,b\in A$, $x\in M$, die $A\otimes_R M$ zu einem A-Modul macht. Man sagt: $A\otimes_R M$ entsteht durch* Skalarerweiterung. *Ist $f:M\to N$ R-linear, dann ist $id_A\otimes f:A\otimes_R M\to A\otimes_R N$ A-linear.*

Beweis. Beweisskizze: Sei $l_a:A\to A$ die Linksmultiplikation mit $a\in A$. Dann ist l_a R-linear: $rl_a(b)=r(a\cdot b)=a\cdot(rb)=l_a(rb)$. -> induziert die Skalarmultiplikation $l_a\otimes id_M:A\otimes_R M\to A\otimes_R M, b\otimes x\mapsto ab\otimes x$. Der Rest ist Nachrechnen □

Beispiel 5.33. Ist $f : V \to W$ eine $\mathbb{R}$ -lineare Abbildung zwischen endlichdimensionalen $\mathbb{R}$-VR, dann ist $id_{\mathbb{C}} \otimes f : \mathbb{C} \otimes_{\mathbb{R}} V \to \mathbb{C} \otimes_R W$ eine $\mathbb{C}$-lineare Abbidlung mit der gleichen Abbildungsmatix[35].

Satz 5.34. *Es seien M und N freie R-Moduln mit Basen $\{x_1, \dots, x_m\}$ für M und $\{y_1, \dots, y_n\}$ für N. Sei weiter A eine R-Algebra.*

(i) $M \otimes_R N$ ist ein freier R-Modul mit Basis $\{x_i \otimes y_j \mid i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\}$

(ii) $A \otimes_R M$ ist ein freier A-Modul mit Basis $\{1 \otimes x_1, \dots, 1 \otimes x_m\}$.

Beweis. i) Basen induzieren Isomorphismen $M \cong R^m$ und $N \cong R^n$. => $M \otimes_R N \cong R^m \otimes_R R^n \cong \underbrace{R^m \otimes_R R}_{\cong R^m} \oplus \cdots \oplus R^m \otimes_R R \cong \underbrace{R^m \oplus \cdots \oplus R^m}_{n \text{ mal}} \cong R^{n \cdot m}$ Inspektion des Isomorphismuses zeigt, dass $\{x_i \otimes y_i\}$ eine R-Basis ist.

ii) $A \otimes_R M \cong A \otimes_R R^m \cong A \otimes_R \oplus \cdots \oplus A \otimes_R R \cong A \oplus \cdots \oplus A \cong = A^m$ Standardbasis in A^m entspricht $\{1 \otimes x_i \mid i \in \{1, \dots, n\}\}$ under dem obigen Isomorphismus. □

Korollar 5.35. *Sei R kommutativer Ring, aber nicht der Nullring. Ist M ein freier R-Modul mit zwei Basen $\{x_1, \dots, x_m\}$ und $\{y_1, \dots, y_n\}$, dann ist $n = m$.*

Beweis. Lemma 2.27 liefert uns ein maximales Ideal $\mathfrak{m} \subset R$. Dann ist $R/\mathfrak{m} =: K$ ein Körper. K ist auch eine R-Algebra. Durch Skalarerweiterung erhält man den K-VR $K \otimes_R M$ mit den K-Basen $\{1 \otimes x_1, 1 \otimes x_2, \dots\}$ und $\{1 \otimes y_1, 1 \otimes y_2, \dots\}$ (Satz 5.34), Lineare Algebra => $n = m$. □

Satz 5.36. *Seien A, B R-Algebren. Auf $A \otimes_R B$ existiert genau eine Struktur als R-Algebra so, dass $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$ für alle $a_1, a_2 \in A$ und $b_1, b_2 \in B$.*

