Albert-Ludwigs-Universität Freiburg im Breisgau
Fakultät für Mathematik und Physik
Mathematisches Institut
Abteilung für mathematische Logik

Unbeschränkte PAC-Körper sind nicht einfach

Diplomarbeit
vorgelegt von
Nina Frohn

bei Prof. Dr. Martin Ziegler

August 2003

Inhaltsverzeichnis

Einführung

Geschichtliches

Ein Ziel der Modelltheorie ist es, Zusammenhänge zwischen den Eigenschaften einer meist vollständigen erststufigen Theorie und den Eigenschaften der Modelle bzw. der Modellklasse der Theorie zu finden:
Zu einer gegebenen Struktur sind die Eigenschaften ihrer erststufigen Theorie von Interesse, da diese Informationen über die Struktur liefern können (zum Beispiel ist der Beweis des Hilbertschen Nullstellensatzes einfacher als der klassische algebraische Beweis, wenn man benutzt, daß die Theorie algebraisch abgeschlossener Körper Quantoren eliminiert). Weiter möchte man wissen, wie sich Eigenschaften von Theorien auf Seite der Modelle auswirken (ein Beispiel: Ist in einer Theorie T jede Formel äquivalent zu einer Allformel, so folgt für zwei Modelle $\mathcal{A}, \mathcal{B} \models T$ aus $\mathcal{A} \subseteq \mathcal{B}$ schon $\mathcal{A} \prec \mathcal{B}$). Schließlich möchte man alle Modelle klassifizieren, deren Theorien bestimmte Eigenschaften besitzen (zum Beispiel bemüht man sich, alle Körper mit stabiler Theorie zu bestimmen).

In dieser Arbeit werden wir uns mit einfachen Theorien beschäftigen. Dieser Begriff entstand in Folge des Studiums stabiler Theorien. Ein paar Worte zur Geschichte einfacher und stabiler Theorien:
M. Morley arbeitete in [Mo, 1965] bereits mit ω-stabilen Theorien, jedoch ohne diesen Begriff zu benutzen. In [R, 1964] definierte F. Rowbottom κ-stabile Theorien für beliebige Kardinalzahlen κ. Ende der 60er in den 70er Jahren beschäftigt sich unter anderem S. Shelah mit stabilen Theorien; von ihm stammt mit [Sh1] das wohl umfassendste Werk über stabile Theorien. Für diese stand damit ein starker Apparat zur Analyse von Modellen zur Verfügung.
Allerdings sind viele interessante Strukturen nicht stabil, obwohl sie eine „schöne“ Modelltheorie zulassen.

S. Shelah führte 1980 in [Sh2] als Verallgemeinerung von stabilen Theorien den Begriff der einfachen Theorie ein. Doch erst fast 20 Jahre später rückte das Studium einfacher Theorien in den Mittelpunkt des allgemeinen Interesses: Ausgehend von der Arbeit [K1], in der die Symmetrie des Forkens in einfachen Theorien bewiesen wird, entwickelten B. Kim und A. Pillay die grundlegende Theorie einfacher Theorien; siehe unter anderem [K2, KP1, KP2]. Das Studium einfacher Theorien ist ein aktuelles Forschungsgebiet; viele der Ergebnisse für stabile Theorien wurden inzwischen auf einfache Theorien übertragen.
Ein klassisches Beispiel für eine einfache, nicht-stabile Struktur ist der Zufallsgraph. Es stellte sich heraus, daß viele bereits früher betrachtete algebraische Strukturen einfach sind, wie zum Beispiel pseudo-endliche Körper und algebraisch abgeschlossene Körper mit einem generischen Automorphismus. Ein weiteres Beispiel sind be-

schränkte pseudo-algebraisch abgeschlossene Körper[1]:

Ein Körper K heißt beschränkt, wenn er für jedes $n \in \mathbb{N}$ nur endlich viele Galoiserweiterungen von Grad n besitzt. Er heißt pseudo-algebraisch abgeschlossen (oder kurz ein PAC-Körper), wenn jede über K definierte, absolut irreduzible Varietät einen K-rationalen Punkt besitzt.
Die Modelltheorie von PAC-Körpern wurde in den siebziger und achtziger Jahren intensiv studiert. Ausgangspunkt hierfür war die Arbeit [Ax] von J. Ax über endliche und pseudo-endliche Körper; das weitere Studium von PAC-Körpern wurde besonders durch die Arbeiten [JK], [Ja], [CDM], [E1] und [E2] vorangebracht. Ein paar Daten über die Modelltheorie von Körpern, insbesondere von PAC-Körpern:

Im Jahre 1979 bewies A. Macintyre in [Mc], daß ω-stabile Körper schon algebraisch abgeschlossen sind. G. Cherlin und S. Shelah verallgemeinerten dies 1980 in [CS]: Auch superstabile Körper sind algebraisch abgeschlossen. Beispiele für stabile, nicht superstabile Körper sind separabel abgeschlossene Körper (vergleiche [W],1979).
J. L. Duret zeigte 1980 in [Du], daß stabile PAC-Körper separabel abgeschlossen sind. Anfang der neunziger Jahre bewies Hrushovski in [Hr], daß perfekte beschränkte PAC-Körper supereinfach sind, und damit insbesondere einfach. A. Pillay und Z. Chatzidakis erweiterten dieses Ergebnis in [ChP] auf beliebige beschränkte PAC-Körper: Beschränkte PAC-Körper sind einfach. Schließlich hat Z. Chatzidakis in [Ch1] gezeigt, daß einfache PAC-Körper beschränkt sind; die vorliegende Arbeit ist eine Ausarbeitung dieses Ergebnisses.

Es wird vermutet, daß alle stabilen Körper schon separabel abgeschlossen sind. Z. Chatzidakis bemerkt in [Ch1], daß aus [Poi2, Theorem 5.10] folgt, daß stabile Körper entweder separabel abgeschlossen oder unbeschränkt sind. Würde es also gelingen, die vorliegende Arbeit auf beliebige beschränkte, aber nicht notwendigerweise pseudo-algebraisch abgeschlossene Körper zu verallgemeinern, so wäre die Vermutung bewiesen.

Aufbau der Arbeit

Grundlage dieser Arbeit ist der Artikel [Ch1] von Z. Chatzidakis. Ziel ist der Beweis des folgenden Theorems:

Theorem 5.9.
Es sei F ein unbeschränkter PAC-Körper. Dann ist die Theorie von F nicht einfach.

In den ersten drei Kapiteln wird der für den Beweis von Theorem 5.9 notwendige algebraische und modelltheoretische Hintergrund entwickelt. Hauptsächlich werden dabei allgemein bekannte Ergebnisse zitiert; ergänzend sind einige später nützliche

[1] Eigentlich handelt es sich um pseudo-(algebraisch abgeschlossene) Körper, oder besser noch um algebraisch pseudo-abgeschlossene Körper.

Folgerungen aus diesen Ergebnissen enthalten.

- In Kapitel 1 werden die algebraischen Grundlagen für diese Arbeit bereitgestellt; diese sind vor allem unendliche Galoistheorie, Grundlagen über separable (reguläre, primäre) Körpererweiterungen, Bewertungstheorie und ein paar Ergebnisse aus der algebraischen Geometrie.
- Kapitel 2 enthält eine Einführung in die benötigte Modelltheorie. In dieser Arbeit benötigen wir vor allem einige Ergebnisse über erststufige Formulierbarkeit in der Sprache L_{Kp} der Körper und ein Basiswissen über einfache Theorien.
- In Kapitel 3 werden kurz die für uns wichtigen Ergebnisse über pseudo-algebraisch abgeschlossene Körper zusammengefaßt.

Kapitel 4 beschäftigt sich mit einem rein algebraischen Problem, der regulären Realisierung[2] von großen direkten Produkten der alternierenden Gruppe:

- In Abschnitt 4.1 wird gezeigt, daß sich über Körpern der Charakteristik ungleich 2 die alternierende Gruppe A_n für beliebig große natürliche Zahlen n regulär realisieren läßt. Diesen Teil der Arbeit verdanke ich Jochen Koenigsmann, der die entscheidenden Ideen für den Beweis lieferte.
- Abschnitt 4.2 orientiert sich wieder an [Ch1]: Es wird gezeigt, daß es in PAC-Körpern möglich ist, große direkte Produkte der alternierenden Gruppe regulär zu realisieren.

  Ist die Charakteristik des Grundkörpers gleich 2, so benutzen wir hierzu [Pop, Theorem A] von F. Pop über die reguläre Realisierung von endlichen Gruppen in sogenannten „large fields", zu denen insbesondere PAC-Körper gehören. Für alle anderen Charakteristiken gelingt es uns mit Hilfe von Abschnitt 4.1, beliebig große $n \in \mathbb{N}$ zu finden, für die die reguläre Realisierung von großen direkten Produkten der A_n auch ohne [Pop, Theorem A] möglich ist.

Schließlich enthält Kapitel 5 das Kernstück dieser Arbeit: den Beweis, daß unbeschränkte PAC-Körper nicht einfach sind.

- In Abschnitt 5.1 beweisen wir ein Kriterium dafür, daß eine Theorie nicht einfach ist. Wir werden dieses Kriterium im Beweis von 5.9 benutzen.
- In Abschnitt 5.2 zeigen wir als einfachen Spezialfall, daß ein PAC-Körper der Charakteristik ungleich 2 mit unendlich vielen quadratischen Erweiterungen nicht einfach ist.
- Schließlich enthält Abschnitt 5.3 den Beweis von Theorem 5.9. Wir starten mit einem unbeschränkten PAC-Körper F. Nun konstruieren wir eine geeignete elementare Oberstruktur $K \succ F$, die $\aleph_1$-viele Galoiserweiterungen $L_i \supset K$ besitzt,

[2] Üblicherweise heißt eine Gruppe G regulär realisierbar über F, wenn es ein $n \in \mathbb{N}$ und einen rationalen Funktionenkörper $K = F(t_1, \ldots, t_n)$ vom Transzendenzgrad n über F gibt, so daß sich G so als Galoisgruppe über K realisieren läßt, daß die entstehende Erweiterung von F regulär ist. Ich meine in dieser Arbeit mit regulärer Realisierbarkeit immer den Spezialfall der regulären Realisierbarkeit über einem Funktionenkörper in einer Variablen.

und wählen ein über K transzendentes Element a. Wir beweisen die Existenz einer elementaren Oberstruktur $K^* \ni a$ von K mit der Eigenschaft, daß sich die Erweiterung $L_iK^* \supset K^*$ sowohl mit Parametern (d_i, a) mit $d_i \in F$, als auch mit Parametern $c_i \in K$ definieren läßt. Man kann diese Konstruktion so durchführen, daß zu jeder abzählbaren Menge B ein $i < \aleph_1$ mit $c_i \notin \mathrm{acl}(FB)$ existiert. Dann ist $\mathrm{tp}(a/K)$ eine forkende Fortsetzung von $\mathrm{tp}(a/FB)$.

Zu guter Letzt enthält diese Arbeit noch einen Anhang, in dem der modelltheoretische algebraische Abschluß von PAC-Körpern bestimmt wird. Dieser Teil der Arbeit ist [ChP] entnommen.

Abweichungen des Beweises von der ihm zugrundeliegenden Arbeit [Ch1] von Z. Chatzidakis

Wie bereits erwähnt, ist diese Arbeit eine Ausarbeitung des ersten Teils des Artikels [Ch1], in dem gezeigt wird, daß einfache PAC-Körper beschränkt sind. Es gibt jedoch zwei Stellen, an denen ich vom Originalbeweis abweiche:

1) [Ch1] benutzt zur regulären Realisierung der alternierenden Gruppe [Pop, Theorem A]; dieser Satz sagt allgemeiner etwas über die reguläre Realisierung beliebiger endlicher Gruppen über „large fields“ aus, also insbesondere über PAC-Körpern. In Abschnitt 4.1 zeigen wir ohne [Pop, Theorem A] zu benutzen, daß sich die A_n für Charakteristiken ungleich 2 über jedem beliebigen Körper realisieren läßt. Dies führt dazu, daß wir in einem wichtigen Teil des Beweises von 5.9 für Charakteristiken ungleich 2 nicht benutzen, daß wir in einem PAC-Körper arbeiten.
2) Der erste Teil des Beweises von 5.9 verläuft ähnlich wie in [Ch1]: Ausgehend von einem unbeschränkten PAC-Körper F konstruieren wir eine elementare Oberstruktur $K \succ F$ und für $i < \aleph_1$ Galoiserweiterungen $L_i \supset K$, so daß für jedes über K transzendente Element a gilt: Es existiert ein $K^* \succ K$, so daß für $i < \aleph_1$ eine Galoiserweiterung $M_i \supset F(a)$ existiert mit $K^*L_i = K^*M_i$. Danach unterscheidet sich der hier ausgeführte Beweis jedoch von der Vorlage:
   Ich zeige in dieser Arbeit auf elementare Weise, daß $\mathrm{tp}(a/K)$ über jeder abzählbaren Menge teilt; hieraus folgt, daß $\mathrm{Th}(F)$ nicht einfach ist. Dabei gebe ich nicht nur an, welcher Typ den lokalen Charakter des Teilens verletzt; dies tut auch Z. Chatzidakis in ihrem Beweis. Es wird auch klar, welche Formel aus dem Typ über jeder kleinen Menge teilt. Daher ist auch intuitiv nachvollziehbar, warum diese Theorie nicht einfach ist.
   Z. Chatzidakis dagegen zeigt zunächst ein technisches Theorem, nämlich [Ch1, Theorem 3.5], das bestimmte Eigenschaften nichtforkender Erweiterungen in beliebigen[3] Körpern beschreibt. Zusammen mit der genauen Bestimmung des algebrai-

[3] Z. Chatzidakis benutzt dabei, daß in beliebigen Körpern aus $B \underset{A}{\smile} C$ auch $\mathrm{acl}(B) \underset{A}{\smile} \mathrm{acl}(C)$ für die modelltheoretischen algebraischen Abschlüsse $\mathrm{acl}(B)$, $\mathrm{acl}(C)$ folgt. Mir scheint dies nur für einfache

schen Abschlusses in PAC-Körpern ermöglicht ihr dieses Theorem, die Einfachheit unbeschränkter PAC-Körper zu widerlegen.
Theorem [Ch1, Theorem 3.5] ist für die Analyse von ω-freien PAC-Körpern interessant, da die dort beschriebenen Eigenschaften von Erweiterungen in ω-freien PAC-Körpern die Forking-Relation charakterisieren (siehe [Ch2, Theorem 3.3, Korollar 3.4]). Um zu beweisen, daß einfache PAC-Körper beschränkt sind, erscheint mir dies jedoch unnötig kompliziert. Außerdem erschwert es der sehr technische Widerspruchsbeweis aus [Ch1], eine intuitive Vorstellung davon zu bekommen, warum unbeschränkte PAC-Körper nicht einfach sind.

Die im Anhang befindliche Analyse des algebraischen Abschlusses in PAC-Körpern ist für meine Version des Ergebnisses nicht erforderlich, stellt für sich genommen jedoch ein interessantes Ergebnis dar. Ich habe sie daher vom Hauptteil der Arbeit getrennt.

Mein Dank gilt:

In fachlicher Hinsicht:

- Markus Junker, der die Idee für das Thema dieser Arbeit hatte, und der die nie versiegende Flut meiner Fragen mit engelsgleicher Geduld beantwortet hat.
- Professor Martin Ziegler für die Betreuung dieser Arbeit; er hat viele im Verlauf der Arbeit auftretende Probleme gelöst.
- Jochen Koenigsmann, der die wesentlichen Ideen für Abschnitt 4.1 hatte, und der sich immer Zeit für meine Fragen genommen hat.
- Jan Christoph Schlage-Puchta; die Gespräche mit ihm haben mir wichtige Anregungen gegeben.

Und ansonsten:

- meinen Eltern, die mir jede nur denkbare Unterstützung haben zukommen lassen.
- der alltäglichen Mensagruppe für regelmäßige Zerstreuung und Aufmunterung.
- Andreas Dedner für viele Rezeptevorschläge, für gemeinsames Probe-Kochen und Probe-Essen.

Theorien offensichtlich zu sein. Für den Beweis, daß ein einfacher PAC-Körper beschränkt ist, wäre diese Einschränkung aber unwesentlich.

1 Etwas Algebra und algebraische Geometrie

1.1 Algebra

1.1.1 Bezeichnungen und Konventionen

Fortan seien $K, L, M...$ Körper der Charakteristik p (p prim oder $p = 0$). Wir arbeiten in einem Universalbereich Ω; dies ist ein algebraisch abgeschlossener Oberkörper von so großem Transzendenzgrad über dem jeweiligen Grundkörper, daß sich alle betrachteten Erweiterungen des Grundkörpers in ihn einbetten lassen. K^{a} sei der algebraische und K^{s} der separable Abschluß des Körpers K; für $q \in \mathbb{Z} \setminus \{0\}$ sei $K^q := \{x^q \mid x \in K\}$. Für Körper K der Charakteristik $p \neq 0$ sei $K^{1/p^\infty} := \bigcup_{n \in \mathbb{N}} K^{1/p^n}$ die perfekte Hülle von K, für $p = 0$ sei $K^{1/p^\infty} := K$. Für einen Ring R sei $R^\times$ die Menge der Einheiten in R; insbesondere ist also $K^\times = K \setminus \{0\}$.
Ist $L \supseteq K$ eine Galoiserweiterung, so bezeichne ich die Galoisgruppe von L über K mit $\mathrm{Gal}(L/K)$, die absolute Galoisgruppe von K, also $\mathrm{Gal}(K^{\mathrm{s}}/K)$, mit $\mathcal{G}(K)$. Ist H eine Untergruppe von $\mathrm{Gal}(L/K)$, so sei $\mathrm{Fix}(H) \subseteq L$ der Fixkörper von H.
Ist $(K_i \supseteq K)_{i \in I}$ eine Familie von Körpererweiterungen, so bezeichne $\prod_{i \in I} K_i$ das Kompositum der Körper, für eine Familie $(G_i)_{i \in I}$ von Gruppen sei $\prod_{i \in I} G_i$ das direkte Produkt der Gruppen. Dabei ist je nach Kontext das innere oder das äußere Produkt gemeint. Äußere direkte Produkte, die sich nur in der Reihenfolge der Faktoren unterscheiden, werde ich ohne Einschränkung als gleich betrachten.
Ist a algebraisch über K, so bezeichne $\mathrm{Irr}(a, K)$ das Minimalpolynom von a über K.
Ist R ein Ring und R_0 eine Teilmenge von R, so bezeichne $(R_0)_R$ oder kurz (R_0) das von R_0 in R erzeugte Ideal. Ist G eine Gruppe und U eine Teilmenge von G, so sei $\langle U \rangle_G$ bzw. $\langle U \rangle$ die von U in G erzeugte Untergruppe.

1.1.2 Unendliche Galoistheorie

Ich möchte an dieser Stelle nur an die wichtigsten Ergebnisse der (unendlichen) Galoistheorie erinnern. Eine ausführliche Einführung in die endliche Galoistheorie findet man in [La1, Kapitel 6], eine detailliertere Einführung in die unendliche Galoistheorie in [FJ, Kapitel 1]. Mit „kompakt“ meine ich im folgenden immer quasikompakt und hausdorffsch.

Ist $L \supset K$ eine unendliche Galoiserweiterung, so geht die im endlichen Fall geltende 1-1-Korrespondenz zwischen den Zwischenkörpern der Erweiterung $L \supset K$ und den Untergruppen der Galoisgruppe $G := \mathrm{Gal}(L/K)$ verloren: Es gibt zu viele Untergruppen in G. Der Hauptsatz der Galoistheorie läßt sich jedoch auf den unendlichen Fall übertragen, wenn man auf G eine geeignete Topologie einführt:
G ist auf natürliche Weise isomorph zum projektiven Limes der endlichen Gruppen $\mathrm{Gal}(M/K)$, wobei M alle galoisschen Zwischenkörper von $L \supset K$ durchläuft,

die über K endlichen Grad haben. Für $M' \subseteq M$ sei der Homomorphismus zwischen $\mathrm{Gal}(M/K)$ und $\mathrm{Gal}(M'/K)$ dabei die Restriktionsabbildung. Die von der proendlichen Topologie auf $\varprojlim \mathrm{Gal}(M/K)$ induzierte Topologie auf G heißt **Krull-Topologie**, G wird so zu einer proendlichen Gruppe.
Eine Basis der Topologie bilden dabei die Mengen

$$\{\tau \mathrm{Gal}(L/M) \mid \tau \in G, M \supseteq K \text{ endlich galoissch}, M \subseteq L\}.$$

Galoisgruppen sind als proendliche Gruppen kompakt und total unzusammenhängend. Man erhält das folgende Theorem:

Theorem 1.1 (Krull). *Sei $L \supseteq K$ eine Galoiserweiterung und $G := \mathrm{Gal}(L/K)$. Dann ist die Abbildung $M \overset{\varphi}{\mapsto} \mathrm{Gal}(L/M)$ eine Bijektion zwischen den Zwischenkörpern M von $L \supseteq K$ und den abgeschlossenen Untergruppen von G. Ist H eine abgeschlossene Untergruppe von G, so bildet die Umkehrabbildung H auf $\mathrm{Fix}(H)$ ab.*

Viele Eigenschaften von endlichen Galoiserweiterungen übertragen sich entsprechend auf unendliche Erweiterungen; die folgenden Lemmata sind Beispiele hierfür. Da ich zum einen, obwohl die Ergebnisse wohlbekannt sind, keine Quelle kenne, die ich zitieren könnte, und die Beweise zum anderen gut geeignet sind, einige typische Techniken der unendlichen Galoistheorie zu demonstrieren, werde ich die Beweise hier ausführen.
Zur Erinnerung: Eine Teilmenge eines kompakten Raumes ist genau dann abgeschlossen, wenn sie kompakt ist. Sind T_1, T_2 topologische Räume und ist $\varphi : T_1 \to T_2$ stetig, so ist das Bild einer kompakten Menge wieder kompakt. Sind weiter T_1 und T_2 kompakt, so ist φ abgeschlossen. Eine abgeschlossene Bijektion zwischen topologischen Räumen ist offen.

Lemma 1.2. *Sei $F \supseteq K$ galoissch und $M \supseteq K$ beliebig mit $F \cap M = K$. Dann ist die Restriktion*

$$res : \mathrm{Gal}(FM/M) \to \mathrm{Gal}(F/K)$$

ein Isomorphismus topologischer Gruppen.

Beweis: Die Abbildung $res : \mathrm{Gal}(FM/M) \to \mathrm{Gal}(F/K)$, $\sigma \mapsto \sigma|_F$ ist ein Gruppenhomomorphismus. Außerdem ist sie injektiv, denn ist ein Homomorphismus auf F und auf M die Identität, so auch auf dem Kompositum FM.
Zur Stetigkeit von res:
$\mathcal{B} := \{\mathrm{Gal}(F/K') \mid K' \supseteq K \text{ endlich galoissch}\}$ ist eine Umgebungsbasis der 1. Es genügt also zu zeigen, daß Urbilder von Mengen der Form $U = \mathrm{Gal}(F/K')$ aus $\mathcal{B}$ offen sind. Es ist $res^{-1}(U) = \{\sigma \in \mathrm{Gal}(FM/M) \mid \sigma|_{K'} = \mathrm{id}_{K'}\} = \mathrm{Gal}(FM/MK')$, $res^{-1}(U)$ ist also offen.
Zur Surjektivität von res:
Sei $H := \mathrm{Im}(res) \subseteq \mathrm{Gal}(F/K)$. Einerseits ist $K \subseteq \mathrm{Fix}(H)$; wird andererseits

$a \in F$ von H festgehalten, so liegt a in $\mathrm{Fix}(\mathrm{Gal}(FM/M)) = M$, das heißt es ist $a \in M \cap F = K$. Es ist also $\mathrm{Fix}(H) = K$; da H als Bild einer kompakten Menge unter einer stetigen Funktion abgeschlossen ist, folgt mit Theorem 1.1 schon $H = \mathrm{Gal}(F/K)$. Also ist res surjektiv.
Da $\mathrm{Gal}(FM/M)$ und $\mathrm{Gal}(F/K)$ kompakt sind und res stetig ist, ist res abgeschlossen. Aus der Bijektivität folgt dann weiter, daß res offen ist. ■

Bemerkung: Wie der Beweis zeigt, ist res ohne die Voraussetzung $F \cap M = K$ ein stetiger, injektiver Homomorphismus.

Lemma 1.3. *Sei K ein Körper, für $i \in I$ sei L_i eine Galoiserweiterung von K mit $\mathrm{Gal}(L_i/K) \cong G_i$. Weiter gelte $L_i \cap \prod_{j \neq i} L_j = K$ für $i \in I$. Dann ist*

$$G := \mathrm{Gal}\left(\prod_{i \in I} L_i/K\right) \cong \prod_{i \in I} G_i,$$

via Restriktion, wobei die rechte Seite die Produkttopologie trägt.