Beweisskizze. Sei $a \in A$ und $b \in B$. Die Abbildungen $r_a : A \to A, x \mapsto xa$ und $r_b : B \to B, x \mapsto xb$ sind R-linear. Wir erhalten somit eine R-lineare Abbildung $r_{(a,b)} := r_a \otimes r_b : A \otimes_R B \to A \otimes_R B, x \otimes y \mapsto xa \otimes yb$. Sei $z \in A \otimes_R B$. Die Abbildung $f_z : A \times B \to A \otimes_R B, f_z((a,b)) = r_{(a,b)}(z)$ ist R-linear. -> $f_z : A \otimes_R B \to A \otimes_R B$ -> Wohldefinierte Abbildung $A \otimes_R B \times A \otimes_R B \to A \otimes_R B, (z,w) \mapsto f_z(w)$, die auf Elementartensoren wie folgt aussieht: $(x \otimes y, a \otimes b) \mapsto xa \otimes yb$. Es verbleibt die Ringaxiome nachzuweisen! □

Bemerkung 5.37. In der obigen Situation sind $A \to A \otimes_R B, a \mapsto a \otimes 1$ $A \to A \otimes_R B, b \mapsto 1 \otimes b$Homomorphismus von R-Algebren.

Satz 5.38. *Sei A, B zwei R-Algebren, so hat $A \otimes_R B$ folgende univeselle Eigenschaft: Für jede weitere R-Algebra C und Homomorphismen $f : A \to C$, $g : B \to C$ mit der Eigenschaft*

[35] Wenn w und V die Basen $\{v_1 \dots,\}$ und $\{w_1, \dots\}$, dann wäre $\{1 \otimes v_1, 1 \otimes v_2, \dots\}$ und $\{1 \otimes w_1, \dots\}$ Basen zu $\mathbb{C} \otimes_R V$ und $\mathbb{C} \otimes_R W$.

$\forall a \in A, b \in B : f(a) \cdot g(b) = g(b) \cdot f(a)$ *existiert ein eindeutiger Homomorphismus von R-Algebren $\phi : A \otimes_R B \to C$ mit $\phi(a \otimes b) = f(a) \cdot g(b)$*

$$\begin{tikzcd} A \arrow[d] \arrow[dr, "f"] & \\ A \otimes_R B \arrow[r, dashed, "\exists! \phi"] & C \\ B \arrow[u] \arrow[ur, "g"'] & \end{tikzcd}$$

mit $f(a) \cdot g(b) = g(b) \cdot f(a)$

$$\phi(a \otimes b) = \phi(a \otimes 1 \cdot 1 \otimes b) = \phi(a \otimes 1) \cdot \phi(1 \otimes b) = f(a) \cdot g(b)$$

Beweis. Die Abbildung $A \times B \to C, (a,b) \mapsto f(a) \cdot g(b)$ ist R-bilinear. Somit erhält man $\phi : A \otimes_R B \to C$ mit $\phi(a \otimes b) = f(a) \cdot g(b)$ R-linear.

Beh: ϕ ist Ringhomomorphismus: $\phi(a_1 \otimes b_1 \cdot a_2 \otimes b_2) = \phi(a_1 a_2 \otimes b_1 b_2) = f(a_1 a_2) \cdot g(b_1 b_2)$ $\phi(a_1 \otimes b_1) \cdot \phi(a_2 \otimes b_2) = f(a_1) \cdot g(b_1) \cdot f(a_2) \cdot g(b_2) = f(a_1) f(a_2) g(b_1) g(b_2) = f(a_1 a_2) \cdot g(b_1 b_2)$ f, g Ringhomomorphismen. □

Beispiel 5.39. Sei A eine R-Algebra mit Skalarabbildung $i : R \to Z(A) \subseteq A, r \mapsto r1_A$. Beh: $A \otimes_R M_n(R) \cong M_n(A)$ als R-Algebren.

Betrachte $f : A \in M_n(A), a \mapsto (Dialgonalmatrixmitaaufderdiag), g : M_n(R) \to M_n(A), (r_{ij} \mapsto (i(r_{ij})) \in M_n(Z(A)) \subseteq M(A)$. dann gilt $f(a)g((r_{ij})) = g((r_{ij}))f(a)$. Nach der universellen Eigenschaft existiert $A \otimes_R M_n(R) \to M_n(A), a \otimes (r_{ij}) \mapsto (diag - matixmitaindiag) \cdot (r_1)$ Homomorphismus. Warum ϕ Iso? $A \otimes_R \underbrace{M_n(R)}_{=R^{n^2}} \cong A^{n^2}$ und ϕ überführt die SStandardbasen".

$M_n(A) \cong A^{n^2}$

09.02.2024

§5.3 Neothersche Moduln und Ring

[R möglicherweise nicht kommutativer Ring]

Beispiel 5.40. $R = \mathbb{C}[X_1, X_2, \dots]$ Polynomring in abzählbar unendlich vielen Variablen. $M = R$ R-Modul ist endlich erzeugt: $M = \langle 1_R \langle$. Sei $I = \langle X_1, X_2, \dots \rangle \subseteq M$ der von allen Varialben erzeugte Untermodul. dann ist I nicht endlich erzeugt.

Seien $f_1, \dots, f_m \in I$. Sei X_n eine Variable, die nicht in den Polynomen $f_1, \dots, f_m$ vorkommt. Dann $x_n \notin \langle f_1, \dots, f_m \rangle = \{\sum_{i=1}^m g_i f_i \mid g_1, \dots, g_m \in R\}$. Somit sind Untermoduln von endlich erzeugten R-Moduln i.A. nicht endlich erzeugt.

Definition 5.41. Ein R-Modul M heißt *noethersch*, wenn jeder Untermodul von M endlich erzeugt ist.

Satz 5.42. *Sei M ein R-Modul. Dann sind folgende Aussagen äquivalent:*

(i) M ist noethersch

(ii) Ist $M_1 \subseteq M_2 \subseteq \dots$ eine aufsteigende Kette von Untermoduln von M, dann gibt es ein $n_0 \in \mathbb{N}$ mit $M_{n_0} = M_{n_0+1} = M_{n_0+1} = \dots$.

(iii) Jede nicht leere Menge von Untermoduln von M besitzt ein maximales Element[36].

Beweis.

(i) $\Rightarrow$ (ii) Sei $M_1 \subseteq M_2 \subseteq \dots$ eine aufsteigende Kette und $N := \bigcup_{i=1}^{\infty} M_i$. M noethersch => N endlich erzeugt, d.h. $N = \langle m_{i_1}, \dots, m_{i_n} \rangle$ mit $m_{i_k} \in M_{i_k}$ Setze $n_0 = \max\{i_1, i_n\}$. Dann ist $N = M_{n_0}$

(ii) $\Rightarrow$ (iii) Durch Wiederspruch:
Sei $\mathscr{X}$ eine nicht leere Menge von Untermoduln, die kein maximales Element hat. Wähle $M_1 \in \mathscr{X}$. M_1 nicht maximal =>[37] es gibt $M_2 \in \mathscr{X}$ mit $M_1 \subset M_2$. M_2 nicht maximal => es gibt $M_3 \in \mathscr{X}$ mit $M_2 \subset M_3$... Wir erhalten induktiv eine strikt aufsteigende Kette von Untermoduln $M_1 \subset M_2 \subset M_3 \subset \dots$ ↯

(iii) $\Rightarrow$ (i) Sei $N \subset M$ ein Untermodul. Betrachte $\mathscr{X} = \{N' \subseteq N \mid N' \text{ endlich erzeugt}\} \neq \emptyset$, wegen $\{0\} \in \mathscr{X}$. Sei $N_0 \in \mathscr{X}$ ein maximales Element. Beh. $N_0 = N$. Angenommen $x \in N \setminus N_0$. Dann $\langle N_0 \cup \{x\} \rangle \in \mathscr{X}$ im Widerspruch zur Maximalität.

□

Lemma 5.43. *Es sei $0 \to M' \to M \xrightarrow{p} M'' \to 0$ eine kurze exalkte Folge von R-Moduln. Dann ist M genau dann noethersch, wenn M' und M'' noethersch sind.*

Beweis.

$\Rightarrow$ Sei M noethersch. Dann ist jeder Untermodul von M' isomorph zu einen Untermodul von M und somit endlich erzeugt. Also ist M' noethersch.

Sei $N \subseteq M''$ ein Untermodul. Dann ist $p^{-1}(N) \subseteq M$ endlich erzeugt. Somit ist $p(p^{-1}(N)) = N$ auch endlich erzeugt. Also ist M'' noethersch.

$\Leftarrow$ Sei $W \subseteq M$ ein Untermodul. Dann ist

$$0 \to \underbrace{j^{-1}(w)}_{\subseteq M'} \xrightarrow{j} W \xrightarrow{p} \underbrace{p(W)}_{\subseteq M''} \to 0$$

exakt und $j^{-1}(W)$ und $p(W)$ sind endlich erzeugt.