Beweis: Betrachte den Homomorphismus $res : G \to \prod_{i \in I} G_i$, $\sigma \mapsto \prod_{i \in I} \sigma|_{L_i}$ zwischen den topologischen Gruppen G mit der Krull-Topologie und $\prod_{i \in I} G_i$ mit der Produkttopologie. Dann sind G (als profinite Gruppe) und $\prod_{i \in I} G_i$ (nach dem Satz von Tychonoff) kompakt.
res ist injektiv, denn ist ein Automorphismus auf allen L_i die Identität, so auch auf dem Kompositum $L := \prod_{i \in I} L_i$.
Die Mengen $\left\{ \prod_{i \neq j} G_i \times \{\sigma_j\} \mid j \in I, \sigma_j \in G_j \right\}$ bilden eine Basis der Topologie auf $\prod_{i \in I} G_i$. Da das Urbild der Menge $\prod_{i \neq j} G_i \times \{\sigma_j\}$ für eine beliebige Fortsetzung $\widetilde{\sigma_j}$ von σ_j auf $\prod_{i \in I} L_i$ genau die offene Menge $\left\{\sigma \in G \mid \sigma|_{L_j} = \sigma_j\right\} = \widetilde{\sigma_j}\,\mathrm{Gal}(L/L_j)$ ist, folgt die Stetigkeit von res.
Es bleibt noch die Surjektivität von res zu zeigen: Da G und $\prod_{i \in I} G_i$ kompakt sind und res stetig ist, ist $res(G)$ abgeschlossen. Es reicht also zu zeigen, daß $res(G)$ dicht in $\prod_{i \in I} G_i$ liegt. Sei also $U = \prod_{i \neq j} G_i \times \{\sigma_j\} \subset \prod_{i \in I} G_i$ offen; wegen des letzten Lemmas existiert dann ein $\widetilde{\sigma_j} \in \mathrm{Gal}(L/\prod_{i \neq j} L_i) \subset \mathrm{Gal}(L/K)$ mit $\widetilde{\sigma_j}|_{L_j} = \sigma_j$ und $\widetilde{\sigma_j}|_{L_i} = \mathrm{id}_{L_i}$ für $i \neq j$, es ist also $res(\widetilde{\sigma_j}) \in U$. Als abgeschlossene Bijektion ist res auch offen. ■

Lemma 1.4. *Seien $F \supseteq K$ und $M \supseteq K$ Galoiserweiterungen. Dann gilt*

$$\begin{aligned}\mathrm{Gal}(FM/K) &\cong \mathrm{Gal}(F/K) \times_{F \cap M} \mathrm{Gal}(M/K) \\ &:= \left\{(\sigma, \tau) \in \mathrm{Gal}(F/K) \times \mathrm{Gal}(M/K) \mid \sigma|_{F \cap M} = \tau|_{F \cap M}\right\}\end{aligned}$$

Beweis: Der einzige vernünftige Kandidat für einen Isomorphismus ist die Abbildung

$$\begin{aligned} res : \mathrm{Gal}(FM/K) &\to \mathrm{Gal}(F/K) \times_{F \cap M} \mathrm{Gal}(M/K), \\ \sigma &\mapsto (\sigma|_F, \sigma|_M). \end{aligned}$$

res ist wohldefiniert und ein Homomorphismus; außerdem ist res offensichtlich injektiv.
Zum Beweis der Surjektivität:
Es sei $\sigma \in \mathrm{Gal}(F/K)$ und $\tau \in \mathrm{Gal}(M/K)$ mit $\sigma|_{F\cap M} = \tau|_{F\cap M} =: \gamma \in \mathrm{Gal}(F \cap M/K)$ gegeben. Ist $\gamma = \mathrm{id}_{F\cap M}$, so sind wir wegen Lemma 1.3 fertig. Sei also $\gamma \in \mathrm{Gal}(F \cap M/K)$ beliebig, und sei $\tilde{\gamma}$ eine beliebige Fortsetzung von γ auf FM. Dann ist $\sigma' := \sigma\big(\tilde{\gamma}^{-1}|_F\big) \in \mathrm{Gal}\big(F/(F\cap M)\big)$ und $\tau' := \tau\big(\tilde{\gamma}^{-1}|_M\big) \in \mathrm{Gal}\big(M/(F\cap M)\big)$, es gibt also eine gemeinsame Fortsetzung α von σ' und τ' auf FM. Dann ist $\alpha\tilde{\gamma}$ das gesuchte Urbild von (σ, τ).
Zur Stetigkeit:
Es sei U eine offene Umgebung der 1 in $\mathrm{Gal}(F/K) \times_{F\cap M} \mathrm{Gal}(M/K)$, also etwa $U = \big(\mathrm{Gal}(F/K_1) \times \mathrm{Gal}(M/K_2)\big) \cap \big(\mathrm{Gal}(F/K) \times_{F\cap M} \mathrm{Gal}(M/K)\big)$ für endlich erzeugte Zwischenkörper K_1, K_2 von $F \supseteq K$ bzw. $M \supseteq K$. Dann ist $res^{-1}(U) = \mathrm{Gal}(FM/K_1K_2)$ offen.
Wieder folgt die Offenheit von res. ■

Bemerkung: Sind $F \supseteq K$ und $M \supseteq K$ Galoiserweiterungen und ist $E \subseteq F \cap M$, so heißt

$$\mathrm{Gal}(F/K) \times_E \mathrm{Gal}(M/K) := \big\{(\sigma, \tau) \in \mathrm{Gal}(F/K) \times \mathrm{Gal}(M/K) \mid \sigma|_E = \tau|_E\big\}$$

Faserprodukt von $\mathrm{Gal}(F/K)$ und $\mathrm{Gal}(M/K)$ über E.

Zum Abschluß dieses Abschnitts noch folgende Erinnerung: Ein Körper K heißt **unbeschränkt**, wenn er für ein $n \in \mathbb{N}$ unendlich viele Galoiserweiterungen von Grad n besitzt.

1.1.3 Lineare und algebraische Disjunktheit

Zu jedem der in diesem Abschnitt zitierten Ergebnisse findet sich in mindestens einem der beiden Bücher [FJ, Kapitel 9.1] und [La1, Kapitel 8.1] ein Beweis.

L und M seien zwei Erweiterungen von K. Dann heißt L **linear disjunkt** von M über K, falls für alle endlichen Teilmengen S von L gilt: Ist S linear unabhängig über K (im Körper L), so ist S auch linear unabhängig über M (im Körper LM); kurz: $\boldsymbol{L \underset{K}{\overset{l}{\perp}} M}$.

L heißt **algebraisch disjunkt** von M über K, falls für alle endlichen Teilmengen S von L gilt: Ist S algebraisch unabhängig über K (im Körper L), so ist S auch algebraisch unabhängig über M (im Körper LM); kurz: $\boldsymbol{L \underset{K}{\overset{a}{\perp}} M}$.

Es läßt sich zeigen, daß die beiden Definitionen symmetrisch in L und M sind. In den nächsten beiden Bemerkungen sind einige grundlegende Eigenschaften linearer und algebraischer Disjunktheit aufgeführt, die ich im Rest der Arbeit (oft stillschweigend) benutzen werde:

Bemerkung 1.5. *Seien $L \supseteq K$ und $F \supseteq M \supseteq K$ Erweiterungen von K. Dann gilt:*

1) Lineare und algebraische Disjunktheit haben endlichen Charakter: L ist linear bzw. algebraisch disjunkt von M über K genau dann, wenn alle über K endlich erzeugten $L_0 \subseteq L$ und $M_0 \subseteq M$ linear bzw. algebraisch disjunkt über K sind.

2) Ist $L \supseteq K$ oder $M \supseteq K$ algebraisch, so sind L und M algebraisch disjunkt über K.

3) Aus $L \underset{K}{\overset{l}{\downarrow}} M$ folgt $L \underset{K}{\overset{a}{\downarrow}} M$ (die Umkehrung ist falsch, wie das Beispiel $L = M = K^a \supsetneq K$ zeigt), stärker sogar $L^a \underset{K}{\overset{a}{\downarrow}} M^a$.

4) Ist $[L : K] < \infty$, so gilt

$$L \underset{K}{\overset{l}{\downarrow}} M \iff [L : K] = [LM : M].$$

Gilt außerdem $[M : K] < \infty$, so ist dies gleichbedeutend mit

$$[LM : K] = [L : K][M : K].$$

5) Ist $L \supseteq K$ galoissch, so ist äquivalent:

- $L \underset{K}{\overset{l}{\downarrow}} M$
- $L \cap M = K$
- *Die Restriktion $res : \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$ ist eine Bijektion.*
- *Die Restriktion $res : \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$ ist ein Isomorphismus topologischer Gruppen.*

6) • $L \underset{K}{\overset{l}{\downarrow}} F \iff$ *es ist* $L \underset{K}{\overset{l}{\downarrow}} M$ *und* $LM \underset{M}{\overset{l}{\downarrow}} F$

• $L \underset{K}{\overset{a}{\downarrow}} F \iff$ *es ist* $L \underset{K}{\overset{a}{\downarrow}} M$ *und* $LM \underset{M}{\overset{a}{\downarrow}} F$

Die in Bemerkung 1.5.6 beschriebene Eigenschaft linearer und algebraischer Disjunktheit bezeichne ich fortan als **Turmeigenschaft**.

Anschaulich kann man sich lineare Disjunktheit von Körpererweiterungen folgendermaßen vorstellen: L und M sind linear disjunkt über K, wenn sie so wenig wie möglich miteinander zu tun haben; das heißt mindestens, daß ihr Schnitt nur K enthält, aber zum Beispiel auch, daß sie nicht verschiedene Nullstellen eines über K irreduziblen Polynoms enthalten. Sind zum Beispiel ξ_1 und ξ_2 verschiedene dritte Wurzeln aus 2, so ist $\mathbb{Q}(\xi_1) \underset{\mathbb{Q}}{\overset{l}{\not\downarrow}} \mathbb{Q}(\xi_2)$, denn es gilt $[\mathbb{Q}(\xi_1) : \mathbb{Q}] = 3 > [\mathbb{Q}(\xi_1, \xi_2) : \mathbb{Q}(\xi_1)] = 2$.

Sind Körpererweiterungen $L_i \supseteq K$ für $i \in I$ gegeben, so heißen die Erweiterungen L_i **linear disjunkt** über K, wenn für alle $i \in I$ gilt, daß L_i linear disjunkt von $\prod_{j \neq i} L_j$ über K ist. Ist I linear geordnet, so ist mit den vorangegangenen Bemerkungen leicht zu zeigen, daß dies äquivalent dazu ist, daß $L_i \underset{K}{\overset{l}{\downarrow}} \prod_{j<i} L_j$ für alle $i \in I$ gilt.

1.1.4 p-Basen, λ-Funktionen und Separabilität

Die Darstellung in diesem Abschnitt orientiert sich an [FJ, Kapitel 9.2, 9.3] und an [La1, Kapitel 8.4]; dort finden sich auch die hier nicht ausgeführten Beweise.

Es sei K ein Körper der Charakteristik $p > 0$; weiter sei K_0 ein Unterkörper von K, der K^p enthält. Ist $a \in K$, so ist der Grad von $\mathrm{Irr}(a, K_0)$ entweder 1 oder p: Denn ist $\deg(\mathrm{Irr}(a, K_0)) = l$ für ein $l < p$, dann folgt $a^l \in K_0$ und $a^p \in K_0$, also auch $a^{p-l} \in K_0$; Division mit Rest ergibt dann $a^{\mathrm{ggT}(l,p)} = a \in K_0$, also $l = 1$.
Sind $a_1, \dots, a_n \in K$, so gilt also $[K_0(a_1, \dots, a_n) : K_0] = p^i$ für ein $i \leq n$. Für eine Teilmenge B von K seien

$$M(B) := \{b_1^{i_1} \cdot \ldots \cdot b_n^{i_n} \mid n \in \mathbb{N},\ b_k \in B \text{ p.v. }, 0 \leq i_k < p \text{ für } 1 \leq k \leq n)\}$$

die **p-Monome** von B. Es sei $(M_i(B))_{i \in I}$ jeweils eine Aufzählung von $M(B)$.

Definition und Lemma 1.6. *Es sei K ein Körper der Charakteristik p und K_0 ein Unterkörper von K, der K^p enthält; weiter seien $a_1, \dots, a_n \in K$. Dann heißen $a_1, \dots, a_n$* **p-unabhängig über $\mathbf{K_0}$**, *falls eine der folgenden äquivalenten Bedingungen erfüllt ist:*

1) Es ist $[K_0(a_1, \dots, a_n) : K_0] = p^n$.
2) Für alle $1 \leq i \leq n$ ist der Grad $[K_0(a_i) : K_0] = p$ und die Erweiterungen $(K_0(a_i))_{1 \leq i \leq n}$ sind linear disjunkt über K_0.
3) Die Elemente $a_1, \dots, a_N$ sind p. v. und die p-Monome $M(\{a_1, \dots a_n\})$ sind linear unabhängig im K_0-Vektorraum K.

Eine Teilmenge $B \subset K$ heißt p-unabhängig über K_0, wenn je endlich viele Elemente aus B p-unabhängig über K_0 sind. Ist B p-unabhängig über K_0, so sind die p-Monome $M(B)$ eine Vektorraumbasis von $K_0(B)$ über K_0.
Ist B p-unabhängig über K_0 und gilt $K_0(B) = K$, so ist B eine **p-Basis von K über $\mathbf{K_0}$**. Ist $K_0 = K^p$, so spricht man von **p-Unabhängigkeit** und **p-Basen** schlechthin.

Bemerkung: B ist genau dann p-abhängig, wenn für ein $b \in B$ eine Linearkombination $b = \sum k_i^p M_i(B \setminus \{b\})$ existiert.

Beweis: „$\Leftarrow$" ist klar. Also zu „$\Rightarrow$": B sei p-abhängig; ohne Einschränkung sei $B \setminus \{b\}$ für alle $b \in B$ p-unabhängig. Wir zeigen, daß jedes $b \in B$ in $K(B \setminus \{b\})$ enthalten ist: Denn wäre $b \notin K(B \setminus \{b\})$, so hätte b über $K(B \setminus \{b\})$ schon Grad p, also wäre $b^0, \dots, b^{p-1}$ eine Vektorraumbasis von $K(B)$ über $K(B \setminus \{b\})$. Dann wäre $M(B)$ eine Vektorraumbasis von $K(B) \supseteq K$, und damit wäre B p-unabhängig. ■

Das $n \in \mathbb{N} \cup \{\infty\}$ mit $p^n = [K : K^p]$ heißt **Imperfektionsexponent**, die p-Potenz p^n heißt **Imperfektionsgrad** von K. Für p-Basen gelten der übliche Basisaustausch- und Basisergänzungssatz.

Um im weitern den Fall $p = 0$ nicht immer getrennt behandeln zu müssen, führen wir die folgende Konvention ein:

Ist $p = 0$, so sei $K^p := K$; dann ist $\{1\}$ eine p-Basis von K, der Imperfektionsgrad von K ist 1 und der Imperfektionsexponent ist 0. Alle im folgenden auftauchenden Aussagen über p-Basen, λ-Funktionen und Separabilität werden in diesem Falle trivial.

Definition 1.7 (λ-Funktionen). *Sei K ein Körper der Charakteristik $p > 0$. Für $n \in \mathbb{N}$ sei $(M_{n,i}(\bar{X}))_{0 \leq i \leq p^n - 1}$ eine Aufzählung der Monome $X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$ mit $0 \leq i_1, \ldots, i_n \leq p-1$. Die $n+1$-stelligen Funktionen $\lambda_{n,i}^K : K^n \times K \to K$ seien wie folgt definiert:*

Ist das n-Tupel $\bar{a}$ p-abhängig, oder ist das $n+1$-Tupel $(\bar{a}, b)$ p-unabhängig, so ist $\lambda_{n,i}^K(\bar{a}, b) = 0$. Andernfalls ist $\lambda_{n,i}^K(\bar{a}, b)$ durch die Beziehung

$$b = \sum_{i=0}^{p^n - 1} \lambda_{n,i}^K(\bar{a}, b)^p M_{n,i}(\bar{a})$$

eindeutig bestimmt. Die Funktionen $\lambda_{n,i}^K$ heißen **λ-Funktionen des Körpers $\mathbf{K}$**[4].

Die λ-Funktionen eines Körpers K sind in K $\emptyset$-definierbar.

Bei der nächsten Definition handelt es sich um eine Verallgemeinerung des Begriffs der separablen algebraischen Erweiterung. Es hängt vom Kontext ab, mit welcher der äquivalenten Formulierungen es sich am besten arbeiten läßt:

Definition und Lemma 1.8 (Separabilität). *Eine Körpererweiterung $L \supseteq K$ ist* **separabel**, *wenn eine der folgenden äquivalenten Bedingungen gilt:*

1) $L \underset{K}{\overset{l}{\downarrow}} K^{1/p^\infty}$

2) $L \underset{K}{\overset{l}{\downarrow}} K^{1/p}$

3) Jede p-unabhängige Teilmenge von K bleibt p-unabhängig in L.

4) K ist unter den λ-Funktionen von L abgeschlossen.

5) Die λ-Funktionen von K sind genau die auf K eingeschränkten λ-Funktionen von L, das heißt es gilt $\lambda_{n,i}^K = \lambda_{n,i}^L|_K$.

Hat K die Charakteristik 0, so ist jede Erweiterung von K separabel.

Den Abschluß von K unter den λ-Funktionen von L bezeichne ich fortan mit $\mathrm{cl}_{\lambda_L}(K)$.

Beweis: Für die Äquivalenz von 1) und 2) siehe [FJ, Lemma 9.5].

2)$\Rightarrow$3): Es sei B eine in K p-unabhängige Teilmenge von K; ohne Einschränkung sei B endlich, etwa $B = \{b_1, \ldots, b_n\}$. Angenommen B ist p-abhängig über L, etwa

$$\sum_{j=0}^{p^n - 1} l_j^p M_j(B) = 0$$

[4] Ist zum Beispiel $\mathrm{char}(K) = 0$, so ist $\lambda_{1,1}$ die Identität auf K, alle anderen λ-Funktionen sind identisch 0

mit $l_j \in L$. Aus $L \underset{K}{\overset{l}{\smile}} K^{1/p}$ folgt $L^p \underset{K^p}{\overset{l}{\smile}} K$, also existieren $(k_j)_{0 \leq j \leq p^n - 1} \in K$ mit $\sum_{j=0}^{p^n-1} k_j^p M_j(B) = 0$, das heißt B ist p-abhängig über K. Widerspruch!
3)⇒4): Es seien $a_1, \ldots, a_n, b \in K$. Seien $a_1, \ldots, a_n$ p-unabhängig in L und $a_1, \ldots, a_n$, b p-abhängig in L, etwa

$$b = \sum_{j=0}^{p^n-1} \lambda_{j,n}^L(\bar{a}, b)^p M_j(\{a_1, \ldots, a_n\}).$$

Da nach Voraussetzung $\bar{a}, b$ schon p-abhängig über K sind, und die obige Darstellung von b eindeutig ist, liegen die $\lambda_{j,n}^L(\bar{a}, b)$ schon in K. Also ist K unter den λ-Funktionen von L abgeschlossen.
4)⇒2): Es seien $k_1, \ldots, k_r \in K$ und $l_1, \ldots, l_r \in L$mit $\sum_{i=1}^r l_i \sqrt[p]{k_i} = 0$; dabei sei r minimal gewählt. Dann ist auch $\sum_{i=1}^r l_i^p k_i = 0$. Da K gegen die λ-Funktionen von L abgeschlossen ist, liegen die l_i schon in K. Also sind $\sqrt[p]{k_1}, \ldots, \sqrt[p]{k_r}$ schon linear abhängig über K. Also ist $L \underset{K}{\overset{l}{\smile}} K^{1/p}$.
3), 4)⇒5): Es seien $a_1, \ldots, a_n, b \in K$. Dann gilt

$$\begin{aligned}
\lambda_{n,i}^K(\bar{a}, b) = 0 \text{ für alle } i \in \{0, \ldots, p^n - 1\} &\iff \bar{a} \text{ ist } p\text{-abh. über } K \text{ oder } \bar{a}, b \text{ sind } p\text{-unabh. über } K \\
&\overset{3)}{\iff} \bar{a} \text{ ist } p\text{-abh. über } L \text{ oder } \bar{a}, b \text{ sind } p\text{-unabh. über } L \\
&\iff \lambda_{n,i}^L(\bar{a}, b) = 0 \text{ für alle } i \in \{0, \ldots, p^n - 1\}
\end{aligned}$$

Gilt $b = \sum_{j=0}^{p^n-1} \lambda_{j,n}^L(\bar{a}, b)^p M_j(\{a_1, \ldots, a_n\})$, so sind die $\lambda_{j,n}^L(\bar{a}, b)$ wegen 4) schon aus K; aus der Eindeutigkeit der λ-Funktionen folgt dann $\lambda_{j,n}^L(\bar{a}, b) = \lambda_{j,n}^K(\bar{a}, b)$.
5)⇒4) ist klar. ■

Für algebraische Erweiterungen stimmt diese Definition mit der herkömmlichen überein. Aus Punkt 1) bzw. 2) ergibt sich sofort der endliche Charakter der Definition, das heißt eine Erweiterung $L \supseteq K$ ist genau dann separabel, wenn alle über K endlich erzeugten $L_0 \subseteq L$ separabel über K sind.

Im folgenden sind die wichtigsten Eigenschaften separabler Erweiterungen aufgeführt:

Lemma 1.9. *Seien $K \subseteq L \subseteq F$ und $K \subseteq M$ Körpererweiterungen.*

1) Jede Erweiterung eines perfekten Körpers ist separabel.
2) **(Transitivität)** *Sind $K \subseteq L$ und $L \subseteq F$ separabel, so ist es auch $K \subseteq F$.*
3) **(schwache Monotonie)** *Ist $K \subseteq F$ separabel, so auch $K \subseteq L$; dagegen ist $L \subseteq F$ nicht notwendigerweise separabel. Ist dagegen $K \subseteq L$ algebraisch separabel und $K \subseteq F$ separabel, so ist auch $L \subseteq F$ separabel.*
4) Ist $K \subseteq L$ separabel und ist $L \underset{K}{\overset{a}{\smile}} M$, so ist auch die Erweiterung $M \subseteq LM$ separabel. Ist auch $K \subseteq M$ separabel, so folgt die Separabilität von $K \subseteq LM$.

Zu Punkt 3) betrachte man zum Beispiel den Körperturm $K \subset K(x) \subset K(\sqrt[p]{x})$, wobei x transzendent über K und $p \neq 0$ die Charakteristik von K ist: $K \subset K(x)$ ist separabel, denn $\{x^s \mid s \in \mathbb{Z}\}$ ist eine Vektorraumbasis von $K(x)$ über K und von $K^{1/p}(x)$ über $K^{1/p}$, also ist $K(x) \underset{K}{\overset{l}{\downarrow}} K^{1/p}$. Genauso ist $K(\sqrt[p]{x}) \supset K$ separabel. Dagegen ist $K(\sqrt[p]{x}) \supset K(x)$ rein inseparabel und damit keine separable Erweiterung.

1.1.5 Reguläre und primäre Erweiterungen

Definition und Lemma 1.10. *Eine Körpererweiterung $L \supseteq K$ heißt* **regulär**, *wenn eine der folgenden äquivalenten Bedingungen gilt:*

1) $L \underset{K}{\overset{l}{\downarrow}} K^a$
2) $L \supseteq K$ ist separabel und es gilt $L \cap K^a = K$
3) $L \supseteq K$ ist separabel und es gilt $L \cap K^s = K$
4) $L \supseteq K$ ist separabel und die Restriktion $res : \mathcal{G}(L) \to \mathcal{G}(K)$ ist surjektiv.

Bemerkung: Ist $\mathrm{char}(K) = 0$, so ist $L \supseteq K$ genau dann separabel, wenn die Restriktion $res : \mathcal{G}(L) \to \mathcal{G}(K)$ surjektiv ist.

Beweis: Für 1)⇔2) siehe z.B. [La1, Seite 366]. Die Implikation 2)⇒3) ist trivial.
3)⇒4) ist klar, denn mit Bemerkung 1.5.5 folgt aus $L \cap K^{\mathrm{s}} = K$, daß die Galoisgruppen $\mathrm{Gal}(K^{\mathrm{s}}/K)$ und $\mathrm{Gal}(LK^{\mathrm{s}}/L)$ via Restriktion isomorph sind; da die Restriktion von $\mathcal{G}(L)$ auf $\mathrm{Gal}(LK^{\mathrm{s}}/L)$ surjektiv ist, folgt auch die Surjektivität von $res : \mathcal{G}(L) \to \mathcal{G}(K)$.
Zu 4)⇒3): Ist $res : \mathcal{G}(L) \to \mathcal{G}(K)$ surjektiv, so ist es auch die Restriktion von $res_1 : \mathrm{Gal}(LK^{\mathrm{s}}/L) \to \mathcal{G}(K)$ (denn res ist die Verkettung der Restriktion von $\mathcal{G}(L)$ auf $\mathrm{Gal}(LK^{\mathrm{s}}/L)$ mit res_1). Außerdem ist res_1 injektiv, also ein Isomorphismus. Mit Bemerkung 1.5.5 folgt $L \cap K^{\mathrm{s}} = K$.
3)⇒2): $L \cap K^{\mathrm{s}} = K$ bedeutet wegen Bemerkung 1.5.5 schon $L \underset{K}{\overset{l}{\downarrow}} K^{\mathrm{s}}$. Mit Lemma 1.9.4 folgt aus der Separabilität von $L \supseteq K$ auch die Separabilität von $LK^{\mathrm{s}} \supseteq K^{\mathrm{s}}$; also ist $LK^{\mathrm{s}} \underset{K^{\mathrm{s}}}{\overset{l}{\downarrow}} (K^{\mathrm{s}})^{1/p^\infty} = K^{\mathrm{a}}$. Insgesamt folgt mit der Turmeigenschaft also $L \underset{K}{\overset{l}{\downarrow}} K^{\mathrm{a}}$. ∎

Es folgen einige Eigenschaften regulärer Erweiterungen; insbesondere erhalten wir ein Kriterium dafür, wann aus algebraischer Disjunktheit auch lineare Disjunktheit folgt:

Lemma 1.11. *Seien $K \subseteq L \subseteq F$ und $K \subseteq M$ Körpererweiterungen.*

1) **(Transitivität)** *Sind $K \subseteq L$ und $L \subseteq F$ regulär, so ist es auch $K \subseteq F$.*
2) **(schwache Monotonie)** *Ist $K \subseteq F$ regulär, so auch $K \subseteq L$; dagegen ist $L \subseteq F$ nicht notwendigerweise regulär.*
3) Ist $L \supseteq K$ eine reguläre und $M \supseteq K$ eine beliebige Erweiterung mit $L \underset{K}{\overset{a}{\downarrow}} M$, so gilt schon $L \underset{K}{\overset{l}{\downarrow}} M$, und $LM \supseteq M$ ist ebenfalls regulär.
4) Sind zwei reguläre Erweiterungen $L \supseteq K$ und $M \supset K$ algebraisch disjunkt, so ist

auch $LM \supseteq K$ regulär.