Die Aussage folgt aus der folgenden Implikation: $0 \to M_1 \xrightarrow{j} M_2 \xrightarrow{p} M_3 \to 0$ kurze exakte Folge und M_1, M_3 endlich erzeugt => M_2 endlich erzeugt.

[36]Eine Menge N ist maximal in $\mathscr{X}$, wenn für jedes Element $N' \in \mathscr{X}$ gilt $N' \supseteq N \Rightarrow N = N'$

[37]Gäbe es keine echte Obermenge gäbe, wäre es maximal. Wenne es eine gibt, dann ist sie nach Definition von Maximal ungleich.

Seien $M_1 = \langle x_1, \dots, x_n \rangle$ und $M_3 = \langle y_1, \dots, y_m \rangle$. Dann ist $M_2 = \langle \tilde{y}_1, \dots, \tilde{y}_m, j(x_1), \dots, j(x_n) \rangle$ für $\tilde{y}_i \in p^{-1}(\{y_i\})$

Sei $z \in M_z$. Dann gibt es $r_1, \dots, r_m \in R$ mit $p(z) = r_1 \cdot y_1 + \cdots + r_m \cdot y_m$. Somit ist $z - (r_1\tilde{y}_1 + \cdots + r_m\tilde{y}_m) \in \ker(p) = Bild(j)$. => es gibt $s_1, \dots, s_n \in R$ mit $z - (r_1\tilde{y}_1 + \cdots + r_m \cdot \tilde{y}_m) = s_1 j(x_1) + \cdots + s_n j(x_n)$.

□

Korollar 5.44.

(i) Jeder Untermodul und jeder Faktormodul eines noethersch Moduls ist noethersch.

(ii) Jede endliche direkte Summe von noetherschen Moduln ist noethersch.

Beweis.

(i) direkte Konsequenz von 5.43

(ii) Es genügt zu zeigen, dass $M \oplus N$ noethersch ist, falls M, N noethersch sind. Folgt aus 5.43 und der kurzen exakten Sequenz $0 \to M \to M \oplus N \to N \to 0$

□

Definition 5.45. Ein Ring heißt *linksnoethersch*, wenn er als Linksmodul über sich selbst noethersch ist.

Analog definiert man *rechtsnoethersch*. Ein Ring heißt *noethersch*, wenn er links- und rechtsnoethersch ist.

Beispiel. für noethersche Ringe:

- $R = K$ Körper
- Hauptidealringe (folgt aus dem Sturktursatz für Hauptidealringe)
- $R = M_n(K)$, K Körper. Jedes (Links-) Ideal in R ist ein K-Untervektorraum von $M_n(K) = K^{n^2}$, somit endlich erzeugt als K-VR. Somit erst recht endlich erzeugt als R-Ideal

Bsp 5.40: $\mathbb{C}[X_1, X_2, \dots]$ nicht noethersch.

Lemma 5.46. *Jeder endlich erzeugte Modul über einem linksnoetherschen Ring ist noethersch*

Beweis. 5.44 (ii) => R^n ist noethersch für $n \in \mathbb{N}$. Sei $M = \langle x_1, \dots, x_n \rangle$ ein endlich erzeugter Modul. Dann ist $R^n - >> M, e_i \mapsto x_i$ ein Epimorphismus. 5.44(i) => M noethersch. □

Lemma 5.47. *Sei M ein noetherscher R-Modul. Falls $M \cong M \oplus N$ für einen R-Modul N, so gilt $N = 0$.*

Satz 5.48. *Sei R ein linksnoetherscher Ring, aber nicht der Nullring. Sei M ein freier R-Modul mit Basen $\{x_1,\ldots,x_n\}$ und $\{y_1,\ldots,y_m\}$. Dann gilt $n=m$.*

Beweis. Ang. $m \leq n$. Dann gilt $R^m \cong M \cong R^n = R^m \oplus R^{n-m}$. Weiter ist R^m noethersch, weil R linksnoethersch ist. Lemma 5.47 =d $R^{n-m} = 0$ = R nicht Nullring => n-m = 0 □