Schließlich benötigen wir noch den Begriff der primären Erweiterung:

Definition und Lemma 1.12. *Eine Körpererweiterung $L \supseteq K$ heißt* **primär**, *wenn eine der folgenden äquivalenten Bedingungen gilt:*

1) $L \underset{K}{\overset{l}{\downarrow}} K^s$
2) $L \cap K^a \supseteq K$ ist rein inseparabel.

Primäre Erweiterungen haben die folgenden Eigenschaften:

Lemma 1.13. *Seien $K \subseteq L \subseteq F$ und $K \subseteq M$ Körpererweiterungen.*

1) Jede Erweiterung eines separabel abgeschlossenen Körpers ist primär.
2) Sind $L \supseteq K$ und $F \supseteq L$ primär, so ist es auch $F \supseteq K$.
3) Ist $F \supseteq K$ primär, so ist es auch $L \supseteq K$.
4) Sind L und M algebraisch disjunkt über K, so ist mit $L \supseteq K$ auch $M \subseteq LM$ primär.
5) Sind L und M algebraisch disjunkt über K und sind $L \supseteq K$ und $M \supseteq K$ primär, so ist es auch $LM \supseteq K$.

Die Begriffe separabel, regulär und primär hängen folgendermaßen zusammen:

Korollar 1.14. *Die Erweiterung $M \supseteq K$ ist genau dann regulär, wenn sie separabel und primär ist.*

Lemma 1.15. *Es sei $L \supseteq K$ eine reguläre Erweiterung. Dann ist auch $L^s \supseteq K^s$ regulär.*

Beweis: $L \supseteq K$ ist regulär, das heißt es ist $L \underset{K}{\overset{l}{\downarrow}} K^{\mathrm{a}}$; also gilt mit der Turmeigenschaft auch $LK^{\mathrm{s}} \underset{K^{\mathrm{s}}}{\overset{l}{\downarrow}} K^{\mathrm{a}}$. Weiter ist $L^{\mathrm{s}} \supseteq LK^{\mathrm{s}}$ separabel algebraisch, also separabel; demnach ist L^{s} linear disjunkt von $(LK^{\mathrm{s}})^{1/p^\infty}$ über LK^{s}. Wegen $LK^{\mathrm{a}} \subseteq (LK^{\mathrm{s}})^{1/p^\infty}$ gilt also erst recht $L^{\mathrm{s}} \underset{LK^{\mathrm{s}}}{\overset{l}{\downarrow}} LK^{\mathrm{a}}$. Insgesamt folgt mit der Turmeigenschaft $L^{\mathrm{s}} \underset{K^{\mathrm{s}}}{\overset{l}{\downarrow}} K^{\mathrm{a}}$, das heißt $L^{\mathrm{s}} \supseteq K^{\mathrm{s}}$ ist regulär. ∎

Den Abschluß dieses Abschnittes bildet ein Lemma, das ein bestimmtes, im Hauptteil der Arbeit auftretendes Diagramm von Körpern analysiert. Es handelt sich um [Ch1, Lemma 3.1].

Lemma 1.16. *Es seien L und M reguläre Erweiterungen von K mit $L \underset{K}{\overset{l}{\downarrow}} M$. Weiter seien $\hat{K} \supseteq K$, $\hat{L} \supseteq L$ und $\hat{M} \supseteq M$ Galoiserweiterungen, so daß $\hat{L}$ und $\hat{M}$ reguläre Erweiterungen von $\hat{K}$ sind. Dann ist $\hat{L} \underset{\hat{K}}{\overset{l}{\downarrow}} \hat{M}$, und es gilt*

$$\mathrm{Gal}(\hat{L}\hat{M}/LM) \cong \mathrm{Gal}(\hat{L}/L) \times_{\hat{K}} \mathrm{Gal}(\hat{M}/M)$$

Bemerkung: Wegen Lemma 1.15 gilt die Aussage insbesondere für $\hat{K} = K^{\mathrm{s}}$, $\hat{L} = L^{\mathrm{s}}$ und $\hat{M} = M^{\mathrm{s}}$.

Beweis: Aus $L \underset{K}{\overset{l}{\downarrow}} M$ erhält man mit Bemerkung 1.5.3 auch $\hat{L} \underset{K}{\overset{a}{\downarrow}} \hat{M}$ und mit der Turmeigenschaft dann auch $\hat{L} \underset{\hat{K}}{\overset{a}{\downarrow}} \hat{M}$. Da $\hat{L} \supseteq \hat{K}$ regulär ist, folgt mit Lemma 1.11.3 schon die lineare Disjunktheit. Es gilt:

1) Wegen $L \underset{K}{\overset{l}{\downarrow}} M$ ist $LM \supseteq L$ regulär, $\hat{L} \supseteq L$ dagegen ist algebraisch; wegen Bemerkung 1.5.5 ist also $\mathrm{Gal}(\hat{L}M/LM) \cong \mathrm{Gal}(\hat{L}/L)$ via Restriktion. Genauso gilt $\mathrm{Gal}(L\hat{M}/LM) \cong \mathrm{Gal}(\hat{M}/M)$.
2) Aus $\hat{L} \underset{\hat{K}}{\overset{l}{\downarrow}} \hat{M}$ folgt mit der Turmeigenschaft $\hat{L}M \underset{LM\hat{K}}{\overset{l}{\downarrow}} \hat{M}L$, also $\hat{L}M \cap \hat{M}L = \hat{K}LM$.
   Zur Situation:

$$\begin{tikzcd}[column sep=small]
 & \hat{L}\hat{M} \arrow[dl, dash] \arrow[dr, dash] & \\
\hat{L}M \arrow[dr, dash] & & \hat{M}L \arrow[dl, dash] \\
 & \hat{K}LM \arrow[d, dash] & \\
 & LM &
\end{tikzcd}$$

   Mit Lemma 1.4 folgt also

$$\mathrm{Gal}(\hat{L}\hat{M}/LM) \cong \mathrm{Gal}(\hat{L}M/LM) \times_{LM\hat{K}} \mathrm{Gal}(L\hat{M}/LM)$$

   via Restriktion.

Nach 1) sind die Restriktionsabbildungen $res_1 : \mathrm{Gal}(\hat{L}M/LM) \to \mathrm{Gal}(\hat{L}/L)$ und $res_2 : \mathrm{Gal}(L\hat{M}/LM) \to \mathrm{Gal}(\hat{M}/M)$ Isomorphismen topologischer Gruppen, also ist auch das Produkt

$$res_\times : \mathrm{Gal}(\hat{L}M/LM) \times \mathrm{Gal}(L\hat{M}/LM) \to \mathrm{Gal}(\hat{L}/L) \times \mathrm{Gal}(\hat{M}/M)$$

ein Isomorphismus topologischer Gruppen.
Das Bild von $\mathrm{Gal}(\hat{L}M/LM) \times_{LM\hat{K}} \mathrm{Gal}(L\hat{M}/LM)$ unter $res_\times$ ist wegen $LM\hat{K} \cap \hat{L} \cap \hat{M} = \hat{K}$ genau $\mathrm{Gal}(\hat{L}/L) \times_{\hat{K}} \mathrm{Gal}(\hat{M}/M)$. Also ist die Einschränkung von $res_\times$ auf $\mathrm{Gal}(\hat{L}M/LM) \times_{LM\hat{K}} \mathrm{Gal}(L\hat{M}/LM)$ ein Isomorphismus zwischen $\mathrm{Gal}(\hat{L}M/LM) \times_{LM\hat{K}} \mathrm{Gal}(L\hat{M}/LM)$ und $\mathrm{Gal}(\hat{L}/L) \times_{\hat{K}} \mathrm{Gal}(\hat{M}/M)$. ■

1.1.6 Diskriminante und Resultante

Die Ergebnisse dieses Abschnitts finden sich in [Wae, Kapitel 5, §33 - §35].

Ist K ein Körper und

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{i=1}^{n}(X - \alpha_i) \in K[X],$$

so heißt das Produkt

$$D(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$$

die **Diskriminante** von f.
Sind zwei Polynome $f(X) := a_nX^n + \cdots + a_0$ und $g(X) := b_mX^m + \cdots + b_0$ aus $K[X]$ mit $a_n, b_n \neq 0$ gegeben, so heißt

$$R(f,f') = \left|\begin{array}{ccccccccc} a_n & a_{n-1} & & \cdots & & a_0 & & & \\ 0 & a_n & a_{n-1} & & \cdots & & a_0 & & \\ & & \ddots & & & & & \ddots & \\ & & & \ddots & & & & & \ddots \\ & & & & a_n & a_{n-1} & & \cdots & a_0 \\ \hdashline b_m & b_{m-1} & & \cdots & & b_0 & & & \\ 0 & b_m & b_{m-1} & & \cdots & & b_0 & & \\ & & \ddots & & & & & \ddots & \\ & & & \ddots & & & & & \ddots \\ & & & & b_m & b_{m-1} & & \cdots & b_0 \end{array}\right| \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} m \\ \left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} n \end{array}$$

die **Resultante** von f und g.
Zwischen Diskriminante und Resultante besteht der folgende Zusammenhang: Ist $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$, so ist

$$R(f,f') = \pm D(f).$$

1.2 Bewertungstheorie

Eine detaillierte Einführung in die Bewertungstheorie (und insbesondere Beweise zu allen hier zitierten Ergebnissen) findet sich in [En]. Die Bewertungstheorie von algebraischen Funktionenkörpern wird ausführlich in [St] dargestellt.

1.2.1 Grundlegende Begriffe

Die Darstellung in diesem und dem nächsten Abschnitt ist in weiten Teilen der Vorlesung „Arithmetik von Körpern“ , gehalten im Wintersemester 2002/2003 von Jochen Koenigsmann an der Albert-Ludwigs-Universität in Freiburg, entnommen.

Es sei K ein Körper und $(\Gamma, +, <)$ eine angeordnete abelsche Gruppe. Eine surjektive Abbildung $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ heißt **Bewertung mit Wertegruppe $\mathbf{\Gamma}$**, falls für alle $x, y \in K$ gilt:

1) $v(x) = \infty \iff x = 0$;
2) $v(x \cdot y) = v(x) + v(y)$;
3) $v(x + y) \geq \min\{v(x), v(y)\}$.

Für das Symbol ∞ gelten die folgenden Regeln: Für alle $\gamma \in \Gamma$ ist $\gamma < \infty$, $\gamma + \infty = \infty + \gamma = \infty$ und es ist $\infty + \infty = \infty$.

v sei eine Bewertung des Körpers K. Ist $x \in K^\times$, so gilt $v(x^{-1}) = -v(x)$. Es ist $v(1) = 0$; für beliebige $x, y \in K$ gilt $v(x) = v(-x)$. Ist $v(x) < v(y)$, so ist $v(x+y) = v(x)$. Eine Bewertung heißt trivial auf K, wenn sie auf K identisch 0 ist.

Ein Teilring $\mathcal{O} \subseteq K$ heißt **Bewertungsring von K**, wenn für alle $x \in K$ gilt, daß x oder x^{-1} in $\mathcal{O}$ liegt.

Bewertungsringe sind lokal: Die Menge $\mathcal{M}_{\mathcal{O}} := \mathcal{O} \setminus \mathcal{O}^\times = \{x \in \mathcal{O} \mid x^{-1} \notin \mathcal{O}\}$ der Nichteinheiten in $\mathcal{O}$ ist maximales Ideal von $\mathcal{O}$. Demnach ist $K_{\mathcal{O}} := \mathcal{O}/\mathcal{M}_{\mathcal{O}}$ ein Körper, der **Restklassenkörper von $\mathcal{O}$**. Hat K die Charakteristik 0, so kann $K_{\mathcal{O}}$ die Charakteristik $p \neq 0$ für eine Primzahl p haben. Hat dagegen K die Charakteristik $p \neq 0$, so hat auch $K_{\mathcal{O}}$ die Charakteristik p.

Seien nun K und L Körper. Eine Abbildung $\varphi : K \to L \cup \{\infty\}$ heißt **Stelle**, falls für alle $x, y \in K$ gilt:

1) Ist $\varphi(x) + \varphi(y)$ definiert, so gilt $\varphi(x + y) = \varphi(x) + \varphi(y)$;
2) Ist $\varphi(x) \cdot \varphi(y)$ definiert, so gilt $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$;
3) $\varphi(1) = 1$.

Für das Symbol ∞ gelten die folgenden Regeln: Für alle $x \in L$ ist $x + \infty = \infty + x = \infty$, für alle $x \in L \setminus \{0\}$ ist $x \cdot \infty = \infty \cdot x = \infty \cdot \infty = \infty$; die Ausdrücke $\infty + \infty$, $0 \cdot \infty$ und $\infty \cdot 0$ sind nicht definiert.

Ist $\varphi : K \to L \cup \{\infty\}$ eine Stelle, so ist $\varphi(0) = 0$, für $x \neq 0$ ist $\varphi(x^{-1}) = (\varphi(x))^{-1}$ und es gilt $\varphi(x) = 0 \iff \varphi(x^{-1}) = \infty$.

Zwischen Bewertungen, Bewertungsringen und Stellen besteht der folgende Zusammenhang:

Theorem 1.17.

- *Ist v eine Bewertung von K, so ist $\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ ein Bewertungsring von K mit maximalem Ideal $\mathcal{M}_v := \{x \in K \mid v(x) > 0\}$.*
- *Ist $\mathcal{O}$ ein Bewertungsring, so wird $K^\times/\mathcal{O}^\times$ durch $x\mathcal{O}^\times \leq y\mathcal{O}^\times :\iff \frac{y}{x} \in \mathcal{O}$ zu einer angeordneten abelschen Gruppe. Die Projektion $v_{\mathcal{O}} : K^\times \twoheadrightarrow K^\times/\mathcal{O}^\times$ ist eine Bewertung von K, wenn man $v(0) = \infty$ setzt; die Projektion $\varphi_{\mathcal{O}} : K \twoheadrightarrow \mathcal{O}/\mathcal{M}_{\mathcal{O}}$ ist eine Stelle, wenn man für $x \in K \setminus \mathcal{O}$ die Abbildung durch $\varphi_{\mathcal{O}}(x) := \infty$ definiert.*
- *Ist $\varphi : K \to L \cup \{\infty\}$ eine Stelle, so ist $\mathcal{O}_\varphi := \{x \in K \mid \varphi(x) \neq \infty\}$ ein*

Bewertungsring mit maximalem Ideal $\mathcal{M}_\varphi = \{x \in K \mid \varphi(x) = 0\}$.

Seien nun v und v' zwei Bewertungen von K mit den Wertegruppen Γ und Γ'; weiter seien $\varphi : K \to L \cup \{\infty\}$ und $\varphi' : K \to L' \cup \{\infty\}$ zwei Stellen. Definiert man nun eine Äquivalenzrelation auf den verschiedenen Bewertungen des Körpers K durch

$$v \sim v' :\Longleftrightarrow \quad \text{es ex. ein Ordnungsisomorphismus } \delta : \Gamma \cong \Gamma' \text{ mit } v' = \delta \circ v,$$

und eine Äquivalenzrelation auf den verschiedenen Stellen des Körpers K durch

$$\varphi \sim \varphi' :\Longleftrightarrow \quad \text{es ex. ein Körperisomorphismus } \sigma : L \cong L' \text{ mit } \varphi' = \sigma \circ \varphi,$$

so liefert Theorem 1.17 eine Bijektion zwischen den Bewertungsringen, den Äquivalenzklassen von Bewertungen und den Äquivalenzklassen von Stellen eines Körpers. Der Einfachheit halber werde ich im folgenden von Bewertungen bzw. Stellen sprechen statt von Äquivalenzklassen von Bewertungen bzw. Stellen[5]. Zum Beispiel heißt „es gibt genau eine verzweigte Bewertung“ , daß es genau eine Äquivalenzklasse von Bewertungen gibt, in der alle Bewertungen verzweigen. Die Begriffe Bewertung, Bewertungsring und Stelle sind dann austauschbar; ich werde sie nach Lust und Laune verwenden. Ist zum Beispiel $\mathcal{O}$ der zur Bewertung v gehörende Bewertungsring, so ist $K_\mathcal{O} = K_v$ der Restklassenkörper der Bewertung.

1.2.2 Fortsetzungen von Bewertungen

Es sei $L \supseteq K$ eine Körpererweiterung. Eine Bewertung w auf L heißt **Fortsetzung der Bewertung v auf K** (kurz: $(L, w)/(K, v)$), falls $w|_K = v$ ist; für die zugehörige Stelle gilt dann entsprechend $\varphi_w|_K = \varphi_v$. In diesem Fall ist $\mathcal{O}_v = \mathcal{O}_w \cap K$, $\mathcal{O}_v^\times = \mathcal{O}_w^\times \cap K$ und $\mathcal{M}_v = \mathcal{M}_w \cap K$. Weiter ist $\Gamma_v \leq \Gamma_w$, und die Abbildung $\varphi : K_v \hookrightarrow L_w$, $x + \mathcal{M}_v \mapsto x + \mathcal{M}_w$ zwischen den beiden Restklassenkörpern ist eine Injektion; fortan werde ich daher ohne Einschränkung $K_v \subseteq L_w$ annehmen. Es gilt das folgende

Theorem 1.18 (Fortsetzungssatz von Chevalley). *Sei K ein Körper und $R \subseteq K$ ein Teilring mit 1; weiter sei $\mathcal{A} \subsetneq R$ ein echtes Ideal von R. Dann gibt es einen Bewertungsring $\mathcal{O}$ von K mit maximalem Ideal $\mathcal{M}$, so daß $R \subseteq \mathcal{O}$ und $\mathcal{A} \subseteq \mathcal{M}$ gilt.*

Beweis: siehe [En, Korollar 9.7]

Korollar 1.19. *Jede Bewertung hat Fortsetzungen auf beliebige Oberkörper.*

Sei $(L, w)/(K, v)$ gegeben. Dann heißt $e = e(w/v) := [\Gamma_w : \Gamma_v]$ **Verzweigungsindex** von w/v; weiter heißt $f = f(w/v) := [L_w : K_v]$ der **Trägheitsgrad** von w/v.

[5] Dies ist möglich, da alle späteren Aussagen über Verzweigung, Trägheit usw. unabhängig vom gewählten Repräsentanten einer Äquivalenzklasse sind.

Ist $(L,w)/(K,v)$, so gilt die **fundamentale Ungleichung**

$$e \cdot f \leq [L:K].$$

Die Bewertung v **verzweigt von** K **nach** L, wenn sie eine Fortsetzung auf L mit Verzweigungsgrad größer 1 besitzt. Gilt für alle endlichen Teilerweiterungen L_0 von $K \subseteq L$ jeweils $[L_0 : K] = f(w|_{L_0}, v)$, so heißt die Erweiterung $(L,w)/(K,v)$ **träge**; gilt entsprechend immer $[L_0 : K] = e$, so heißt die Erweiterung $(L,w)/(K,v)$ **rein verzweigt**. Gilt $e = f = 1$, so heißt die Erweiterung $(L,w)/(K,v)$ **unmittelbar**. Eine Körpererweiterung $L \supseteq K$ heißt **verzweigt**, wenn es eine Bewertung v auf K gibt, die nach L verzweigt.

Die folgende Tatsache werden wir in Abschnitt 4.1 direkt mehrfach benutzen:

Bemerkung: Ist $\mathcal{O}$ ein Bewertungsring von K, so ist $\mathcal{O}$ ganz abgeschlossen in K.

Im folgenden interessieren wir uns vornehmlich für Fortsetzungen $(L,w)/(K,v)$, bei denen $L \supseteq K$ eine Galoiserweiterung ist. Eine wichtige Feststellung ist dann der sogenannte Konjugiertensatz:

Theorem 1.20 (Konjugiertensatz). *Ist $L \supseteq K$ eine Galoiserweiterung und ist v eine Bewertung von K, so sind alle Fortsetzungen von v auf L über K konjugiert.*

Beweis: siehe [En, Korollar 14.3]

Um Galoiserweiterungen bewerteter Körper analysieren zu können, sind einige Begriffe notwendig:

Definition 1.21. *$(L,w)/(K,v)$ sei eine Galoiserweiterung bewerteter Körper mit Galoisgruppe $G := \mathrm{Gal}(L/K)$.*

1) *$Z = Z(w/v) := \{\sigma \in G \mid$ für alle $x \in \mathcal{O}_w$ ist $\sigma(x) - x \in \mathcal{O}_w\}$ heißt* **Zerlegungsgruppe** *von $(L,w)/(K,v)$; weiter heißt $L_Z := \mathrm{Fix}(Z)$* **Zerlegungskörper** *von $(L,w)/(K,v)$.*
2) *$T = T(w/v) := \{\sigma \in G \mid$ für alle $x \in \mathcal{O}_w$ ist $\sigma(x) - x \in \mathcal{M}_w\}$ heißt* **Trägheitsgruppe** *von $(L,w)/(K,v)$; weiter heißt $L_T := \mathrm{Fix}(T)$* **Trägheitskörper** *von $(L,w)/(K,v)$.*
3) *$V = V(w/v) := \{\sigma \in G \mid$ für alle $x \in \mathcal{O}_w$ ist $\sigma(x) - x \in x\mathcal{M}_w\}$ heißt* **Verzweigungsgruppe** *von $(L,w)/(K,v)$; weiter heißt $L_V := \mathrm{Fix}(V)$* **Verzweigungskörper** *von $(L,w)/(K,v)$.*

Im nächsten Satz sind die wichtigsten Eigenschaften von Z, T und V zusammengefaßt. Ich beschränke mich hier auf den Fall einer endlichen Galoiserweiterung $L \supseteq K$; für unendliche Erweiterungen ist die Charakterisierung der Erweiterung $(L_V, w|_{L_V})/(L_T, w|_{L_T})$ etwas komplizierter. Für eine abelsche Gruppe H und eine Primzahl p sei $\frac{1}{p'^\infty}H$ die divisible Hülle von H bzgl. allen Primzahlen $p' \neq p$. Weiter sei $H_{p'}$ die maximale p-freie Untergruppe von H, also $H_{p'} := \{h \in H \mid \mathrm{ord}(h)$ teilerfremd zu $p\}$.

Theorem 1.22. *$(L, w)/(K, v)$ sei eine Galoiserweiterung bewerteter Körper der Charakteristik p mit Galoisgruppe $G := \mathrm{Gal}(L/K)$. Es sei $w_Z = w|_{L_Z}$, $w_T = w|_{L_T}$ und $w_V = w|_{L_V}$; weiter seien $L_{Z_{w_Z}}$, $L_{T_{w_T}}$ und $L_{V_{w_V}}$ die entsprechenden Restklassenkörper und Γ_Z, Γ_T und Γ_V die entsprechenden Wertegruppen.*

1) Z ist eine abgeschlossene Untergruppe von G. Weiter ist w die einzige Fortsetzung von w_Z auf L; v hat genau $[G : Z] = [L_Z : K]$ viele verschiedene Fortsetzungen auf L. Die Fortsetzung $(L_Z, w_Z)/(K, v)$ ist unmittelbar.

2) T ist ein abgeschlossener Normalteiler von Z. Die Erweiterung $(L_T, w_T)/(L_Z, w_Z)$ ist träge; für den Restklassenkörper gilt $L_{T_{w_T}} = L_w \cap (K_v)^s$.

3) V ist ein abgeschlossener Normalteiler von T; weiter ist V die (einzige) p-Sylowgruppe von T (ist insbesondere $p = 0$, so ist $V = \{1\}$). Die Erweiterung $(L_V, w_V)/(L_T, w_T)$ ist rein verzweigt. Es ist $\Gamma_V = \frac{1}{p'^\infty}\Gamma_v \cap \Gamma_w$ und $T/V \cong (\Gamma_w/\Gamma_v)_{p'}$.

4) Die Erweiterung der Restklassenkörper $L_w \supseteq L_{V_{w_V}} = L_w \cap (K_v)^s$ ist rein inseparabel; der Verzweigungsgrad der Erweiterung $(L, w)/(L_V, w_V)$ ist eine p-Potenz.

Beweis: siehe [En, Kapitel 3]. Das folgende Bild gibt eine Übersicht über die Ergebnisse aus Theorem 1.22:

$$
\begin{tikzcd}
& \text{Galois-gruppe} & \text{Körper} & \text{Werte-gruppe} & \text{Restklassen-körper} \\
& \{1\} \arrow[r, dash, dashed] \arrow[d, dash] & L \arrow[r, dash, dashed] \arrow[d, dash] \arrow[dr, phantom, "p\text{-Potenz}"] & \Gamma_w \arrow[r, dash, dashed] \arrow[d, dash] \arrow[dr, phantom, "\text{rein inseparabel}"] & L_w \arrow[d, dash] \\
p\text{-Sylow-gruppe} & V \arrow[r, dash, dashed] \arrow[d, dash, "T/V \cong (\Gamma_w/\Gamma_v)_{p'}"'] & L_V \arrow[r, dash, dashed] \arrow[d, dash] \arrow[dr, phantom, "\text{rein verzweigt}"] & \Gamma_V = \frac{1}{p'^\infty}\Gamma_v \cap \Gamma_w \arrow[r, dash, dashed] \arrow[d, dash] & L_{V_{w_V}} = L_w \cap K_v^s \arrow[d, equal] \\
& T \arrow[r, dash, dashed] \arrow[d, dash] & L_T \arrow[r, dash, dashed] \arrow[d, dash] \arrow[dr, phantom, "\text{träge}"] & \Gamma_T = \Gamma_v \arrow[r, dash, dashed] \arrow[d, equal] & L_{T_{w_T}} = L_w \cap K_v^s \arrow[d, dash] \\
& Z \arrow[r, dash, dashed] \arrow[d, dash] & L_Z \arrow[r, dash, dashed] \arrow[d, dash] \arrow[dr, phantom, "\text{unmittelbar}"] & \Gamma_Z = \Gamma_v \arrow[r, dash, dashed] \arrow[d, equal] & L_{Z_{w_Z}} = K_v \arrow[d, equal] \\
& G \arrow[r, dash, dashed] & K \arrow[r, dash, dashed] & \Gamma_v \arrow[r, dash, dashed] & K_v
\end{tikzcd}
$$

Aus Theorem 1.22 erhält man nun leicht das folgende

Korollar 1.23. *Es sei $(L, w)/(K, v)$ eine endliche Galoiserweiterung mit $[L : K] = n$; weiter sei r die Anzahl der Fortsetzungen von v auf L, e der Verzweigungsindex und f der Trägheitsgrad von $(L, w)/(K, v)$. Dann existiert ein $k \in \mathbb{N}$, so daß für*

$$d := \begin{cases} p^k & \textit{falls } \mathrm{char}(K_v) = p \textit{ für ein } p > 0 \\ 1 & \textit{sonst} \end{cases}$$

gilt:

$$n = r \cdot d \cdot e \cdot f$$

Die p-Potenz $d = d(w/v)$ heißt **Defekt** von $(L, w)/(K, v)$.

Ebenfalls leicht zu zeigen ist der folgende Sachverhalt:

Lemma 1.24. *Sei $(L, w)/(M, u)/(K, v)$ ein Turm von Galoiserweiterungen bewerteter Körper. Dann bildet die Restriktionsabbildung*

$$res : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(M/K)$$

die Zerlegungs-, Trägheits- und Verzweigungsgruppe von w/v auf die von u/v ab. Sind T_L und T_M die Trägheitsgruppen von $(L, w)/(K, v)$ und $(M, u)/(K, v)$, so ist $\mathrm{Fix}(T_M) = \mathrm{Fix}(T_L) \cap M$*; entsprechendes gilt für Z und V.*

Lemma 1.25. *Sei $(L, w)/(M, u)/(K, v)$ ein Turm von Galoiserweiterungen bewerteter Körper; $(M, u)/(K, v)$ sei träge, weiter sei die Restklassenkörpererweiterung $M_u \supseteq K_v$ separabel.*
Dann ist M im Fixkörper L_T der Trägheitsgruppe T von $(L, w)/(K, v)$ enthalten.

Beweis: Da $(M, u)/(K, v)$ träge ist, gilt $n := [M : K] = f(u/v)$. Also ist $e(u/v) = r(u/v) = d(u/v) = 1$, für die Trägheitsgruppe T_M von $(M, u)/(K, v)$ gilt also $T_M = 1$. Demnach gilt $M = \mathrm{Fix}(T_M)$; wegen Lemma 1.24 ist M dann in L_T enthalten. ■

Das folgende Theorem liefert ein notwendiges Kriterium dafür, ob eine Erweiterung $L \supseteq K$ verzweigt:

Theorem 1.26. *(K, v) sei ein bewerteter Körper und $f(X) \in \mathcal{O}_v[X]$ sei separabel und normiert. Es sei L der Zerfällungskörper von f über K und $\alpha_1, \ldots \alpha_n$ seien die Nullstellen von f, das heißt es ist $f = \prod_{i=1}^n (X - \alpha_i)$. Weiter sei $D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$ die Diskriminante von f.*
Ist $L \supseteq K$ verzweigt, so ist $D(f) \in \mathcal{M}_v$.

Beweis: Ist L/K verzweigt, so gibt es eine verzweigte Fortsetzung w von v auf L. Es sei T die Trägheitsgruppe von $\mathrm{Gal}(L/K)$ bezüglich w/v. Da w/v verzweigt ist, existiert ein $\sigma \in T \setminus \{1\}$. Dieses σ bewegt mindestens eine Nullstelle von f, es sei etwa $\sigma(\alpha_i) = \alpha_j \neq \alpha_i$. Da $\mathcal{O}_w$ ganz abgeschlossen in L ist, liegen alle α_i in $\mathcal{O}_w[X]$. Nach Definition von T ist also $\sigma(\alpha_i) - \alpha_i = \alpha_j - \alpha_i \in \mathcal{M}_w$, das heißt auch $D(f)$ liegt in $\mathcal{M}_w$. Weiter liegt $D(f)$ als symmetrische Funktion in den Wurzeln von f in K, also ist $D(f) \in \mathcal{M}_w \cap K = \mathcal{M}_v$. ■

1.2.3 Bewertungen von Funktionenkörpern

Es sei F ein **rationaler Funktionenkörper** über K, also $F = K(t)$ für ein über K transzendentes Element t. Wir betrachten die folgenden auf K trivialen Bewertungen von F (bzw. die zugehörigen Stellen, die auf K die Identität sind):

- Die **$(t-a)$-adische Bewertung** bzw. die **Stelle bei $a \in K^{\mathrm{a}}$**: Es sei $p(t) := \mathrm{Irr}(a, K)$ das Minimalpolynom von $a \in K^{\mathrm{a}}$. Dann ist
$$\mathcal{O}_{p(t)} = \mathcal{O}_a := \left\{ \frac{f(t)}{g(t)} \middle| f(t), g(t) \in K[t], p(t) \nmid g(t) \right\}$$
ein Bewertungsring von $K(t)$, das zugehörige maximale Ideal ist
$$\mathcal{M}_{p(t)} = \mathcal{M}_a = \left\{ \frac{f(t)}{g(t)} \middle| f(t), g(t) \in K[t], p(t) | f(t), p(t) \nmid g(t) \right\}.$$
Für die zugehörige Bewertung $v_a : F(t) \to \mathbb{Z} \cup \{\infty\}$ gilt $v_a(p(t)^r \frac{f(t)}{g(t)}) = r$ für alle $f, g \in F[t]$, die beide nicht durch p teilbar sind. Für die zugehörige Stelle $\varphi_a : K(t) \to K^{\mathrm{a}} \cup \{\infty\}$ erhält man
$$\varphi_a \left(\frac{f(t)}{g(t)} \right) = \frac{f(a)}{g(a)},$$
wobei $\frac{f(a)}{g(a)} = \infty$ ist, falls g öfter von p geteilt wird als f. Für den Restklassenkörper gilt $K(t)_{v_a} \cong K[t]/\langle p(t) \rangle$.
Ist insbesondere $a \in K$, also $p(t) = t - a$, so ist der Restklassenkörper $K(t)_{v_a} \cong K$.
- Die sog. **Gradbewertung** bzw. die **Stelle bei ∞**: Der Ring
$$\mathcal{O}_\infty := \left\{ \frac{f(t)}{g(t)} \middle| f(t), g(t) \in K[t], \deg(f) \leq \deg(g) \right\}$$
ist ein Bewertungsring von $K(t)$, das zugehörige maximale Ideal ist
$$\mathcal{M}_\infty = \left\{ \frac{f(t)}{g(t)} \middle| f(t), g(t) \in K[t], \deg(f) < \deg(g) \right\}.$$
Für die zugehörige Bewertung $v_\infty : F(t) \to \mathbb{Z} \cup \{\infty\}$ gilt $v_\infty(\frac{f(t)}{g(t)}) = \deg(g) - \deg(f)$. Für die zugehörige Stelle $\varphi_\infty : K(t) \to K \cup \{\infty\}$ gilt
$$\varphi_\infty \left(\frac{a_m t^m + \cdots + a_0}{b_n t^n + \cdots + b_0} \right) = \begin{cases} \infty & \text{, falls } m > n \\ \frac{a_m}{b_n} & \text{, falls } m = n \\ 0 & \text{, falls } m < n \end{cases}$$
Der Restklassenkörper ist $K(t)_{v_\infty} \cong K$.

K läßt sich also in die Restklassenkörper von $K(t)$ bzgl. aller $(t-a)$-adischen Bewertungen, wie auch bzgl. der Gradbewertung, einbetten. Insbesondere hat der Restklassenkörper also die gleiche Charakteristik wie K. Die oben betrachteten Bewertungen sind schon alle auf K trivialen Bewertungen von $K(t)$:

Theorem 1.27. *Die Bewertungen v_∞ und v_a für $a \in K^a$ sind die einzigen auf $K(t)$ nicht-trivialen Bewertungen, die auf K trivial sind.*

BEWEIS: siehe [St, Theorem I.2.2]

Wir werden in Abschnitt 4.1 noch die folgenden Ergebnisse über Bewertungen von endlichen algebraischen Erweiterungen von rationalen Funktionenkörpern benötigen:

Lemma 1.28. *Es sei F ein rationaler Funktionenkörper über K in einer Variablen. L sei eine endliche algebraische Erweiterung von F. Weiter sei v eine Bewertung von L, die auf K trivial ist (v ist also eine Fortsetzung der Gradbewertung oder einer der $(t-a)$-adischen Bewertungen von F auf L). Dann ist $L \cap K^a \subseteq \mathcal{O}_v$ und $L \cap K^a \cap \mathcal{M}_v = \{0\}$. Also läßt sich $L \cap K^a$ in den Restklassenkörper L_v einbetten.*

BEWEIS: siehe [St, Lemma II.1.5.c]

Hieraus erhält man insbesondere:

Lemma 1.29. *Es sei $K' \supseteq K$ eine endliche algebraische Erweiterung von K und t sei transzendent über K. Weiter sei v eine auf K triviale Bewertung von $K(t)$ mit $K(t)_v = K$. Dann sind alle Bewertungsfortsetzungen $(K'(t), w)/(K(t), v)$ träge.*

BEWEIS: Es sei $[K' : K] = n$. Nach Lemma 1.28 läßt sich dann $K'(t) \cap K^{\mathrm{a}} = K'$ in den Restklassenkörper $K'(t)_w$ einer beliebigen Bewertungsfortsetzung w von v auf $K'(t)$ einbetten. Also ist $[K'(t)_w : K(t)_v] \geq [K' : K] = n$; es gilt also $f = n$. Wegen Korollar 1.23 ist $(K'(t), w)/(K(t), v)$ dann träge. ■

1.3 Algebraische Geometrie

Die folgenden beiden Abschnitte orientieren sich an der Darstellung in [FJ, Kapitel 9.4, 9.5]. Eine ausführlichere Einführung findet man in [La2, Kapitel II, III]; in [Bou, Anand Pillay: Model theory of algebraically closed fields, Abschnitte 1-3] wird vermehrt auf die modelltheoretischen Hintergründe eingegangen.

1.3.1 Algebraische Mengen

Sei K ein Körper und $\mathfrak{a}_0 \subseteq K[X_1, \ldots, X_n]$. Weiter sei Ω ein Universalbereich wie in Abschnitt 1.1.1 beschrieben. Dann heißt

$$V(\mathfrak{a}_0) := \{\bar{x} \in \Omega^n \mid f(\bar{x}) = 0 \text{ für alle } f \in \mathfrak{a}_0\}$$

die **zu $\mathfrak{a}_0$ gehörende K-algebraische Menge**. Die Elemente von $V(\mathfrak{a}_0)$ heißen die **rationalen Punkte** von $V(\mathfrak{a}_0)$; ist $L \supseteq K$, so heißt ein Tupel $\bar{l} \in L$ mit $f(\bar{l}) = 0$ für alle $f \in \mathfrak{a}_0$ ein **L-rationaler Punkt** von $V(\mathfrak{a}_0)$. Ist $\mathfrak{a}$ das von $\mathfrak{a}_0$ erzeugte Ideal in $K[\bar{X}]$, so gilt $V(\mathfrak{a}) = V(\mathfrak{a}_0)$.

Die Komplemente der K-algebraischen Mengen bilden eine Topologie auf Ω^n, die ***K*-Zariski-Topologie**; die K-algebraischen Mengen sind also gerade die K-abgeschlossenen Mengen.
Umgekehrt kann man jeder Teilmenge $A \subseteq \Omega^n$ ein Ideal aus $K[\bar{X}]$ zuordnen, das sogenannte Verschwindungsideal von A:

$$I_K(A) := \{f \in K[\bar{X}] \mid f(\bar{x}) = 0 \text{ für alle } \bar{x} \in A\}.$$

Es sei $\mathfrak{a}$ ein Ideal und $\sqrt{\mathfrak{a}} := \{f \in K[\bar{X}] \mid \text{es existiert ein } r \in \mathbb{N} \text{ mit } f^r \in \mathfrak{a}\}$ das **Radikalideal** von $\mathfrak{a}$. Primideale sind stets Radikalideale. Für die Funktionen I_K und V gilt:

- $I_K(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$
- Ist $A \subseteq \Omega^n$, so ist $V(I_K(A)) = \bar{A}$, der ***K*-Zariski-Abschluß** von A.

Eine nichtleere K-algebraische Menge V heißt ***K*-irreduzibel** oder eine ***K*-Varietät**, wenn sie sich nicht als echte Vereinigung von K-algebraischen Mengen A und B schreiben läßt (wenn also nicht $V = A \cup B$ mit $A \not\subseteq B$ und $B \not\subseteq A$ ist). V ist genau dann K-irreduzibel, wenn $\mathfrak{p} = I_K(V)$ ein Primideal in $K[\bar{X}]$ ist. In diesem Fall ist $K[\bar{X}]/\mathfrak{p}$ ein Integritätsbereich, der Quotientenkörper $\mathrm{Quot}(K[\bar{X}]/\mathfrak{p})$ läßt sich in Ω einbetten. Ein Bild von $X_1 + \mathfrak{p}, \ldots, X_n + \mathfrak{p}$ unter einer solchen Einbettung heißt **generischer Punkt** von $\mathfrak{p}$ beziehungsweise von V. Wie man leicht zeigt, ist $\bar{x} \in \Omega$ genau dann ein generischer Punkt von V, wenn $I_K(V) = I_K(\{\bar{x}\})$ gilt. Ist $\bar{x}$ ein generischer Punkt von V, so heißt $K(\bar{x})$ **Funktionenkörper von *V***. Ist $\bar{x} \in \Omega$ gegeben, so ist $I_K(\{\bar{x}\})$ ein Primideal und $\bar{x}$ ist generischer Punkt von $I_K(\{\bar{x}\})$. Ist V eine K-Varietät und $\bar{x}$ ein generischer Punkt von V, so heißt der Transzendenzgrad von $K(\bar{x})$ über K die ***K*-Dimension von *V***.
Ist beispielsweise $V = V(X^2 + Y^2 - 1)$, ist t transzendent über K und ist s so, daß $s^2 = t^2 - 1$ gilt, so ist (t, s) ein generischer Punkt von V. Dann ist $K(t, s)$ ein Funktionenkörper von V über K, und es ist $\dim(V) = 1$.
Eine K-Varietät der Dimension 1 heißt ***K*-Kurve**; ist $V \subseteq \mathbb{A}^2$, so ist V eine **ebene *K*-Kurve**. Jede ebene K-Kurve V hat die Form $V = V(\{f\})$ für ein nichtkonstantes irreduzibles Polynom $f(X, Y) \in K[X, Y]$.

1.3.2 Varietäten

V sei eine K-Varietät, etwa $V = V(f_1, \ldots f_n)$[6] mit $f_i \in K[\bar{X}]$. Ist L ein beliebiger Oberkörper von K, so läßt sich V auch als L-algebraische Menge auffassen. V ist jedoch nicht notwendigerweise L-irreduzibel: Ist zum Beispiel $V = V(f(x)) = \{a_1, \ldots a_n\}$ für ein separables irreduzibles Polynom f von Grad $n > 1$, so zerfällt V als K^{a}-algebraische Menge in die Irreduzibilitätskomponenten $\{a_1\}, \ldots, \{a_n\}$. Eine K-Varietät V, die auch K^{a}-irreduzibel ist, heißt **absolut irreduzibel** oder kurz **irreduzibel** oder eine **Varietät**.

[6] $K[\bar{X}]$ ist noethersch, das heißt jedes Ideal ist endlich erzeugt.

Sei V eine absolut irreduzible K-Varietät, sei $L \supseteq K$. Das von V in $L[\bar{X}]$ erzeugte Ideal $I_L(V)$ wird nicht unbedingt von Polynomen aus $K[\bar{X}]$ erzeugt: Ist etwa $\mathrm{char}(K) = p$ und $V = V(x^p - a)$ für ein $a \in K$, dessen p-te Wurzel α nicht in K liegt, so besteht V nur aus dem einen Punkt α, ist also irreduzibel. Trotzdem ist das von $x^p - a$ in $K^{\mathrm{a}}[\bar{X}]$ erzeugte Ideal ein echtes Unterideal von $I_{K^{\mathrm{a}}}(V) = (x-\alpha)_{K^{\mathrm{a}}[\bar{X}]}$.
Sei $L \subseteq K^{\mathrm{a}}$. Eine irreduzible K-Varietät V heißt **über L definiert**, wenn $I_{K^{\mathrm{a}}}(V)$ von Polynomen aus $L[\bar{X}]$ erzeugt wird, wenn also $I_{K^{\mathrm{a}}}(V) = (I_L(V))_{K^{\mathrm{a}}[\bar{X}]}$ gilt; L heißt dann **Definitionskörper** von V [7]. Es gilt:

Theorem 1.30 (Weil). *Jede irreduzible K-Varietät hat einen minimalen Definitionskörper.*

Beweis: siehe [La2, Kapitel III, Abschnitt 2, Theorem 7]

Der folgende Satz gibt Auskunft darüber, wann eine K-Varietät über K definierbar und absolut irreduzibel ist:

Theorem 1.31. *Sei V eine K-Varietät mit generischem Punkt $\bar{x}$. Dann ist V genau dann eine über K definierte Varietät, wenn die Erweiterung $K(\bar{x}) \supseteq K$ regulär ist.*

Beweis: siehe [FJ, Korollar 9.23]

An dieser Stelle hat sich der Leser eine erste Stärkung verdient. Mein Vorschlag:

BIRNENPIZZA MIT GORGONZOLA

Vorspeise für 6 Personen

Eine Rolle Blätterteig (aus dem Kühlregal) auf einem Backblech ausbreiten und mit Birnenschnitzen von ca. 4 Birnen belegen. 100-150g Gorgonzola auf der Pizza verteilen, mit 100g grob gehackten Walnüssen bestreuen. Bei 200° C im vorgeheizten Backofen goldbraun backen. Dazu paßt ein Kopfsalat mit Ruccola und Tomaten.

[7] (siehe [Bou]) Vorsicht: Diese Definition unterscheidet sich vom modelltheoretischen Begriff der Definierbarkeit einer Varietät! Tatsächlich besteht zwischen den Begriffen der folgende Zusammenhang: Eine K-Varietät ist natürlich immer im modelltheoretischen Sinne über K definierbar. Eine K-Varietät V ist genau dann im modelltheoretischen Sinne über einem Körper L definierbar, wenn sie im algebraischen Sinne über L^{1/p^∞} definiert ist. Der minimale Definitionskörper (zu dessen Existenz siehe 1.30) einer K-Varietät V ist also immer in K^{1/p^∞} enthalten. Für perfekte Körper fallen die beiden Begriffe zusammen.

2 Modelltheoretische Grundlagen

Dieses Kapitel enthält nur einige ausgewählte modelltheoretische Ergebnisse, die für die vorliegende Arbeit notwendig sind. Alle nicht näher zitierten Ergebnisse und eine umfassende Einführung in die Modelltheorie findet man beispielsweise in [CK], [Poi1] oder in [Ho].

2.1 Bezeichnungen und Konventionen

Alle modelltheoretischen Betrachtungen in dieser Arbeit basieren auf der Prädikatenlogik erster Stufe mit Gleichheit. Im folgenden sei L eine Sprache und T eine vollständige L-Theorie.

Je nach Kontext bezeichnen $A, B, \dots$ Mengen oder mengengroße Modelle. Will ich besonders hervorheben, daß es sich um Strukturen handelt, so schreibe ich $\mathcal{A}$ und $\mathcal{B}$; A und B sind dann die Träger von $\mathcal{A}$ und $\mathcal{B}$. Weiter sind $\bar{a}, \bar{b}, \dots$ (eventuell unendliche) Tupel; $a, b, \dots$ können Elemente oder endliche Tupel sein. Für ein Tupel $\bar{a}$ der Länge κ schreibe ich kurz $\bar{a} \in A$ anstelle von $\bar{a} \in A^\kappa$.
Ist A eine Menge, so ist $\mathrm{L}(A)$ die Erweiterung von L, die durch Hinzufügen von neuen Konstantensymbolen für die Elemente aus A entsteht. Ist $\psi(x, \bar{a})$ eine Formel mit Parametern $\bar{a} \in A$, so schreibe ich, falls es der Kontext erlaubt, $\psi(x, A)$, ohne die Parameter aus A genau anzugeben. Für Mengen A, B schreibe ich kurz $\mathrm{tp}(A/B)$ und meine damit $\mathrm{tp}((a_i)_{i\in I}/(b_j)_{j\in J})$ für Aufzählungen $(a_i)_{i\in I}$ und $(b_j)_{j\in J}$ von A und B. Genauso schreibe ich $\mathrm{tp}(A/B) \vdash \varphi(\bar{x}, B)$, ohne genauer anzugeben, mit welchem Tupel $\bar{a} \in A$ die Variablen $\bar{x}$ belegt werden sollen, wenn dies aus dem Zusammenhang klar ist. $\psi(x, \bar{b}) \in \mathrm{L}(A\bar{b})$ soll bedeuten, daß $\psi(x, y) \in \mathrm{L}(A)$ ist, $\psi(x, \bar{b})$ enthält also keine „versteckten" Parameter aus $\bar{b}$.
Im folgenden sei $\psi(x)^M$ die Erfüllungsmenge von ψ im Modell M. Es bezeichne $\mathrm{acl}(A)$ den algebraischen und $\mathrm{dcl}(A)$ den definierbaren Abschluß von A.

Es sei $\mathbb{C}$ ein **Monstermodell**[8] von T: Sein Universum ist eine echte Klasse, und es hat die folgenden Eigenschaften:

M1 Jedes (Mengen-)Modell von T läßt sich elementar in $\mathbb{C}$ einbetten.
M2 Sind N und M (Mengen-)Modelle von T mit $N \prec M$ und $N \prec \mathbb{C}$, so läßt sich M elementar über N in $\mathbb{C}$ einbetten.
M3 Ist A eine Teilmenge von $\mathbb{C}$, und sind a^I und b^I Folgen aus $\mathbb{C}$ mit $\mathrm{tp}(a^I/A) = \mathrm{tp}(b^I/A)$, so existiert ein Automorphismus f von $\mathbb{C}$ über A mit $f(a^I) = b^I$.

In der Regel kann man das Monstermodell durch eine genügend saturierte und homogene mengengroße Struktur ersetzen. Allerdings werden viele Formulierungen einfacher, wenn man in $\mathbb{C}$ arbeitet. Ein Beispiel:

[8] vergl. Vorlesungsskript zur Vorlesung Stabilitätstheorie, gehalten im Wintersemester 1988/1989 von M. Ziegler an der Albert-Ludwigs-Universität Freiburg

Es sei $F \models T$ und $\Phi(x)$ sei eine Menge von Formeln mit Parametern aus F. Arbeiten wir ohne Monstermodell, so ist Φ genau dann in einer elementaren Oberstruktur von F erfüllbar, wenn die Formelmenge Φ zusammen mit dem elementaren Diagramm von F erfüllbar ist. Arbeiten wir dagegen mit dem Monstermodell, so können wir wegen M1 ohne Einschränkung annehmen, daß $F \prec \mathbb{C}$ gilt. Wird nun Φ in $\mathbb{C}$ erfüllt, so gibt es schon eine mengengroße elementare Oberstruktur von F, in der Φ erfüllt wird.

Wir werden uns fortan alle mengengroßen Modelle von T elementar in $\mathbb{C}$ eingebettet vorstellen. Alle Parametermengen seien in $\mathbb{C}$ enthalten. „Erfüllbar“ heißt fortan immer „erfüllbar in $\mathbb{C}$“.

Die mehrsortige Struktur $\mathbb{C}^{\mathrm{eq}}$ entsteht aus $\mathbb{C}$, indem man für jede $\emptyset$-definierbare Äquivalenzrelation E eine neue Sorte für die Äquivalenzklassen von E hinzunimmt. Die Sprache L^{eq} enthalte zusätzlich zu L noch Symbole für die Projektionsabbildungen, die einem Elemententupel seine Äquivalenzklasse zuordnen. Ebenso erhält man für mengengroße Modelle M die Struktur M^{eq}. Es sei T^{eq} die L^{eq}-Theorie von $\mathbb{C}^{\mathrm{eq}}$.

2.2 Existentielle Abgeschlossenheit

Um im Kapitel 3 eine geeignete Charakterisierung der Klasse der PAC-Körper angeben zu können, brauche ich den Begriff der existentiellen Abgeschlossenheit von einer Substruktur $\mathcal{A} \subseteq \mathcal{B}$ in $\mathcal{B}$:
Es sei $\mathcal{A}$ eine L-Struktur, weiter sei $\mathcal{B}$ eine algebraische Oberstruktur von $\mathcal{A}$. $\mathcal{A}$ heißt **existentiell abgeschlossen in $\mathcal{B}$** (kurz: $\mathcal{A} \subseteq_\exists \mathcal{B}$), wenn jede in $\mathcal{B}$ erfüllbare quantorenfreie $\mathrm{L}(A)$-Formel $\varphi(\bar{x}, A)$ auch in $\mathcal{A}$ erfüllbar ist.

Theorem 2.1. *$\mathcal{A} \subseteq \mathcal{B}$ seien L-Strukturen. Dann ist $\mathcal{A}$ genau dann existentiell abgeschlossen in $\mathcal{B}$, wenn eine elementare Oberstruktur $\mathcal{A}^* \succ \mathcal{A}$ existiert mit $\mathcal{B} \subseteq \mathcal{A}^*$.*

Beweis: „$\Rightarrow$“ Seien L-Strukturen $\mathcal{A} \subseteq_\exists \mathcal{B}$ gegeben. Zu zeigen ist die Erfüllbarkeit des quantorenfreien Diagramms $D_{qf}(\mathcal{B})$ von $\mathcal{B}$; hierzu genügt die endliche Erfüllbarkeit von $D_{qf}(\mathcal{B})$ in $\mathcal{A}$. Da $D_{qf}(\mathcal{B})$ gegen Konjunktionen abgeschlossen ist, reicht es zu zeigen, daß jede in $\mathcal{B}$ erfüllbare quantorenfreie $\mathrm{L}(A)$-Formel $\varphi(\bar{x})$ auch in $\mathcal{A}$ erfüllbar ist; dies ist genau die existentielle Abgeschlossenheit von $\mathcal{A}$ in $\mathcal{B}$.
„$\Leftarrow$“ $\varphi(\bar{x}, A)$ sei eine quantorenfreie, in $\mathcal{B}$ erfüllbare Formel. Dann gilt natürlich auch $\mathcal{A}^* \models \exists \bar{x} \varphi(\bar{x}, A)$ und wegen $\mathcal{A} \prec \mathcal{A}^*$ auch $\mathcal{A} \models \exists \bar{x} \varphi(\bar{x}, A)$. ■

L_{Kp} sei die Sprache, die aus den beiden zweistelligen Funktionssymbolen $+$ und $\cdot$ und aus den Konstantensymbolen 0 und 1 besteht. Jeder Körper K läßt sich dann auf natürliche Weise als L_{Kp}-Struktur interpretieren. Sind $K \subseteq L$ zwei Körper, so läßt sich existentielle Abgeschlossenheit von K in L auch algebraisch charakterisieren. Wir benötigen dazu das folgende Lemma:

Lemma 2.2. *Sei K ein Körper, $\varphi(\bar{x})$ sei eine quantorenfreie $L_{Kp}(K)$-Formel. Dann gibt es natürliche Zahlen $d, k_0, \ldots, k_d$ und Polynome $f_{ij}(\bar{X}), g_i(\bar{X}) \in K[\bar{X}]$ $(0 \leq i \leq d, 0 \leq j \leq k_i)$, so daß gilt:*

$$K \vDash \forall \bar{x} \varphi(\bar{x}) \iff K \vDash \forall \bar{x} \bigvee_{i=0}^{d} \left(\bigwedge_{j=0}^{k_i} f_{ij}(\bar{x}) \doteq 0 \wedge \neg g_i(\bar{x}) \doteq 0 \right).$$

Beweis: Nach dem Satz über die disjunktive Normalform ist jede $\mathrm{L}_{\mathrm{Kp}}(K)$-Formel $\varphi(\bar{x})$ äquivalent zu einer Disjunktion von Konjunktionen von Literalen aus $\mathrm{L}_{\mathrm{Kp}}(K)$. In L_{Kp} sind diese Literale gerade polynomiale Gleichungen und Ungleichungen für $\bar{x}$ mit Koeffizienten aus K. In Körpern ist jede dieser (Un-)Gleichungen für ein Polynom $p \in K[\bar{X}]$ logisch äquivalent zu einer Formel der Form $(\neg)p(\bar{x}) = 0$. Schließlich ist für $q_i \in K[\bar{X}]$ die Formel $\bigwedge_{i=0}^{n} \neg q_i(\bar{x}) \doteq 0$ in K äquivalent zu der Formel $\neg \prod_{i=0}^{n} q_i(\bar{x}) \doteq 0$. ∎

Theorem 2.3. *$K \subseteq L$ seien Körper. Dann sind äquivalent:*

1) $K \subseteq_\exists L$

2) Jede K-Varietät mit rationalem Punkt in L hat auch einen rationalen Punkt in K.

Beweis: „$\Leftarrow$" Es sei $\varphi(\bar{x}, \bar{k})$ eine $\mathrm{L}_{\mathrm{Kp}}(K)$-Formel und es gelte $L \vDash \exists \bar{x} \varphi(\bar{x}, \bar{k})$. Nach dem letzten Lemma ist klar, daß man φ ohne Einschränkung von der Form

$$\bigwedge_{j=0}^{k} f_j(\bar{x}) \doteq 0 \wedge \neg g(\bar{x}) \doteq 0$$

mit Polynomen $f_j, g \in K[\bar{X}]$ wählen kann. Sei $\bar{a} \in L$ so, daß $f_j(\bar{a}) = 0$ und $g(\bar{a}) \neq 0$ ist (für $0 \leq j \leq k$). Dann gilt für $b := g(\bar{a})^{-1}$ auch $g(\bar{a}) \cdot b - 1 = 0$.
Sei nun $V := V(I_K(\{\bar{a}, b\}))$; dann ist V eine K-Varietät mit generischem Punkt $(\bar{a}, b)$. Nach Voraussetzung hat V einen rationalen Punkt $(\bar{a}', b')$ in K. Für diesen gilt $f_j(\bar{a}') = 0$ und $g(\bar{a}') \neq 0$, es gilt also $K \vDash \varphi(\bar{a}', \bar{k})$.
„$\Rightarrow$" V sei eine K-Varietät, etwa $V = V(\{f_0, \ldots, f_n\})$ für $f_0, \ldots, f_n \in K[\bar{X}]$. Hat V eine Nullstelle in L, so gilt $L \vDash \exists \bar{x} \bigwedge_{i=0}^{n} f_i(\bar{x}) \doteq 0$, also nach Voraussetzung auch $K \vDash \exists \bar{x} \bigwedge_{i=0}^{n} f_i(\bar{x}) \doteq 0$; also hat V einen K-rationalen Punkt. ∎

2.3 Interpretierbarkeit

Von grundlegender Bedeutung für diese Arbeit ist die Möglichkeit, in einem Körper mittels FO-Formeln Aussagen über endliche Erweiterungen des Körpers und über deren Automorphismengruppen zu treffen. Hierzu benötigen wir das Konzept der Interpretierbarkeit einer Struktur in einer anderen:

Seien $\mathrm{L}_1, \mathrm{L}_2$ zwei Symbolmengen, sei M_1 eine L_1-Struktur und M_2 eine L_2-Struktur. Dann heißt **M_2 in M_1 interpretierbar**, wenn es für ein $n \in \mathbb{N}$ eine mit Parametern aus M_1 definierbare Menge $A \subset M_1^n$ gibt und eine mit Parametern aus M_1 definierbare Äquivalenzrelation E auf A, so daß eine Bijektion $\tau : M_2 \cong A/E$ existiert, für die gilt:

1) Es existiert eine $\mathrm{L}_1(M_1)$-Formel $\varphi_=$, so daß für $a, b \in M_2$ gilt:

$$M_2 \models a = b \iff M_1 \models \varphi_=(\tau(a), \tau(b)).$$

2) Für jede k-stellige Funktion f aus L_2 ($k \geq 0$; wir fassen Konstanten als 0-stellige Funktionen auf) existiert eine $\mathrm{L}_1(M_1)$-Formel φ_f, so daß für alle $a_1, \ldots, a_k, b \in M_2$ gilt:

$$M_2 \models f(a_1, \ldots, a_k) = b \iff M_1 \models \varphi_f(\tau(a_1), \ldots, \tau(a_k), \tau(b)).$$

3) Für jede k-stellige Relation R aus L_2 ($k \geq 1$) existiert eine $\mathrm{L}_1(M_1)$-Formel φ_R, so daß für alle $a_1, \ldots, a_k, b_1, \ldots, b_k \in M_2$ gilt:

$$M_2 \models R(a_1, \ldots, a_k, b_1, \ldots, b_k) \iff M_1 \models \varphi_R(\tau(a_1), \ldots, \tau(a_k), \tau(b_1), \ldots, \tau(b_k)).$$

Im Falle von endlich erzeugten Körpererweiterungen über einem Körper K (und allgemeiner von endlich-dimensionalen K-Algebren) erhält man das folgende Ergebnis:

Theorem 2.4. *Sei K ein Körper und A eine endlich-dimensionale K-Algebra (mit 1; das heißt es ist ohne Einschränkung $K \subseteq A$). Dann gilt:*

1) A ist in K interpretierbar.
2) $\mathrm{Aut}_K(A)$ ist in K interpretierbar.

Beweis: Zu 1): Es sei $b_1, \ldots, b_n$ eine Basis von A über K und $\{e_1, \ldots e_n\}$ sei die Standardbasis des K^n; ohne Einschränkung ist $b_1 = 1$. Dann ist $A \overset{\tau}{\cong} K^n$ durch die Abbildung $b_i \overset{\tau}{\mapsto} e_i$. Gleichheit und Addition sind (jeweils komponentenweise) definierbar; die Konstanten 0 und 1 entsprechen dem Nullelement und dem Element $(1, 0, \ldots, 0) = e_1 \in K^n$. Der Körper K entspricht der definierbaren Menge $\{(k, 0, \ldots, 0) \mid k \in K\} \subseteq K^n$.
Gilt in A für die Multiplikation der Basiselemente $b_i \cdot b_j = \sum_{k=1}^n B_k^{ij} b_k$, so folgt für beliebige Elemente $a = \sum_{i=1}^n \alpha_i b_i$ und $c = \sum_{j=1}^n \gamma_j b_j$ auch

$$a \cdot c = \sum_{k=1}^{n} \Big(\sum_{i,j=1}^{n} \alpha_i \gamma_j B_k^{ij} \Big) b_k.$$

Es gibt also eine Formel $\varphi_\odot(x, y, z, \bar{B})$ mit Parametern $\bar{B} := (B_1^{11}, \ldots, B_n^{nn}) \in K^{n^3}$, so daß für alle $a, b, c \in A$ gilt:

$$A \models a \cdot b = c \iff K \models \varphi_\odot(a^\tau, b^\tau, c^\tau, \bar{B}).$$

Zu 2): Jeder Automorphismus $\varphi \in \mathrm{Aut}_K(A)$ ist insbesondere ein Vektorraumisomorphismus von A über K. Jedem $\varphi \in \mathrm{Aut}_K(A)$ entspricht also bei fester Basis

$\{b_1, \ldots, b_n\}$ eine eindeutig bestimmte invertierbare Matrix $M \in K^{n^2}$. Die Menge aller invertierbaren $n \times n$-Matrizen über K ist (mit Hilfe der Determinante) definierbar; der Verknüpfung von zwei Abbildungen entspricht die (ebenfalls definierbare) Matrizenmultiplikation.
Ein Vektorraumisomorphismus ist genau dann ein Automorphismus von A über K, wenn er zusätzlich mit der Multiplikation auf A verträglich ist und auf K die Identität annimmt; dies ist beides durch $L(\bar{B})$-Formeln definierbar. Also ist $\mathrm{Aut}_K(A)$ isomorph zu der definierbaren Menge

$$\begin{aligned} H := \{\, M \in K^{n\times n} \mid & \text{ der zu } M \text{ gehörige Vektorraumisomorphismus } \varphi_M \text{ ist} \\ & \text{verträglich mit der Multiplikation auf } A,\ \varphi_M|_K = \mathrm{id}_K \} \end{aligned}$$

mit der definierbaren, durch die Matrizenmultiplikation gegebenen Verknüpfung $\circ_H$.
■

Bemerkung: Ist $A = K(\alpha) \supseteq K$ eine separable Körpererweiterung und ist $\mathrm{Irr}(\alpha, K) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, so kann man als K-Basis von $K(\alpha) \subseteq K$ die Elemente $1, \alpha, \ldots, \alpha^{n-1}$ wählen; der zugehörige Vektorraumisomorphismus $\tau_{\bar{a}} : K(\alpha) \to K^n$ bildet dann α^i auf e_{i+1} ab. Die Elemente aus $\bar{B}$ sind dann mit den Parametern $\bar{a}$ definierbar; die Formel $\varphi_{\odot}$ zur Definition der Multiplikation läßt sich also als $\mathrm{L_{Kp}}(\bar{a})$-Formel wählen. Zu jeder $\mathrm{L_{Kp}}(K)$-Formel $\varphi(x_1, \ldots, x_m, \bar{k})$ und zu Elementen $b_1, \ldots, b_m \in K(\alpha)$ existiert dann eine $\mathrm{L_{Kp}}(K)$-Formel $\varphi^{\tau_{\bar{a}}}(\bar{y}_1, \ldots \bar{y}_m, \bar{k}, \bar{a})$ mit

$$K(\alpha) \vDash \varphi(b_1, \ldots b_m, \bar{k}) \iff K \vDash \varphi^{\tau_{\bar{a}}}(\tau_{\bar{a}}(b_1), \ldots, \tau_{\bar{a}}(b_m), \bar{k}, \bar{a}).$$

Ist die Erweiterung eine Galoiserweiterung, so ist auch $\mathrm{Gal}(K(\alpha)/K)$ mit den Parametern $\bar{a}$ interpretierbar.

Zu einem Parametertupel $a_0, \ldots, a_{n-1} \in K$ sei im folgenden $p_{\bar{a}}(\bar{x}) := x^n + a_{n-1}x^{n-1} + \cdots + a_0$ das normierte Polynom n-ten Grades mit den Koeffizienten $a_0, \ldots, a_{n-1}$. Führt Adjunktion einer Nullstelle α von $p_{\bar{a}}$ zu einer Galoiserweiterung von K, so sei $K_{\bar{a}} := K(\alpha)$.

Korollar 2.5. *Sei K ein Körper und G eine Gruppe der Ordnung n. Dann existieren L_{Kp}-Formeln $\varphi_{gal,n}(\bar{x})$ und $\varphi_G(\bar{x})$, so daß für jedes n-Tupel $\bar{a}$ gilt:*

1) $K \vDash \varphi_{gal,n}(\bar{a}) \iff$ Adjunktion einer Nullstelle von $p_{\bar{a}}$ führt zu einer Galoiserweiterung von Grad n von K.
2) $K \vDash \varphi_G(\bar{a}) \iff K \vDash \varphi_{gal,n}(\bar{a})$ und $\mathrm{Gal}(K_{\bar{a}}/K) \cong G$.

Beweis: Zu 1) Adjunktion einer Nullstelle α von $p_{\bar{a}}$ führt genau dann zu einer Galoiserweiterung von K, wenn $p_{\bar{a}}$ irreduzibel und separabel ist, und es in $K_{\bar{a}}$ außerdem n verschiedene Nullstellen von $p_{\bar{a}}$ gibt. Die Irreduzibilität des Polynoms ist leicht formulierbar; die Separabilität läßt sich durch die Formel $\neg\exists\bar{x}(p_{\bar{a}}(\bar{x}) = 0 \wedge p'_{\bar{a}}(\bar{x}) = 0)$ definieren. Wegen der letzten Bemerkung ist klar, daß es eine $L(\bar{a})$-Formel gibt, die

besagt, daß $p_{\bar{a}}(\bar{x})$ in $K_{\bar{a}}$ n verschiedene Nullstellen besitzt; also existiert $\varphi_{\mathrm{gal},n}(\bar{x})$.
Zu 2): Sei $G = \{g_1, \ldots, g_n\}$ und wie im Beweis des letzten Theorems

$$H := \{\ M \in K^{n\times n} \mid \text{der zu } M \text{ gehörige Vektorraumisomorphismus } \varphi_M \text{ ist verträglich mit der Multiplikation auf } A,\ \varphi_{M}|_K = \mathrm{id}_K\}.$$

Die Gruppe G ist genau dann isomorph zu $\mathrm{Gal}(K_{\bar{a}}/K)$, wenn es eine Indizierung $M_1, \ldots, M_n$ der Elemente aus H gibt, so daß $(M_iM_j = M_k \iff g_1 \circ g_j = g_k)$ gilt. Dies ist durch eine $L(\bar{a})$-Formel φ'_G ausdrückbar. Die Konjunktion $\varphi_{\mathrm{gal},n} \wedge \varphi'_G =: \varphi_G$ tut es dann! ■

Lemma 2.6. *Sei K ein Körper und seien $\bar{a}, \bar{b} \in K^n$. Dann existiert eine Formel $\psi_{glErw}\ (x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1})$ mit*

$$K \models \psi_{glErw}(\bar{a}, \bar{b}) \iff K \models \psi_{gal,n}(\bar{a}) \wedge \psi_{gal,n}(\bar{b}) \text{ und es gilt } K_{\bar{a}} = K_{\bar{b}}.$$

Beweis: Gilt $K \models \psi_{\mathrm{gal},n}(\bar{a}) \wedge \psi_{\mathrm{gal},n}(\bar{b})$, so gilt genau dann $K_{\bar{a}} = K_{\bar{b}}$, wenn $p_{\bar{a}}$ eine Nullstelle in $K_{\bar{b}}$ besitzt. Es sei $\tau_{\bar{b}} : K_{\bar{b}} \to K^n$ der in der letzten Bemerkung beschriebene Isomorphismus; ebenso sei zu einer Formel φ die Formel $\varphi^{\tau_{\bar{b}}}$ wie dort angegeben. Dann leistet die Formel

$$\psi_{\mathrm{glErw}}(\bar{a}, \bar{b}) \ = \ (\exists \bar{x} p_{\bar{a}}(x) \doteq 0)^{\tau_{\bar{b}}} \wedge \varphi_{\mathrm{gal},n}(\bar{a}) \wedge \varphi_{\mathrm{gal},n}(\bar{b})$$

das Gewünschte. ■

Hieraus erhalten wir das folgende Korollar:

Korollar 2.7. *Die n-stellige Äquivalenzrelation E mit*

$$\begin{aligned}\bar{a}E\bar{b} :\iff & (K \models \neg\varphi_{gal,n}(\bar{a}) \wedge \neg\varphi_{gal,n}(\bar{b}))\ \text{oder} \\ & (K \models \varphi_{gal,n}(\bar{a}) \wedge \varphi_{gal,n}(\bar{b})\ \text{und}\ K_{\bar{a}} = K_{\bar{b}})\end{aligned}$$

ist durch eine Formel $\chi_{\ddot{A}R,n}(\bar{x}, \bar{y})$ definierbar.

2.4 Einfache Theorien

Es folgt eine kurze Beschreibung einfacher Theorien. Ich übernehme dabei in weiten Teilen die Darstellung aus [Wa, Kapitel 2.2 bis 2.4]; dort finden sich auch eine ausführlichere Einführung und Beweise zu allen nicht genauer zitierten Ergebnissen.

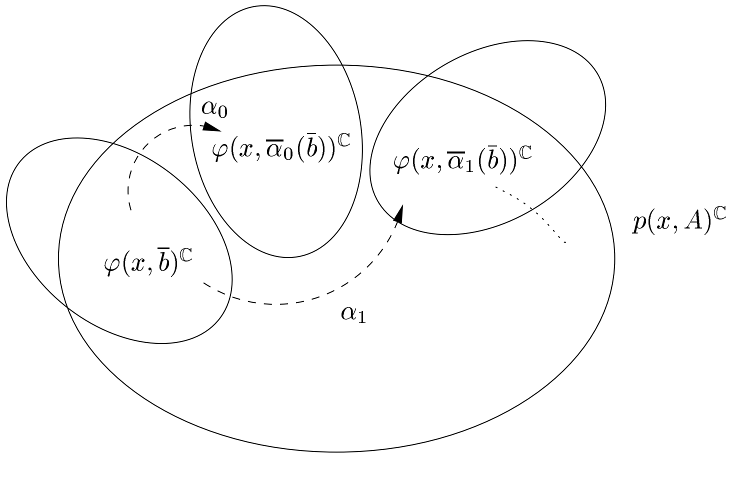
Bevor ich definieren kann, was eine einfache Theorie ist, müssen vorab einige Begriffe geklärt werden:

- Sei $k \in \mathbb{N}$, A sei eine Teilmenge von $\mathbb{C}$ und es sei $\bar{b} \in \mathbb{C}$. Eine Formel $\varphi(\bar{x}, \bar{b})$ ***k*-teilt** über A, wenn es eine Folge $(\bar{b}_i)_{i<\omega}$ in $\mathrm{tp}(\bar{b}/A)$ gibt, so daß die Menge $\{\varphi(\bar{x}, \bar{b}_i) \mid i < \omega\}$ k-inkonsistent ist (das heißt, wenn jede k-elementige Teilmenge von $\{\varphi(\bar{x}, \bar{b}_i) \mid i < \omega\}$ inkonsistent ist). Ein partieller Typ $p(\bar{x})$ k-teilt über A, wenn es eine aus p folgende Formel $\varphi(\bar{x}, \bar{b})$ gibt, die über A k-teilt. Eine Formel/ein Typ **teilt** über A, wenn sie/er für ein $k \in \mathbb{N}$ über A k-teilt.

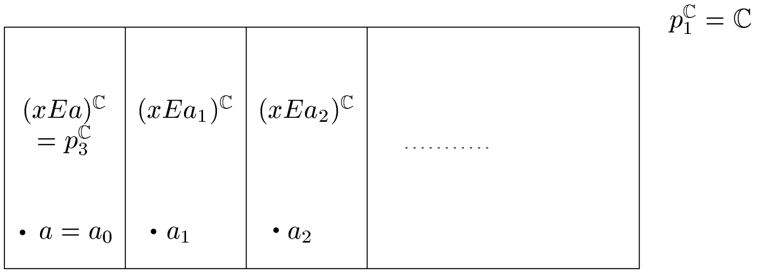
- Ein partieller Typ $p(\bar{x})$ **forkt** über A, wenn es ein $n \in \mathbb{N}$ und Formeln $\varphi_1(\bar{x}, \bar{b}_1)$, $\ldots$, $\varphi_n(\bar{x}, \bar{b}_n)$ gibt, so daß für $1 \leq i \leq n$ jedes $\varphi_i(\bar{x}, \bar{b}_i)$ über A teilt und außerdem $\bigvee_{i=1}^{n} \varphi_i(\bar{x}, \bar{b}_i)$ aus p folgt. Ist $A \subseteq B$ und $p \in S(B)$ forkt nicht über A, so heißt p **nicht-forkende Erweiterung** von $p|_A$.

Die folgende Vorstellung kann zum Verständnis dieser recht technischen Definition beitragen:

Sei $p(x) \in \mathrm{S}(A)$ und $\varphi(x, \bar{b})$ eine mit p konsistente $\mathrm{L}(A\bar{b})$-Formel. φ 2-teilt genau dann über A (das heißt insbesondere, daß $p \cap \{\varphi\}$ eine forkende Erweiterung von p ist), wenn es Automorphismen $\alpha_i \in \mathrm{Aut}_A(\mathbb{C})$, $i < \omega$ gibt, so daß die Mengen $\varphi(x, \bar{\alpha}_i(b))^{\mathbb{C}}$ paarweise disjunkt sind.
p hat also unendlich viele paarweise disjunkte, über A zu $p \cup \{\varphi\}$ konjugierte Fortsetzungen auf $\{b^{\alpha_i} \mid i < \omega\}$; für die Erfüllungsmenge $p(x, a)^{\mathbb{C}}$ heißt dies, daß sie sich durch die Formel $\varphi(x, \bar{b})$ und deren Konjugierte über A in unendlich viele disjunkte Teile zerlegen läßt.



Beispiel: T sei die Theorie einer Äquivalenzrelation E mit unendlich vielen unendlichen Klassen, weiter sei $a \in \mathbb{C}$. Es sei p_1 der einzige Typ in $\mathrm{S}_1(\emptyset)$, weiter seien $p_2 := \{\neg xEa\} \in \mathrm{S}(\{a\})$ und $p_3 := \{xEa\} \in \mathrm{S}(\{a\})$. Sei $a_0 := a$ und seien $(a_i)_{i<\omega}$ Repräsentanten von paarweise verschiedenen Äquivalenzklassen; dann ist $(a_i)_{i<\omega}$ eine Folge in $\mathrm{tp}(a/\emptyset)$. Die Menge $\{xEa_i \mid i < \omega\}$ ist dann 2-inkonsistent, die Formel xEa 2-teilt also über $\emptyset$. Demnach ist p_3 eine forkende Erweiterung von p_1. Die Formel $\neg xEa$ teilt dagegen nicht über $\emptyset$: Ist $(a_i)_{i<\omega}$ eine beliebige Folge in $\mathrm{tp}(a/\emptyset)$, so ist $\{\neg xEa_i \mid i < \omega\}$ konsistent, da in $\mathbb{C}$ klassenviele verschiedene Äquivalenzklassen repräsentiert sind.



Forken und Teilen haben die folgenden Eigenschaften:

- Teilen impliziert Forken.
- (Endlicher Charakter) Ist $A \subseteq B$, so forkt/teilt $\mathrm{tp}(C/B)$ genau dann über A, wenn für ein endliches Tupel $c \in C$ der Typ $\mathrm{tp}(c/B)$ über A forkt/teilt.
- (Existenz nicht-forkender Erweiterungen) Ist $A \subseteq B$ und ist p ein partieller Typ über B, der nicht über A forkt, so gibt es eine Fortsetzung von p zu einem vollständigen Typen über B, der nicht über A forkt.
- Wenn die Formel $\varphi(\bar{x}, \bar{b})$ über A teilt, so kann die Folge $(\bar{b}_i)_{i<\omega}$ in $\mathrm{tp}(\bar{b}/A)$ ohne Einschränkung als Indisceriblefolge gewählt werden.
- (Monotonie) Sei $A \subseteq B \subseteq C$. Forkt $\mathrm{tp}(\bar{a}/C)$ nicht über A, so forkt $\mathrm{tp}(\bar{a}/C)$ nicht über B und $\mathrm{tp}(\bar{a}/B)$ forkt nicht über A.

A, B und C seien Teilmengen von $\mathbb{C}$. A heißt **unabhängig von B über C**, falls $\mathrm{tp}(A/BC)$ nicht über C teilt; kurz $\boldsymbol{A \underset{C}{\perp} B}$.

Definition 2.8. *Eine vollständige Theorie T heißt* **einfach**, *wenn die oben definierte Unabhängigkeitsrelation (im Monstermodell) symmetrisch ist. Eine Struktur M heißt einfach, wenn* $\mathrm{Th}(M)$ *einfach ist.*

Beispiel: E sei ein zweistelliges Relationssymbol und Z der Zufallsgraph; das heißt Z sei ein symmetrischer und irreflexiver Graph, in dem zu je zwei endlichen disjunkten Teilmengen M_1 und M_2 von G immer ein Punkt existiert, der zu allen Punkten aus M_1 in Relation steht und zu allen Punkten aus M_2 nicht. $\mathrm{Th}(Z)$ ist dann ω-kategorisch, hat Quantorenelimination und ist einfach.

Beweis: siehe [Sch, S. 84]

Angenehmerweise muß man in einfachen Theorien nicht mit dem unhandlichen Begriff des Forkens arbeiten, denn es gilt das folgende

Theorem 2.9. *T sei eine einfache Theorie, $A \subseteq B$ seien Teilmengen von $\mathbb{C}$. Forkt der Typ $p \in \mathrm{S}(B)$ nicht über A, so teilt er auch nicht über A.*

Beweis: siehe [Wa, Proposition 2.3.9]

Im nächsten Theorem sind mehrere Möglichkeiten aufgeführt, einfache Theorien zu definieren:

Theorem 2.10. *Es sind äquivalent:*

1) T ist einfach.

2) Forken ist symmetrisch.

3) Teilen ist symmetrisch.

4) Forken ist transitiv: Sind $A \subseteq B \subseteq C$ und D gegeben, so gilt:

$$\begin{aligned}\mathrm{tp}(D/C) \textit{ forkt nicht über } A \iff & \mathrm{tp}(D/B) \textit{ forkt nicht über } A \textit{ und} \\ & \mathrm{tp}(D/C) \textit{ forkt nicht über } B.\end{aligned}$$

5) Teilen ist transitiv.

6) Forken hat lokalen Charakter: Für jedes $p \in \mathrm{S}(A)$ existiert ein $A_0 \subseteq A$ mit $|A_0| \leq |T|$, so daß p nicht über A_0 forkt.

7) Teilen hat lokalen Charakter.

Beweis: siehe [Wa, Theorem 2.4.7]

Im Rest der Arbeit werde ich überwiegend mit der Definition einfacher Theorien durch den lokalen Charakter des Forkens arbeiten.

Beispiel 2.11. *Sei $L = \{<\}$ und T_{doO} die Theorie dichter offener Ordnungen. Dann ist T_{doO} nicht einfach.*

Beweis: Ich werde drei verschiedene Beweise geben: Den ersten mit 2.10.3, den zweiten mit 2.10.5 und den dritten mit 2.10.7.

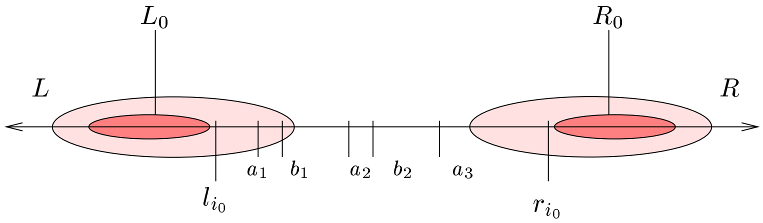
1) Die Unabhängigkeitsrelation ist nicht symmetrisch:
   Es seien $a < b < c \in \mathbb{C} \models \mathrm{T}_{\mathrm{doO}}$. Sei $\varphi(x, a, c) = a < x < c$ und sei $(a_i c_i)_{i<\omega}$ eine Folge in $\mathrm{tp}(ac/\emptyset)$ mit $a_{i+1} > c_i$. Die Intervalle $[a_i, c_i]$ sind dann paarweise disjunkt. Dann ist $\{\varphi(x, a_i, c_i) \mid i < \omega\}$ 2-inkonsistent, das heißt $\mathrm{tp}(b/ac)$ teilt über $\emptyset$.
   Betrachte nun $\mathrm{tp}(ac/b)$. Dieser Typ wird durch die Formel $\psi(x, y, b) = x < b < y$ isoliert; er teilt also nur dann über $\emptyset$, wenn schon $\psi(x, y, b)$ über $\emptyset$ teilt. Es sei $(b_i)_{i<\omega}$ eine Folge in $\mathrm{tp}(b/\emptyset)$ und $b_{i_0}, \ldots, b_{i_{k-1}}$ eine k-elementige Teilfolge. Dann besagt $\bigwedge_{j=0}^{k-1} x < b_{i_j} < y$ nur, daß $x < \min\{b_{i_0}, \ldots, b_{i_{k-1}}\}$ und $y > \max\{b_{i_0}, \ldots, b_{i_{k-1}}\}$ ist; dies ist immer erfüllbar. Also ist $\{\psi(x, y, b_i) \mid i < \omega\}$ konsistent, das heißt $\mathrm{tp}(ac/b)$ teilt nicht über $\emptyset$. Es gilt also $ac \underset{\emptyset}{\perp} b$, aber $b \underset{\emptyset}{\not\perp} ac$. ■1)

2) Die Unabhängigkeitsrelation ist nicht transitiv:
   Es sei $b < c < d$. Dann ist $c \underset{\emptyset}{\perp} b$; weiter gilt $c \underset{b}{\perp} d$: Die Formel $b < x < d$ isoliert $\mathrm{tp}(c/bd)$. Ist $(d_i)_{i<\omega}$ eine Folge in $\mathrm{tp}(d/b)$, so besagt eine endliche Konjunktion von Formeln $b < x < d_i$ nur, daß x zwischen dem Minimum der d_i und b liegt, was in dichten Ordnungen immer erfüllbar ist. Nach 1) gilt aber $c \underset{\emptyset}{\not\perp} bd$. ■2)

3) Es existiert ein Typ, der über jeder abzählbaren Menge teilt:
   Es sei κ eine Kardinalzahl mit Kofinalität $\mathrm{cof}(\kappa) > \aleph_0$. Weiter seien $L = \{l_i \mid i < \kappa\}$ und $R = \{r_i \mid i < \kappa\}$ Teilmengen von $\mathbb{C}$ mit $l_i < l_j$ und $r_i > r_j$ für $i < j$ und $l < r$ für alle $l \in L$ und $r \in R$. Unser Kandidat ist der Typ

$$p(x) = \{x > l \mid l \in L\} \cup \{x < r \mid r \in R\}.$$

Es seien L_0 und R_0 abzählbare Teilmengen von L und R. Wegen $\mathrm{cof}(\kappa) > \aleph_0$ existiert dann ein $i_0 \in \kappa$ mit $l_{i_0} > l_0$ und $r_{i_0} < r_0$ für alle $l_0 \in L_0$ und $r_0 \in R_0$.



Man betrachte die Formel $l_{i_0} < x < r_{i_0}$: Je zwei Punkte $a < b$, die zwischen l_{i_0} und r_{i_0} liegen, haben den gleichen Typ über L_0R_0 wie l_{i_0}, r_{i_0}. Nun existiert eine Folge $(a_ib_i)_{i<\omega}$ in $\mathrm{tp}(l_{i_0}r_{i_0}/L_0R_0)$, so daß die Intervalle $[a_i, b_i]$ paarweise disjunkt sind. Die Formel $l_{i_0} < x < r_{i_0}$ teilt also über L_0R_0. ■3)

Wenn eine abstrakte dreistellige Relation $\mathop{\smile\!\!\!\!|}^{abstr}$ in einer Theorie T bestimmte Eigenschaften besitzt, so ist T bereits einfach und $\mathop{\smile\!\!\!\!|}^{abstr}$ ist die Forking-Unabhängigkeitsrelation:

Theorem 2.12. $\mathop{\smile\!\!\!\!|}^{abstr}$ *sei eine unter Automorphismen invariante, abstrakte, dreistellige Relation, so daß gilt:*

- $\mathop{\smile\!\!\!\!|}^{abstr}$ *ist symmetrisch.*
- $\mathop{\smile\!\!\!\!|}^{abstr}$ *ist transitiv.*
- *Zu* $\bar{a}, A, B$ *existiert ein* $\bar{a}' \models \mathrm{tp}(\bar{a}/A)$ *mit* $\bar{a}' \mathop{\smile\!\!\!\!|}_{A}^{abstr} B$.
- $\mathop{\smile\!\!\!\!|}^{abstr}$ *hat lokalen Charakter.*
- $\mathop{\smile\!\!\!\!|}^{abstr}$ *hat endlichen Charakter.*

Weiter gelte der sogenannte Unabhängigkeitssatz: Ist $\bar{a} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{abstr} \bar{b}$ *für ein Modell* $\mathcal{M}$, *und sind* $\bar{x} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{abstr} \bar{a}$ *und* $\bar{y} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{abstr} \bar{b}$ *mit* $\mathrm{tp}(\bar{x}/\mathcal{M}) = \mathrm{tp}(\bar{y}/\mathcal{M})$, *so existiert ein* $\bar{z} \models \mathrm{tp}(\bar{x}/\mathcal{M}\bar{a}) \cup \mathrm{tp}(\bar{y}/\mathcal{M}\bar{b})$ *mit* $\bar{z} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{abstr} \bar{a}\bar{b}$. *Dann ist* T *einfach und es ist* $\mathop{\smile\!\!\!\!|}^{abstr} = \mathop{\smile\!\!\!\!|}$.

Beweis: siehe [Wa, Theorem 2.6.1]

Sei T nun eine stabile Theorie. Dann erfüllt die dort definierte Nicht-Forking-Relation $\mathop{\smile\!\!\!\!|}^{stab}$ die Bedingungen [SYM], [TRA], [EX], [EC] und [LC]; $\mathop{\smile\!\!\!\!|}^{stab}$ erfüllt aber auch den Unabhängigkeitssatz: Sind $\bar{a}, \bar{b}, \bar{x}, \bar{y}$ und $\mathcal{M}$ wie oben gegeben, so sei q die eindeutig bestimmte nicht-forkende Fortsetzung von $p := \mathrm{tp}(\bar{x}/\mathcal{M})$ auf $\mathcal{M}\bar{a}\bar{b}$. Weiter sei $\bar{z} \in \mathbb{C}$ so, daß $\bar{z} \models q$ gilt. Dann gilt $\bar{z} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{stab} \bar{a}\bar{b}$; insbesondere sind $q|_{\mathcal{M}\bar{a}}$ und $q|_{\mathcal{M}\bar{b}}$ nichtforkende Fortsetzungen von p. Da diese nichtforkenden Fortsetzungen in stabilen Theorien eindeutig bestimmt sind und $\bar{x} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{stab} \bar{a}$ und $\bar{y} \mathop{\smile\!\!\!\!|}_{\mathcal{M}}^{stab} \bar{b}$ gilt, ist q sowohl eine Fortsetzung von $\mathrm{tp}(\bar{x}/\mathcal{M}\bar{a})$ als auch von $\mathrm{tp}(\bar{y}/\mathcal{M}\bar{b})$.
Also sind stabile Theorien einfach und die Unabhängigkeitsrelation $\mathop{\smile\!\!\!\!|}^{stab}$ stimmt mit der in einfachen Theorien definierten Forking-Unabhängigkeit $\mathop{\smile\!\!\!\!|}$ überein.

Zum Abschluß dieses Abschnittes noch ein Theorem und eine Folgerung aus diesem, die es uns später ermöglichen wird, statt mit einem bestimmten einfachen Körper mit einer endlichen Erweiterung desselben zu arbeiten:

Theorem 2.13. *Ist die Theorie T' in der Theorie T interpretierbar, so ist mit T auch T' einfach. Insbesondere folgt: T ist genau dann einfach, wenn T^{eq} einfach ist.*

Beweis: siehe [Wa, Korollar 2.8.11]

Korollar 2.14. *Ist K ein Körper mit einfacher Theorie und ist L eine endliche Erweiterung von K, so ist auch die Theorie von L einfach.*

Beweis: klar mit 2.4.

2.5 Vermischtes

Alle nicht bewiesenen Ergebnisse dieses Abschnittes finden sich in [Las, Kapitel 2, 3 und 4.5].

Wir fixieren eine Theorie T. Es sei $\mathcal{M} \models T$; weiter sei $A \supseteq M$ eine Parametermenge. Es sei $p \in \mathrm{S}(M)$ und q sei eine Erweiterung von p auf A. Dann heißt q **Erbe** von p, wenn für jede Formel $\varphi(\bar{x}, \bar{a}, M) \in q$ mit $\bar{a} \in A$ ein $\bar{m} \in M$ existiert mit $\varphi(\bar{x}, \bar{m}, M) \in p$; das heißt, daß jede Formel aus q in p **repräsentiert** wird. Ich schreibe kurz $\boldsymbol{\bar{b}} \mathop{\downarrow}_{\boldsymbol{M}}^{\boldsymbol{E}} \boldsymbol{A}$, um auszudrücken, daß $\mathrm{tp}(\bar{b}/A)$ Erbe von $\mathrm{tp}(\bar{b}/M)$ ist.
Es sei $M \models T$ und $B \supseteq A \supseteq M$ seien Mengen. Weiter sei $p \in \mathrm{S}(M)$, und $q \in \mathrm{S}(A)$ sei Erbe von p. Dann enthält $\mathrm{S}(B)$ einen Erben von p, der q enthält; insbesondere existiert für jedes $A \supseteq M$ ein Erbe $q \in \mathrm{S}(A)$ von p.
Ist T stabil, so ist dieser Erbe eindeutig bestimmt. Weiter gilt dann: Ist $p \in \mathrm{S}(M)$ und $q \in \mathrm{S}(A)$ für eine Menge $A \supseteq M$ und ist T stabil, so ist q genau dann Erbe von p, wenn q nicht-forkende Erweiterung von p ist.

Beispiel: Algebraisch abgeschlossene Körper
Es sei p gleich 0 oder p prim. Weiter sei $T_{\mathrm{aaK},p}$ die Theorie algebraisch abgeschlossener Körper der Charakteristik p. $T_{\mathrm{aaK},p}$ ist vollständig, modellvollständig, hat Quantorenelimination und ist $\aleph_1$-kategorisch.
Ist K ein Körper und ist $p \in \mathrm{S}_n(K)$, so ist p durch die Menge $I(p) := \{f(X_1, \ldots, X_n) \in K[\bar{X}] \mid f(\bar{x}) \doteq 0 \in p\}$ eindeutig bestimmt; also ist $T_{\mathrm{aaK},p}$ auch ω-stabil.
Ist K ein algebraisch abgeschlossener Körper und sind K_1, K_2 zwei Erweiterungen von K, so sind äquivalent:

$$1)\ K_1 \mathop{\downarrow}_K^{l} K_2 \qquad 2)\ K_1 \mathop{\downarrow}_K^{a} K_2 \qquad 3)\ K_1 \mathop{\downarrow}_K^{E} K_2 \qquad 4)\ K_1 \mathop{\downarrow}_K^{stab} K_2 \qquad 5)\ K_1 \mathop{\downarrow}_K K_2$$

Des weiteren stimmen auf algebraisch abgeschlossenen Körpern der algebraische und der modelltheoretische Begriff des algebraischen Abschlusses überein.

Mit diesem Hintergrund folgt leicht das nächste Lemma, das ich in Kapitel 4.8 benötigen werde:

Lemma 2.15. *Seien A, B, C und K algebraisch abgeschlossene Körper mit $K \subseteq AB \cap C$. Weiter sei $AB \underset{K}{\overset{a}{\downarrow}} C$. Dann gilt*

$$(AB)^a \cap (AC)^a (BC)^a = AB.$$

Beweis: „$\supseteq$" ist klar. Also zu „$\subseteq$":
Ist $a \in (AC)^{\mathrm{a}}(BC)^{\mathrm{a}}$, so gibt es eine Formel $\varphi(a, \bar{a}, \bar{c}_A, \bar{b}, \bar{c}_B)$ die besagt, daß a rationale Funktion von Nullstellen von Polynomen aus $AC[X]$ und $BC[X]$ ist; dabei sind $\bar{a}, \bar{c}_A$ die Parameter aus A und C, die in den Polynomen aus $AC[X]$ vorkommen, und $\bar{b}, \bar{c}_B$ die Parameter aus B und C, die in den Polynomen aus $BC[X]$ vorkommen.
Ist nun $a \in (AB)^{\mathrm{a}}$, so folgt aus $\mathrm{tp}((AB)^{\mathrm{a}}/C)$ die Formel $\varphi(x, \bar{x}, \bar{c}_A, \bar{y}, \bar{c}_B)$. Wegen $AB \underset{K}{\overset{a}{\downarrow}} C$ gilt auch $(AB)^{\mathrm{a}} \underset{K}{\overset{a}{\downarrow}} C$, es ist also $\mathrm{tp}((AB)^{\mathrm{a}}/C)$ Erbe von $\mathrm{tp}((AB)^{\mathrm{a}}/K)$. Es gibt demnach $\bar{k}_A, \bar{k}_B \in K$ mit $\mathrm{tp}((AB)^{\mathrm{a}}/K) \to \varphi(x, \bar{x}, \bar{k}_A, \bar{y}, \bar{k}_B)$. Dies bedeutet, daß a rationale Funktion von Nullstellen von Polynomen aus $A[X]$ und $B[X]$ ist; da A und B algebraisch abgeschlossen sind, ist a also aus AB. ■

Theorem 2.16. *Sei F ein Körper und $A \subseteq F$ eine Teilmenge. Ist $\mathrm{acl}(A) = A$, so ist A ein Körper und die Erweiterung $F \supseteq A$ ist regulär.*

Beweis: Es ist offensichtlich, daß A ein Körper ist. Da alle im körpertheoretischen Sinne algebraischen Elemente auch im modelltheoretischen Sinne algebraisch sind, gilt $K \cap A^{\mathrm{a}} \subseteq A$, also ist $K \supseteq A$ primär. Da schließlich die λ-Funktionen eines Körpers $\emptyset$-definierbar sind, ist A gegen die λ-Funktionen von K abgeschlossen und damit separabel. ■

Der Genuß einer leichten Suppe wird der Konzentration des Lesers jetzt sicher gut tun:

Zuccini-Honigmelonen-Suppe mit Pernod

ergibt 6 Teller

600g junge Zuccini in Würfel schneiden und in reichlich Butter andünsten, mit Pernod ablöschen und mit 1l Wasser auffüllen. Gar kochen lassen und pürieren, mit Salz, Pfeffer, Brühe, Muskat, Sahne und eventuell noch mit etwas Pernod (Vorsichtig dosieren!) abschmecken. Melonen in 1 cm^3 große Würfel schneiden und in die Suppe geben. Nur noch kurz erwärmen und servieren.

3 PAC-Körper

In diesem Kapitel wird definiert, was ein pseudo-algebraisch abgeschlossener Körper (kurz: PAC-Körper) ist. Wir werden einige Beispiele für PAC-Körper und die für uns wichtigsten Eigenschaften dieser Klasse von Körpern kennenlernen; schließlich werden wir eine äquivalente Definition angeben, mit der wir im Verlauf der Arbeit vorwiegend arbeiten werden. Mehr Informationen über PAC-Körper findet man in [FJ, Kapitel 10].

Definition 3.1. *Sei K ein Körper. K heißt* **pseudo-algebraisch abgeschlossen** *(oder kurz ein* **PAC-Körper***), wenn jede absolut irreduzible, über K definierte Varietät einen K-rationalen Punkt besitzt.*

Um herauszufinden, ob ein Körper pseudo-algebraisch abgeschlossen ist, reicht es, die folgende Bedingung zu prüfen:

Theorem 3.2. *L sei eine algebraische Erweiterung von K. Dann ist L genau dann pseudo-algebraisch abgeschlossen, wenn jede über K definierte ebene Kurve einen L-rationalen Punkt besitzt.*

Beweis: siehe [FJ, Theorem 10.4]

Um Beispiele für PAC-Körper angeben zu können, benötigen wir das folgende Ergebnis über die Anzahl von K-rationalen Punkten einer über einem endlichen Körper K definierten flachen Kurve V:

Theorem 3.3. *Es sei $n \in \mathbb{N}$, $q := p^n$ und V eine ebene Kurve über $\mathbb{F}_q$, etwa $V = V(\{f\})$ für ein nichtkonstantes irreduzibles Polynom $f(X,Y) \in \mathbb{F}_q[X,Y]$ von Grad d. Weiter sei $V_{\mathbb{F}_q}(\{f\})$ die Menge der $\mathbb{F}_q$-rationalen Punkte von V. Dann gilt:*

$$|V_{\mathbb{F}_q}(\{f\})| \geq q + 1 - (d-1)(d-2)\sqrt{q} - d$$

Beweis: siehe [FJ, Theorem 4.9]

Beispiel 3.4 (Ershov). *Unendliche algebraische Erweiterungen von endlichen Körpern sind PAC.*

Beweis: Es sei K eine unendliche algebraische Erweiterung eines endlichen Körpers, etwa $K \supset \mathbb{F}_p$, weiter sei $f(X,Y) \in \mathbb{F}_p[X,Y]$ ein nichtkonstantes, irreduzibles Polynom von Grad d.
Es sei $q := p^n$. Es existieren beliebig große $n \in \mathbb{N}$ mit $\mathbb{F}_{p^n} \subset K$. Wähle $n \in \mathbb{N}$ so groß, daß $q > d^4$ ist. Dann gilt

$$q + 1 - (d-1)(d-2)\sqrt{q} - d > 3d^3 - 2d^2 - d + 1 > 0,$$

wegen 3.3 gilt also $|V_{\mathbb{F}_q}(\{f\})| > 0$. Demnach hat V einen rationalen Punkt in $\mathbb{F}_q$ und damit in K. Mit 3.2 folgt dann, daß K pseudo-algebraisch abgeschlossen ist. ■

Beispiel 3.5. *Jede algebraische Erweiterung eines PAC-Körpers ist wieder ein PAC-Körper.*

Beweis: folgt sofort aus 3.3

Weiter kann man mit Hilfe von 3.3 zeigen, daß die Klasse der PAC-Körper FO-axiomatisierbar ist:

Theorem 3.6. *Es gibt eine Satzmenge Φ_{PAC} in L_{Kp}, die genau dann von einem Körper K erfüllt wird, wenn K pseudo-algebraisch abgeschlossen ist.*

Beweis: siehe [FJ, Proposition 10.9]

Hieraus ergibt sich sofort, daß beliebige Ultraprodukte von PAC-Körpern wieder pseudo-algebraisch abgeschlossen sind.

Schließlich beweisen wir noch die folgende Äquivalenz:

Theorem 3.7. *Sei K ein Körper. K ist genau dann pseudo-algebraisch abgeschlossen, wenn es zu jeder regulären Erweiterung $E \supseteq K$ eine elementare Oberstruktur $F \succ K$ mit $E \subseteq F$ gibt.*

Beweis: „$\Rightarrow$“ Sei K ein PAC-Körper und $E \supseteq K$ eine reguläre Erweiterung von K. Nach 2.1 reicht es, die existentielle Abgeschlossenheit von K in E zu zeigen. Nach 2.3 reicht es dazu, zu zeigen, daß jede K-Varietät mit einem rationalen Punkt in E auch einen rationalen Punkt in K besitzt.
Es sei also V eine K-Varietät und $a \in E \cap V$. Dann ist $K(a) \supseteq K$ regulär. Es sei $I_K(\{a\})$ das von a in $K[\bar{X}]$ bestimmte Primideal und $V_a \subseteq V$ die zugehörige K-Varietät. Nach 1.31 ist V_a dann eine über K definierte Varietät, hat also einen rationalen Punkt in K; insbesondere hat also V einen rationalen Punkt in K.
„$\Leftarrow$“ Es sei $V = (f_1, \ldots, f_n)$ eine über K definierte Varietät und a ein generischer Punkt von V. Nach 1.31 ist $K(a) \supseteq K$ dann eine reguläre Erweiterung. Es existiert also ein $F \succ K$, das $K(a)$ enthält. Es gilt $F \models \bigvee_{i=1}^{n} f_i(a) \doteq 0$, also auch $K \models \exists x \bigvee_{i=1}^{n} f_i(x) \doteq 0$; also hat V einen rationalen Punkt in K. ■

Eigentlich gehört das Sorbet zwischen die beiden Hauptgerichte, aber bei der Länge der Kapitel drängt sich eine Änderung der Menüfolge auf. Also schon hier:

Caipirinha-Sorbet

für 4 Personen

Den Saft von 8 Limetten, 400ml Wasser, 4cl Cachaça und 8 Teelöffel braunen Zucker vermischen. Unter gelegentlichem Rühren frieren lassen. Zum Servieren zerstampfen, auf 4 Gläser verteilen und mit soviel Sekt auffüllen, daß das Sorbet gerade von Flüssigkeit bedeckt ist.

4 Reguläre Realisierung von großen direkten Produkten der alternierenden Gruppe

Das Ziel dieses Kapitels ist das folgende Theorem:

Theorem 4.1.
Es sei F ein überabzählbarer Körper der Charakteristik p, es sei t transzendent über F und $n \in \mathbb{N}$, $n > 4$. Ist F ein PAC-Körper oder gilt $p \nmid n(n-1)$, so existiert eine Galoiserweiterung M von $F(t)$ mit

$$\mathrm{Gal}(M/F(t)) \cong \prod_{|F|} A_n,$$

so daß $M \supset F$ eine reguläre Erweiterung ist.

Bemerkung: Gilt $p \nmid n(n-1)$, so folgt $p \neq 2$. Ist $p \neq 2$, so lassen sich beliebig große $n \in \mathbb{N}$ mit $p \nmid n(n-1)$ finden.

Gilt $p \nmid n(n-1)$, so werden wir das Ergebnis aus den bisher bewiesenen bzw. zitierten Ergebnissen folgern. Andernfalls benutzen wir zum Beweis eine direkte Folgerung aus [Pop, Theorem A]:

Theorem 4.2. *Ist F ein PAC-Körper[9] und t transzendent über F, so läßt sich jede endliche Gruppe G so als Galoisgruppe über $F(t)$ realisieren, daß die entstehende Erweiterung von F regulär ist.*

In [Ch1] wird die Existenz einer Galoiserweiterung $M \supset F(t)$ wie in 4.1 nur für PAC-Körper bewiesen; dazu wird Theorem 4.2 benutzt. Durch die Ergebnisse in Abschnitt 4.1 wird es uns gelingen, die allgemeinere Aussage aus Theorem 4.1 zu zeigen; gilt $p \nmid n(n-1)$, so werden wir dabei Theorem 4.2 nicht benötigen.
Wir werden Theorem 4.1 in Kapitel 5 zum Beweis des Hauptsatzes dieser Arbeit benötigen. Daß wir im Beweis von Theorem 4.1 für $p \nmid n(n-1)$ das Ergebnis von F. Pop nicht benötigen, wird dazu führen, daß wir in dem entsprechenden Beweisschritt nur für $p = 2$ benutzen, daß wir uns in einem PAC-Körper befinden.

Zur Gliederung des Kapitels:

In Abschnitt 4.1 werde ich für beliebige Körper K der Charakteristik p und für alle $n > 2$ mit $p \nmid n(n-1)$ zeigen, daß es für jedes über K transzendente Element t eine Galoiserweiterung $L \supset K(t)$ mit $\mathrm{Gal}(L/K(t)) \cong A_n$ gibt, so daß $L \supset K$ regulär ist. Dazu gebe ich zuerst ein Polynom an, so daß die Galoisgruppe des Zerfällungskörpers über $K(t)$ isomorph zur symmetrischen Gruppe S_n ist. Danach zeige ich, daß der Fixkörper der A_n wieder ein rationaler Funktionenkörper ist; schließlich wird be-

[9] In [Pop, Theorem A] wird die Aussage nicht nur für PAC-Körper, sondern allgemeiner für sogenannte „large fields" (das sind Körper K, in denen jede glatte Kurve, die einen K-rationalen Punkt besitzt, bereits unendlich viele K-rationale Punkte besitzt) bewiesen.

wiesen, daß die entstehende Erweiterung von K regulär ist. Hierzu benötige ich die bewertungstheoretischen Grundlagen aus Kapitel 1.

Abschnitt 4.2 enthält den Beweis von Theorem 4.1. Es wird möglich sein, zu einem Körper F, zu $n > 4$ und zu einem über F transzendenten Element t, so daß die Bedingungen aus Theorem 4.1 erfüllt sind, $|F|$-viele, über $F(t)$ linear disjunkte Galoiserweiterung zu konstruieren: Man geht zu einer abzählbaren elementaren Unterstruktur K von F über und fixiert eine Transzendenzbasis B von F über K. Für $b \in B$ realisiert man die A_n nun als Galoiserweiterung von $K(tb)$ und zieht die Erweiterungen wieder hoch auf $F(t)$. Der Nachweis, daß die so entstehenden Erweiterungen von $F(t)$ linear disjunkt sind, wird den Hauptteil des Beweises ausmachen.

4.1 Die reguläre Realisierung der alternierenden Gruppe

Zur Erinnerung: Wann immer wir in einem Körper der Charakteristik p arbeiten, für den ein $n \in \mathbb{N}$ nit $p \nmid n(n-1)$ existiert, so gilt $p \neq 2$.

Der erste Schritt ist die reguläre Realisierung der symmetrischen Gruppe S_n. Hierzu benötige ich zunächst einige Lemmata:

Lemma 4.3. *K sei ein Körper der Charakteristik p, t sei transzendent über K und es sei $n \geq 2$ mit $p \nmid n$. Weiter sei $f(X) := X^n - X^{n-1} - t \in K(t)[X]$. Dann gilt mit $b := \left(\frac{n-1}{n}\right)^n - \left(\frac{n-1}{n}\right)^{n-1}$ für die Diskriminante $D(f)$ von f:*

$$D(f) = \pm n^n t^{n-2}(t-b).$$

Beweis: Es sei $a := 1 - n$. Für die Resultante $R(f, f')$ von f und f' gilt:

$$R(f,f') = \begin{array}{|ccccccc:ccccc|l}
1 & -1 & 0 & \dots & & 0 & -t & & & & & & \\ \hdashline
0 & 1 & -1 & 0 & \dots & & 0 & -t & & & & & \\
& & \ddots & \ddots & & & & \ddots & \ddots & & & & \left.\right\} n-1 \\
& & & \ddots & \ddots & & & & \ddots & \ddots & & & \\
& & & & 1 & -1 & 0 & \dots & & & 0 & -t & \\ \hdashline
n & a & 0 & \dots & & & & & & & & & \\
0 & n & a & 0 & \dots & & & & & & & & \\
& & \ddots & \ddots & & & & & & & & & \left.\right\} n \\
& & & \ddots & \ddots & & & & & & & & \\
& & & & n & a & 0 & & & & & & \\
& & & & & n & a & & & & & & \\
\multicolumn{7}{c}{\underbrace{\hphantom{xxxxxxxxxxxxxxxxxx}}_{n+1}} & \multicolumn{5}{c}{\underbrace{\hphantom{xxxxxxxxxxxx}}_{n-2}} &
\end{array}$$

Durch $(n-2)$-fache Entwicklung nach der letzten Spalte erhält man hieraus

$$R(f,f') = \pm t^{n-2} \begin{vmatrix} 1 & -1 & 0 & \dots & \dots & 0 & -t \\ n & a & 0 & \dots & & & \\ 0 & n & a & 0 & \dots & & \\ & & \ddots & \ddots & & & \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & n & a \end{vmatrix}.$$

Nach Entwicklung nach der ersten Zeile erhält man dann

$$\begin{aligned} R(f,f') &= \pm t^{n-2}\left(a^n + na^{n-1} + (-1)^{n+1} t n^n\right) \\ &= \pm n^n t^{n-2}\left(t - \frac{a^n + na^{n-1}}{(-1)^n n^n}\right) \\ &= \pm n^n t^{n-2}\left(t - \left(\frac{(-a)^n}{n^n} - \frac{(-a)^{n-1}}{n^{n-1}}\right)\right) \\ &= \pm n^n t^{n-2}\left(t - \left(\frac{(n-1)^n}{n^n} - \frac{(n-1)^{n-1}}{n^{n-1}}\right)\right) \\ &= \pm n^n t^{n-2}(t-b). \end{aligned}$$

Nach Kapitel 1, Abschnitt 1.1.6 unterscheiden sich $R(f,f')$ und $D(f)$ nur durch ein Vorzeichen. ∎

Eine transitive Permutationsgruppe G, die auf $A := \{a_1, \dots, a_n\}$ operiert, ist genau dann doppelt transitiv, wenn für ein $a_i \in A$ (äquivalent: für alle $a_i \in A$) der Stabilisator $\mathrm{Stab}(a_i)$ transitiv auf $A \setminus \{a_i\}$ operiert (siehe z.B. [Hu, Kapitel II, Paragraph 1 Hilfssatz 1.8]). Daraus folgt:

Lemma 4.4. *Es sei $n \in \mathbb{N}$ und $G \leq S_n$ eine transitive Permutationsgruppe, die eine Transposition enthält. Dann sind äquivalent:*

1) G enthält einen $(n-1)$-Zykel.
2) G ist 2-fach transitiv.
3) $G = S_n$

Beweis: G operiere auf $A := \{a_1, \dots, a_n\}$.
1)→2): Sei $\tau \in G$ ein $(n-1)$-Zykel, es sei etwa $\tau = \langle a_1, \dots, a_{n-1}\rangle$. Dann ist $\tau \in \mathrm{Stab}(a_n)$; also operiert $\mathrm{Stab}(a_n)$ transitiv auf $A \setminus \{a_n\}$; G ist also 2-fach transitiv.
2)→3): Ich zeige, daß G alle Transpositionen enthält. G enthält nach Voraussetzung eine Transposition, etwa $\langle a_1, a_2\rangle$. Es seien $a_i \neq a_j \in G$ beliebig. Da G doppelt transitiv ist, existiert ein $\sigma \in G$ mit $\sigma(a_1) = a_i$ und $\sigma(a_2) = a_j$. Dann ist $\sigma\langle a_1, a_2\rangle\sigma^{-1} = \langle a_i, a_j\rangle$.
3)→1) ist trivial. ∎

Theorem 4.5. *Es sei K ein Körper der Charakteristik p und t transzendent über K. Weiter sei $n > 2$ mit $p \nmid n(n-1)$. L sei der Zerfällungskörper des Polynoms $f(X) = X^n - X^{n-1} - t \in K(t)[X]$ über $K(t)$. Weiter sei $a := \frac{n-1}{n}$, $b := a^n - a^{n-1}$ und $G := \mathrm{Gal}(L/K(t))$.*
Dann hat die Stelle bei ∞ auf $K(t)$ eine Fortsetzung auf L mit Verzweigungsgrad n, die Stelle bei 0 auf $K(t)$ hat eine Fortsetzung auf L mit Verzweigungsgrad $n-1$ und die Stelle bei b auf $K(t)$ hat eine Fortsetzung auf L mit Verzweigungsgrad 2.

Beweis: Es sei α eine Nullstelle von f. Dann ist wegen $t = \alpha^n - \alpha^{n-1}$ auch $K(t,\alpha) = K(\alpha)$ wieder ein rationaler Funktionenkörper in einer Variablen über K. Es sei $H := \mathrm{Gal}(L/K(\alpha)) \le G$. Wir werden in Teil A die Stelle bei ∞, in Teil B die Stelle bei 0 und in Teil C die Stelle bei b betrachten.

Teil 1: Die Gradbewertung v_∞ auf $\mathbf{K(t)}$.

Behauptung A.1: Die Gradbewertung w_∞ auf $K(\alpha)$ ist die einzige Fortsetzung von der Gradbewertung v_∞ von $K(t)$ auf $K(\alpha)$. Der Verzweigungsindex ist n, das heißt insbesondere ist f irreduzibel und die Fortsetzung ist rein verzweigt.

w sei eine Fortsetzung von v_∞ auf $K(\alpha)$. Es ist $w(\alpha) < 0$, denn sonst wäre $w(t) \ge \min\{w(\alpha^n), w(\alpha^{n-1})\} \ge 0$. Also gilt $w(\alpha^n) < w(\alpha^{n-1})$ und daher

$$w(t) = -1 = w(\alpha^n - \alpha^{n-1}) = w(\alpha^n) = nw(\alpha),$$

also $w(\alpha) = \frac{1}{n} v_\infty(t) = -\frac{1}{n}$. Also hat w mindestens den Verzweigungsgrad $e = n$, dies ist wegen $[K(\alpha) : K(t)] \le n$ aber auch der maximal mögliche. Wegen Korollar 1.23 ist w also die einzige Fortsetzung von v_∞ und die Adjunktion von α führt zu einer Erweiterung von Grad n, f ist also irreduzibel. Da die Gradbewertung w_∞ auf $K(\alpha)$ die einzige auf K triviale Bewertung auf $K(\alpha)$ ist, unter der α einen negativen Wert annimmt, ist $w = w_\infty$. ■Beh.A.1

Behauptung A.2: w_∞ verzweigt nicht in L.

Es sei $g(X) = X^{n-1} + (1 - \frac{1}{\alpha})(X^{n-2} + X^{n-3} + \dots + 1)$. Dann gilt

$$\begin{aligned}
&\alpha^{n-1}(X-\alpha) g\left(\tfrac{X}{\alpha}\right) \\
&\quad = \alpha^{n-1}(X-\alpha)\Big(\tfrac{X^{n-1}}{\alpha^{n-1}} + \big(1 - \tfrac{1}{\alpha}\big)\big(\tfrac{X^{n-2}}{\alpha^{n-2}} + .. + 1\big)\Big) \\
&\quad = (X-\alpha)\Big(X^{n-1} + \big(\alpha^{n-1} - \alpha^{n-2}\big)\big(\tfrac{X^{n-2}}{\alpha^{n-2}} + .. + 1\big)\Big) \\
&\quad = (X-\alpha)\Big(\begin{array}{ccccccc} X^{n-1} & + & \alpha X^{n-2} & + & \dots & + & \alpha^{n-1} \\ & - & X^{n-2} & - & \dots & - & \alpha^{n-2} \end{array}\Big) \\
&\quad = \begin{array}{ccccccccccc} X^n & + & \alpha X^{n-1} & + & \alpha^2 X^{n-2} & + & \dots & + & \alpha^{n-1}X & & \\ & - & X^{n-1} & - & \alpha X^{n-2} & - & \dots & - & \alpha^{n-2}X & & \\ & - & \alpha X^{n-1} & - & \alpha^2 X^{n-2} & - & \dots & - & \alpha^{n-1}X & - & \alpha^n \\ & & & + & \alpha X^{n-2} & + & \dots & + & \alpha^{n-2}X & + & \alpha^{n-1} \end{array} \\
&\quad = X^n - X^{n-1} - (\alpha^n - \alpha^{n-1}) \\
&\quad = X^n - X^{n-1} - t.
\end{aligned}$$

Demnach ist L der Zerfällungskörper von g über $K(\alpha)$.
Es ist $w_\infty(1) = 0$ und $w_\infty\left(\frac{1}{\alpha}\right) = 1$, also liegt $g(X) \in \mathcal{O}_{w_\infty}[X]$. Im Restklassenkörper gilt $(1-\frac{1}{\alpha})+\mathcal{M}_{w_\infty} = 1+\mathcal{M}_{w_\infty}$, g wird in $K(\alpha)_{w_\infty} = \mathcal{O}_{w_\infty}/\mathcal{M}_{w_\infty}$ also zum Polynom

$$\overline{g}^\infty(X) = X^{n-1} + X^{n-2} + \cdots + 1.$$

Es ist $\overline{g}^\infty(X)(X-1) = X^n - 1$; da p teilerfremd zu n ist, hat $X^n - 1$ und damit auch $\overline{g}^\infty(X)$ keine mehrfachen Nullstellen. Hieraus folgt sofort, daß w_∞ in L nicht verzweigt:
Angenommen es gibt eine verzweigte Fortsetzung u von w_∞ auf L. Dann ist die Trägheitsgruppe $T_u \leq H$ der Erweiterung $(L,u)/(K(\alpha), w_\infty)$ nicht trivial. Sei etwa $\sigma \in T_u, \sigma \neq 1$. Da O_u ganz abgeschlossen in L ist, $g(X)$ in $\mathcal{O}_{w_\infty}[X] \subseteq \mathcal{O}_u[X]$ liegt und g in L zerfällt, liegen alle Nullstellen von g in $\mathcal{O}_u$. Da L Zerfällungskörper von g über $K(\alpha)$ ist, existiert folglich eine Nullstelle β von g mit $\sigma(\beta) \neq \beta$ und $\sigma(\beta) - \beta \in \mathcal{M}_u$, es ist demzufolge $\sigma(\beta)+\mathcal{M}_{w_\infty} = \beta+\mathcal{M}_{w_\infty}$. Ergo hat $\overline{g}^\infty(X)$ eine doppelte Nullstelle. Widerspruch! ■Beh.A.2

Teil B: Die Stelle bei 0.

Behauptung B.1: Der Verzweigungsindex von $K(\alpha) \supset K(t)$ bzgl. der t-adischen Bewertung auf $K(t)$ ist $n-1$.

w_0 sei die α-adische Bewertung auf $K(\alpha)$ und v_0 die Einschränkung von w_0 auf $K(t)$. Dann ist

$$v_0(t) = w_0(t) = w_0(\alpha^n - \alpha^{n-1}) = (n-1)w_0(\alpha) = n-1.$$

v_0 ist folglich die $(n-1)$-fache t-adische Bewertung auf $K(t)$, denn nur die t-adische Bewertung auf $K(t)$ nimmt auf t einen positiven Wert an. Also ist der Verzweigungsindex $e(w_0/v_0) = n-1$, und es kann höchstens eine weitere (träge und unverzweigte) Fortsetzung von v_0 geben. ■Beh.B.1

Behauptung B.2: w_0 verzweigt nicht in L.

Es sei wieder $g(X) = X^{n-1} + (1-\frac{1}{\alpha})(X^{n-2} + X^{n-3} + \cdots + 1)$; dann ist

$$\begin{aligned}\alpha X^{n-1} g\left(\tfrac{1}{X}\right) &= \alpha X^{n-1}\left(\tfrac{1}{X^{n-1}} + (1-\tfrac{1}{\alpha})(\tfrac{1}{X^{n-2}} + \cdots + 1)\right)\\ &= \alpha + (\alpha-1)(X + X^2 + \cdots + X^{n-1}) =: h(X).\end{aligned}$$

Demzufolge ist L der Zerfällungskörper von h über $K(\alpha)$.
Es ist $w_0(\alpha) = 1$ und $w_0(\alpha - 1) = w_0(1) = 0$, also ist $h(X) \in \mathcal{O}_{w_0}[X]$. Im Restklassenkörper wird h zu dem Polynom

$$\overline{h}^0(X) = -(X^{n-1} + \cdots + X) = -X(X^{n-2} + \cdots + 1) = -X\frac{X^{n-1}-1}{X-1}.$$

Wegen $p \nmid (n-1)$ ist das Kreisteilungspolynom $X^{n-1} - 1$ separabel, und damit auch $\overline{h}^0(X)$. Mit der gleichen Argumentation wie bei w_∞ folgt auch hier, daß $L \supseteq K(\alpha)$ bzgl. w_0 unverzweigt ist. ■Beh.B.2

Teil C: Die Stelle bei b.

Behauptung C.1: Der Verzweigungsindex von $K(\alpha) \supset K(t)$ bzgl. der $(t-b)$-adischen Bewertung auf $K(t)$ ist 2.

Es sei w_a die $(\alpha - a)$-adische Bewertung auf $K(\alpha)$ und v_b die $(t-b)$-adische Bewertung auf $K(t)$. Es ist $b = -\left(\frac{1}{n}\right)\left(\frac{n-1}{n}\right)^{n-1}$ und

$$t - b = \alpha^n - \alpha^{n-1} + \left(\frac{1}{n}\right)\left(\frac{n-1}{n}\right)^{n-1} =: f_b(\alpha).$$

a ist (genau) doppelte Nullstelle von $f_b(\alpha)$, denn $f_b(a) = 0$ gilt nach Definition von b; weiter ist $f_b'(\alpha) = n\alpha^{n-2}\left(\alpha - \frac{n-1}{n}\right)$, also ist a einfache Nullstelle von f_b'. Demnach ist

$$w_a(t-b) = 2 = 2v_b(t-b),$$

w_a ist folglich Fortsetzung von $2v_b$; der Verzweigungsindex ist 2. ■Beh.C.1

Behauptung C.2: w_a verzweigt nicht in L.

g und h seien wie in 2). Wegen $w_a(\alpha) = w_a(1) = 0$ liegt h auch in $\mathcal{O}_{w_a}[X]$. Es ist $\alpha - a \in \mathcal{M}_{w_a}$ und daher $(\alpha - 1) + \mathcal{M}_{w_a} = (\alpha - a + a - 1) + \mathcal{M}_{w_a} = (a-1) + \mathcal{M}_{w_a}$ und $\alpha + \mathcal{M}_{w_a} = a\mathcal{M}_{w_a}$; im Restklassenkörper gilt daher

$$\overline{h}^a(X) = (a-1)(X^{n-1} + \cdots + X) + a = (a-1)(X^{n-1} + \cdots + X + (1-n)).$$

Es ist

$$\begin{aligned}
\tfrac{1}{a-1}(X-1)\overline{h}^a(X) &= X^n \quad +X^{n-1} \quad + \cdots \quad +X^2 \quad +(1-n)X \\
&\qquad\qquad -X^{n-1} \quad - \cdots \quad -X^2 \qquad\qquad -X \quad -(1-n)) \\
&= X^n - nX - (1-n) =: p(X).
\end{aligned}$$

Die Nullstellen von $p'(X) = n(X^{n-1} - 1)$ sind gerade die $(n-1)$-ten Einheitswurzeln. Ist eine solche Einheitswurzel ζ Nullstelle von p, so gilt $\zeta(1-n) = 1-n$, also $\zeta = 1$. Folglich ist 1 die einzige mehrfache Nullstelle von p, und $\overline{h}^a(X) = \frac{p(x)}{X-1}$ hat demnach keine doppelte Nullstelle. Wieder folgt also, daß es keine verzweigte Fortsetzung von w_a auf L gibt. ■Beh.C.2

■Theorem

Theorem 4.6. *Die Bezeichnungen seien wie in Theorem 4.5. Dann sind die einzigen drei auf K trivialen Bewertungen von $K(t)$, die nach L verzweigen, die zu den Stellen bei ∞, 0 und b gehörigen Bewertungen.*

Beweis: Sei v eine beliebige Bewertung auf $K(t)$ außer der Gradbewertung. Dann ist $v(t) \geq 0$, also liegt $f(X)$ in $\mathcal{O}_v[X]$. Das Polynom f ist irreduzibel und normiert, also auch separabel, denn sonst wäre $f(X) = g(X^p)$ für ein $g(X) \in K(t)[X]$. Aus Lemma 4.3 folgt

$$v(D(f)) = v(\pm n^n t^{n-2}(t-b)) = v(t^{n-2}) + v(t-b).$$

Gehört nun v nicht zu den Stellen bei 0 oder b, so folgt hieraus $v(D(f)) = 0$, also liegt $D(f)$ nicht in $\mathcal{M}_v$. Theorem 1.26 besagt nun, daß v in L nicht verzweigt. ∎

Theorem 4.7. *Die Bezeichnungen seien wie in Theorem 4.5. Dann ist $G \cong S_n$.*

Wir zeigen, daß G einen $(n-1)$-Zykel und eine Transposition enthält und wenden dann Lemma 4.4 an.

Beweis: Die Bezeichnungen seien wie im Beweis von Theorem 4.5. Es sei $\widetilde{w}$ eine Fortsetzung von $w := w_\infty$ (bzw. von $w := w_0$, $w := w_a$) auf L und es sei $v := v_\infty$ (bzw. $v := v_0$, $v := v_b$). Weiter sei T die Trägheitsgruppe und V die Verzweigungsgruppe von $(L, \widetilde{w})/(K(t), v)$ und $s := n$ (bzw. $s := n-1$, $s := 2$).

Behauptung 1): T enthält eine zyklische Untergruppe T' der Ordnung s mit $T' \cap V = \{1\}$.

Wegen $p \nmid n(n-1)$ sind s und p teilerfremd (aus $p \nmid n(n-1)$ folgt $p \neq 2!$), also ist wegen Theorem 1.22

$$T/V \cong (\Gamma_{\widetilde{w}}/\Gamma_v)_{p'} \cong \mathbb{Z}_s.$$

Es sei etwa $T/V = \langle \tau V \rangle$. Da V eine p-Gruppe ist, gilt $\operatorname{ord}(\tau) = sp^k$ für ein $k \in \mathbb{N}$. Sei $\sigma = \tau^{p^k}$; dann hat σ die Ordnung s. Es sei $T' := \langle \sigma \rangle$. Da s und p teilerfremd sind, gilt $T' \cap V = \{1\}$. ∎Beh.1)

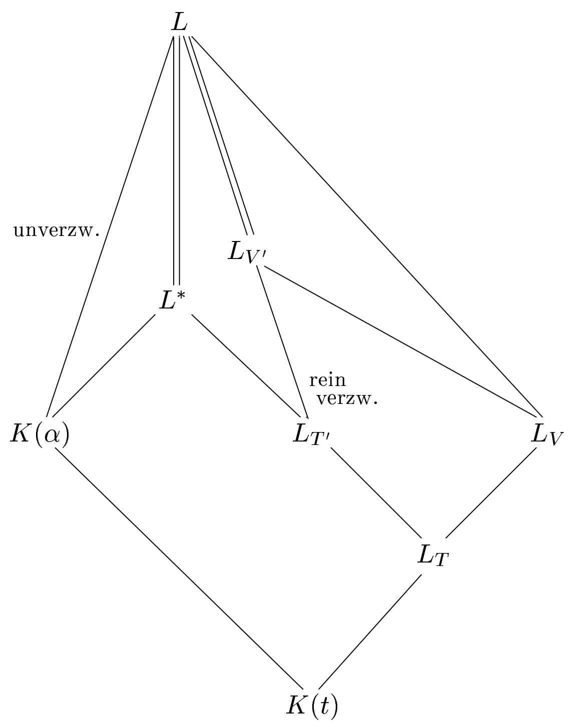
Behauptung 2): Es gilt $T' \cap H = \{1\}$; dabei ist $H := \operatorname{Gal}\big(L/K(\alpha)\big)$ wie in Theorem 4.5.

Das nächste Bild dient der Illustration des Beweises.
Es sei $L_T := \operatorname{Fix}(T)$, $L_{T'} := \operatorname{Fix}(T')$ und $L_V := \operatorname{Fix}(V)$; weiter seien w_T und $w_{T'}$ die Einschränkungen von $\widetilde{w}$ auf L_T und $L_{T'}$. Dann gilt für die Verzweigungsgruppe V' von $(L, \widetilde{w})/(L_{T'}, w_{T'})$

$$\begin{aligned} V' &= \{h \in \operatorname{Gal}(L/L_{T'}) \mid \text{ f. a. } x \in \mathcal{O}_{\widetilde{w}} \text{ ist } h(x) - x \in x\mathcal{M}_{\widetilde{w}}\} \\ &= \{h \in \operatorname{Gal}(L/L_T) \mid \text{ f. a. } x \in \mathcal{O}_{\widetilde{w}} \text{ ist } h(x) - x \in x\mathcal{M}_{\widetilde{w}}, h \in \operatorname{Gal}(L/L_{T'})\} \\ &= V \cap T' = \{1\}. \end{aligned}$$

Angenommen es ist $T' \cap H \neq \{1\}$, etwa $g \in T' \cap H$ mit $g \neq 1$. Dann ist $L^* := \operatorname{Fix}(\{g\})$ ein echter Unterkörper von L, der $K(\alpha)$ und $L_{T'}$ enthält. Es sei $w^* := \widetilde{w}|_{L^*}$.

$w_{T'}$ hat genauso wie w_T nur eine Fortsetzung auf L. Die Restklassenkörpererweiterung von $(L, \widetilde{w})/(L_T, w_T)$ ist rein inseparabel, also auch die von $(L, \widetilde{w})/(L_{T'}, w_{T'})$. Aus $V' = \{1\}$ folgt, daß die Erweiterung $(L, \widetilde{w})/(L_{T'}, w_{T'})$ auch keine inseparable Restklassenkörpererweiterung besitzt, und daß für den Defekt $d(\widetilde{w}/w_{T'}) = 1$ gilt. Folglich ist $[L : L_{T'}] = rfde = e$, die Erweiterungen $(L, \widetilde{w})/(L_{T'}, w_{T'})$ und damit auch $(L, \widetilde{w})/(L^*, w^*)$ sind demzufolge rein verzweigt. Andererseits haben wir im Beweis von Theorem 4.5 gezeigt, daß $(L, \widetilde{w})/(K(\alpha), w)$, und damit auch $(L, \widetilde{w})/(L^*, w^*)$, unverzweigt sind. Die Erweiterung $(L, \widetilde{w})/(L^*, w^*)$ ist ergo rein verzweigt und unverzweigt; demnach gilt $L = L^*$. Widerspruch!



■Beh.2)

<u>Behauptung 3):</u> Das erzeugende Element σ von T' ist ein s-Zykel (wobei T' als Permutationsgruppe auf den Wurzeln von f aufgefaßt wird).

Wir betrachten die Bahn von α unter T'. Gilt $\sigma^i(\alpha) = \alpha$ für ein $i \leq s$, so ist $\mathrm{Fix}(\{\sigma^i\}) \supseteq K(\alpha)$, das heißt es ist $\sigma^i \in T' \cap H = \{1\}$, es ist also $i = s$. Für $s = n$ und $s = n-1$ folgt hieraus schon, daß σ ein s-Zykel ist, denn ein Element der Ordnung n (bzw. $(n-1)$) in der S_n ist ein n-Zykel (bzw ein $(n-1)$ Zykel). Der Fall $s = 2$ ist etwas komplizierter:

Es seien $\alpha_1 := \alpha, \ldots \alpha_n$ die verschiedenen Nullstellen von f. Nach Lemma 4.3 gilt für die Diskriminante $D(f)$

$$D(f) = \prod_{i \neq j} (\alpha_i - \alpha_j) = \pm n^n t^{n-2}(t-b).$$

Wie wir im Beweis von Theorem 4.5 festgestellt haben, gilt dann

$$\begin{aligned} \widetilde{w}(D(f)) &= \widetilde{w}(t-b) = 2 \\ &= \widetilde{w}(\alpha - \sigma(\alpha)) + \widetilde{w}(\sigma(\alpha) - \alpha) + \sum_{\substack{\alpha_i \neq \alpha_j \\ (\alpha_i,\alpha_j) \neq (\alpha,\sigma(\alpha)),(\sigma(\alpha),\alpha)}} \widetilde{w}(\alpha_i - \alpha_j). \end{aligned}$$

Das Polynom f liegt in $\mathcal{O}_v[X] \subseteq \mathcal{O}_{\widetilde{w}}[X]$. Da $\mathcal{O}_{\widetilde{w}}$ ganz abgeschlossen in L ist, liegen alle Nullstellen α_i von f in $\mathcal{O}_{\widetilde{w}}$. Also gilt $\widetilde{w}(\alpha_j - \alpha_i) \geq \min\{\widetilde{w}(\alpha_j), \widetilde{w}(\alpha_i)\} = 0$ für alle $i, j \in \{1, \ldots, n\}$. Angenommen für ein $\alpha_i \neq \alpha, \sigma(\alpha)$ gilt $\sigma(\alpha_i) \neq \alpha_i$. Da σ in T liegt, gilt dann $\sigma(\alpha_i) - \alpha_i \in \mathcal{M}_{\widetilde{w}}$, also ist $\widetilde{w}(\sigma(\alpha_i) - \alpha_i) \geq 1$. Demnach folgt

$$\widetilde{w}(D(f)) = \overbrace{2\widetilde{w}(\alpha - \sigma(\alpha))}^{=2} + \overbrace{2\widetilde{w}(\alpha_i - \sigma(\alpha_i))}^{\geq 2} + \overbrace{\sum_{\substack{\alpha_j \neq \alpha_k \\ (\alpha_j,\alpha_k)\neq(\alpha,\sigma(\alpha)),(\sigma(\alpha),\alpha) \\ (\alpha_j,\alpha_k)\neq(\alpha_i,\sigma(\alpha_i)),(\sigma(\alpha_i),\alpha_i)}} \widetilde{w}(\alpha_j - \alpha_k)}^{\geq 0} \geq 4.$$

Widerspruch! ■Beh.3)

Insgesamt folgt also, daß G einen n-Zykel, einen $(n-1)$-Zykel und eine Transposition enthält. G operiert als Galoisgruppe außerdem transitiv; mit Lemma 4.4 folgt also $G \cong S_n$. ■Theorem

Aus dem letzten Satz folgt nun leicht die reguläre Realisierbarkeit der A_n:

Korollar 4.8. *Es sei K ein Körper der Charakteristik p und es sei v transzendent über K. Weiter sei $n \in \mathbb{N}$, $n > 2$ mit $p \nmid n(n-1)$. Dann existiert eine Galoiserweiterung $L' \supseteq K(v)$, so daß gilt:*

1) $\mathrm{Gal}(L'/K(v)) \cong A_n$.

2) Die Erweiterung $L' \supset K$ ist regulär.

Beweis: **Zu 1):** Es seien L und G wie in Theorem 4.5. Nach Theorem 4.7 folgt dann $G \cong S_n$. Es sei A die der alternierenden Gruppe entsprechende Untergruppe von G und $F := \mathrm{Fix}(A)$. Dann ist $[F : K(t)] = 2$; also entsteht F durch Adjunktion einer Quadratwurzel an $K(t)$. Demnach existieren Polynome $p_1, \dots p_r$ und $q_1, \dots, q_s$ bzw. ohne Einschränkung $p_1, \dots p_r$ und $q_1, \dots, q_r$ aus $K[t]$ mit

$$F = K(t)\left(\prod_{i=1}^{r} \frac{\sqrt{p_i}}{\sqrt{q_i}}\right) = K(t)\left(\prod_{i=1}^{r} \frac{\sqrt{p_i}}{\sqrt{q_i}} \cdot q_i\right) = K(t)(\prod_{i=1}^{r} \sqrt{p_i}\sqrt{q_i}).$$

Ohne Einschränkung ist also $F = K(t)(\prod_{i=1}^{r} \sqrt{p_i})$ mit irreduziblen und paarweise verschiedenen $p_i \in K[t]$.

Angenommen es ist $p_i = \mathrm{Irr}(c_i, K)$ für $i \in \{1, \dots, r\}$ und $c_i \in K^{\mathrm{a}}$. Es sei v_{c_i} die zur Stelle bei c_i gehörige Bewertung auf $K(t)$ und $\widetilde{v_{c_i}}$ eine beliebige Fortsetzung auf F. Dann ist

$$1 = v_{c_i}(p_i) = \widetilde{v_{c_i}}(p_i) = 2\widetilde{v_{c_i}}(\sqrt{p_i});$$

für alle anderen p_j $(j \neq i)$ gilt $\widetilde{v_{c_i}}(p_j) = 0$. Insgesamt gilt demnach

$$\widetilde{v_{c_i}}(\prod_{i=1}^{r} \sqrt{p_i}) = \frac{1}{2},$$

die Bewertung v_{c_i} verzweigt also von $K(t)$ nach F und deshalb auch nach L. Wegen Theorem 4.6 können die p_i daher nur die Form $p_i(t) = t$ oder $p_i(t) = (t-a)$ haben. Ist $\prod_{i=1}^{r} \sqrt{p_i} = t$ oder $\prod_{i=1}^{r} \sqrt{p_i} = t - a$, so ist $F = K(\sqrt{t})$ bzw. $F = K(\sqrt{t-a})$ wieder ein rationaler Funktionenkörper über K.

Sei also $\prod_{i=1}^{r} \sqrt{p_i} = t(t-a) =: u^2$ und $v := t - u$. Dann gilt $K(v) = F = K(t, u)$: Es ist $\frac{v^2}{2v-a} = t$, denn es gilt

$$\begin{aligned} t(2v-a) = v^2 &\iff 2t^2 - 2ut - ta = t^2 - 2ut + u^2 \\ &\iff t^2 - ta = u^2 \\ &\iff t^2 - ta = t^2 - ta. \end{aligned}$$

Also ist $t \in K(v)$ und auch $u = t - v \in K(v)$, damit ist F auch in diesem Fall rationaler Funktionenkörper über K.
Demnach ist F in allen drei Fällen über K isomorph zu $K(t)$; die Fortsetzung dieses Isomorphismus' auf die algebraischen Abschlüsse überführt L in eine Galoiserweiterung L' von $K(t')$ mit Galoisgruppe $G' \cong A_n$, wobei t' transzendent über K ist. ■1)

Zu 2): Da $L' \supset K$ separabel ist, bleibt nur noch zu zeigen, daß $L' \supset K$ primär ist; dies ist äquivalent dazu, daß $L' \cap K^{\mathrm{s}} = K$ gilt.
Die Erweiterung $L \supset K(t)$ hat bezüglich der Gradbewertung den Verzweigungsindex $n > 2$; der entsprechende Verzweigungsindex der Erweiterung $L \supset F$ muß also größer als 1 sein. Demnach ist auch der der Gradbewertung entsprechende Verzweigungsindex von $L' \supset K(t)$ größer als 1.
Angenommen es ist $L' \cap K^{\mathrm{s}} := M \supsetneq K$ eine Erweiterung von Grad $k > 1$. Dann ist $M(t) \supsetneq K(t)$ galoissche Zwischenerweiterung von Grad k von $L' \supset K(t)$. Da $\mathrm{Gal}(L'/K(t)) \cong A_n$ einfach ist, muß dann schon $M(t) = L'$ gelten. Nach Lemma 1.29 ist $L' \supseteq K(t)$ dann bzgl. der Gradbewertung unverzweigt. Widerspruch! ■2)

4.2 Reguläre Realisierung von großen direkten Produkten der alternierenden Gruppe

Bevor wir zum Beweis von Theorem 4.1 kommen, benötigen wir noch einige Lemmata:

Lemma 4.9. *Die Gruppe G sei (inneres) direktes Produkt der Normalteiler $G_1 \trianglelefteq G$ und $G_2 \trianglelefteq G$. Für $i \in \{1,2\}$ sei $N_i \trianglelefteq G_i$ mit $G_1/N_1 \cong G_2/N_2$, weiter sei $H \trianglelefteq G$ mit $HG_i = G$ und $H \cap G_i = N_i$.*
Dann ist $H/N_1N_2 \cong G_i/N_i$ und G_i/N_i ist abelsch.

Zur Veranschaulichung ein Beispiel: Es sei $n \in \mathbb{N}$. Für $i \in \{1,2\}$ sei $G_i \cong S_n$ und $H = \{\sigma_1\sigma_2 \mid \sigma_i \in G_i, \operatorname{sign}(\sigma_1) = \operatorname{sign}(\sigma_2)\}$, wobei sign jeweils die von der S_n auf G_i induzierte Signumfunktion sei. N_i sei die der A_n entsprechenden Untergruppe in G_i. Es ist $H \trianglelefteq G$, für $i = 1, 2$ gilt jeweils $HG_i = G$, und der Schnitt von H und G_i ist jeweils N_i. Dann ist $H/(N_1 \times N_2) \cong \mathbb{Z}_2$ abelsch.

Beweis: Das Produkt N_1N_2 der Normalteiler $N_i \trianglelefteq G_i$ ist offensichtlich wieder ein Normalteiler im Produkt $G_1G_2 = G$. Wegen $H \cap G_i = N_i$ ist außerdem $N_1N_2 \subseteq H$, das heißt N_1N_2 ist Normalteiler von H. Seien fortan $g_i, g_i' \in G_i$.

Behauptung 1): Es gilt $H/N_1N_2 \overset{\varphi}{\cong} G_1/N_1$ via $g_1g_2N_1N_2 \overset{\varphi}{\mapsto} g_1N_1$.
Ist $g_1g_2N_1N_2 = g_1'g_2'N_1N_2$, so ist $g_1'g_2'g_1^{-1}g_2^{-1} = g_1'g_1^{-1}g_2'g_2^{-1} \in N_1N_2$ und damit auch $g_1'g_1^{-1} \in N_1$, das heißt die Abbildung ist wohldefiniert. Weiter ist φ ein Homomorphismus. Wegen $HG_2 = G$ existiert zu jedem $g_1 \in G_1$ ein $h \in H$ und ein $g_2 \in G_2$ mit $g_1 = hg_2$, also $h = g_1g_2^{-1}$; dann ist $\varphi(hN_1N_2) = g_1N_1$, φ ist also surjektiv.
Zur Injektivität von φ: Sei $g_1g_2N_1N_2 \in \ker(\varphi)$. Dann ist $g_1 \in N_1 \subseteq H$. Also ist mit g_1 und g_1g_2 auch $g_2 \in H$; außerdem ist $g_2 \in G_2$, also insgesamt $g_2 \in H \cap G_2 = N_2$. Also ist $g_1g_2 \in N_1N_2$. ■Beh.1)

Behauptung 2): G_1/N_1 ist abelsch.
Für alle $g_1 \in G_1$ existiert ein $g_2 \in G_2$ mit $g_1g_2 \in H \trianglelefteq G$. Für alle $\lambda_1 \in G_1$ ist $(g_1g_2)^{\lambda_1}(g_1g_2)^{-1} = g_1^{\lambda_1}g_2g_2^{-1}g_1 = g_1^{\lambda_1}g_1^{-1} \in H$. Wegen $H \cap G_1 = N_1$ bedeutet dies gerade $\mathrm{Komm}(G_1) \subseteq N_1$, das heißt G_1/N_1 ist abelsch. ■Beh.2)
Entsprechendes gilt für G_2/N_2. ■

Lemma 4.10. *Es sei K ein Körper, $L \supseteq K$ und $R \supseteq K$ seien beliebige Galoiserweiterungen und $M \supseteq K$ sei eine endliche Galoiserweiterung von K. Die Körper L, M und R seien paarweise linear disjunkt über K. Weiter sei $B := \mathrm{Gal}(M/K)$ eine nichtabelsche Gruppe. Dann ist LMR eine echte Erweiterung von LR.*

Beweis: Wegen $L \underset{K}{\overset{l}{\perp}} R$ ist $G := \mathrm{Gal}(LR/K)$ direktes Produkt der Normalteiler $G_L := \mathrm{Gal}(LR/R) \trianglelefteq G$ und $G_R := \mathrm{Gal}(LR/L) \trianglelefteq G$.
Angenommen es ist $LR = LMR$; das Bild auf der nächsten Seite dient der Veranschaulichung des Beweises. Da $M \supset K$ normal ist, ist $H := \mathrm{Gal}(LMR/M) = \mathrm{Gal}(LR/M)$ normal in G. Die Erweiterungen $LM \supseteq M$ und $MR \supseteq R$ sind normal, also ist $N_L := \mathrm{Gal}(LR/MR) \trianglelefteq G_L$ und $N_R := \mathrm{Gal}(LR/LM) \trianglelefteq G_R$.
Nun ist $H \cap G_L = \mathrm{Gal}(LR/M) \cap \mathrm{Gal}(LR/R) = \mathrm{Gal}(LR/MR) = N_L$. Weiter ist $HG_L = \mathrm{Gal}(LR/M)\mathrm{Gal}(LR/R) = \mathrm{Gal}(LR/M \cap R) = \mathrm{Gal}(LR/K) = G$; entsprechendes gilt für $H \cap G_R$ und HG_R. Wegen Lemma 4.9 ist $G_L/N_L \cong \mathrm{Gal}(LM/L) \cong \mathrm{Gal}(M/K)$ dann abelsch. Widerspruch! ■

Lemma 4.11. *Für $i \in I$ sei G_i eine nicht-abelsche einfache Gruppe mit neutralem Element e_i, weiter sei $G := \prod_{i \in I} G_i$ das (äußere) direkte Produkt der G_i und N ein Normalteiler von G. Dann ist für $I_0 = \{j \in I \mid$ es existiert $n = (n_i)_{i \in I} \in N$ mit $n_j \neq e_j\}$ bis auf eine Umordnung der Indizes*

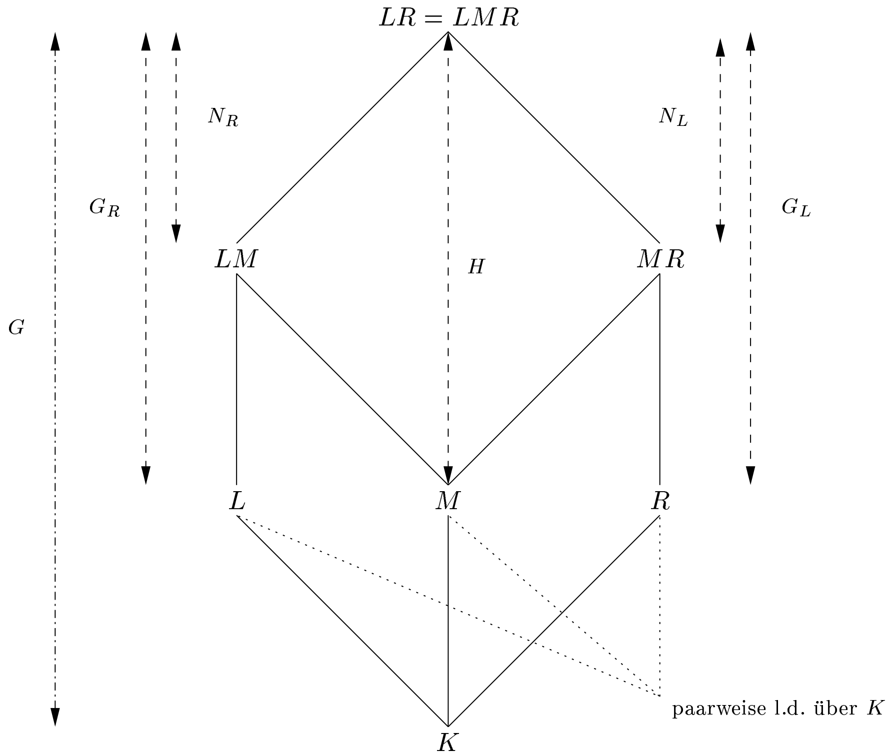
$$N = \prod_{i \in I_0} G_i \times \prod_{i \in I \setminus I_0} \{e_i\}.$$

Ist zum Beispiel $n \in \mathbb{N}$, $n > 4$ und $G_i \cong A_n$ für $i \in I$, so gibt es keine „diagonal" in G liegenden Normalteiler; normale Untergruppen sind genau die direkten Produkte, die in jeder Komponente $j \in I$ entweder die ganze Gruppe $G_i \cong A_n$ oder aber nur das neutrale Element e_i enthalten.

Beweis: Ich zeige: Ist $j \in I_0$, so ist $G_j \times \prod_{i \neq j}\{e_j\} \subseteq N$.
Ohne Einschränkung sei I eine Kardinalzahl und $j = 0$; weiter sei $n = (n_i)_{i \in I} \in$

N mit $n_0 \neq e_0$. Dann ist für alle $\lambda_0 \in G_0$ auch $(n_0^{\lambda_0}, n_1, n_2, \ldots) \in N$, weiter ist $(n_0^{-1}, n_1^{-1}, n_2^{-1}, \ldots) \in N$, also ist auch $(n_0^{-1} n_0^{\lambda_0}, e_1, e_2, \ldots) = ([n_0, \lambda_0], e_1, e_2, \ldots) \in N$. Da das Zentrum von G_0 trivial ist, existiert also ein $g_0' \in G_0$, $g_0' \neq e_0$ mit $(g_0', e_1, e_2, \ldots) \in N$. Da G_0 einfach ist, ist dann für alle $g_0 \in G_0$ jeweils $(g_0, e_1, e_2, \ldots) \in N$. ∎

Zum Beweis von Lemma 4.10:



Beweis von Theorem (4.1):

Sei K eine abzählbare elementare Unterstruktur von F und $\{b_i \mid i < |F|\}$ eine Transzendenzbasis von F über K. Nach Lemma 4.8 existiert für alle $i < |F|$ eine Galoiserweiterung L_i von $K(b_i t)$, so daß $L_i \supset K$ regulär ist und $\mathrm{Gal}(L_i/K(b_i t)) \cong A_n$ gilt.

Sei $M_i := L_i(t)F$. Dann gilt

$$\begin{aligned}\mathrm{Gal}(M_i/F(t)) &\cong \mathrm{Gal}(L_i(t)/K(b_i, t)) \\ &\cong \mathrm{Gal}(L_i/K(b_i t) \\ &\cong A_n,\end{aligned}$$

und die Erweiterungen $M_i \supset F$ sind regulär. Ebenso sind die Erweiterungen $L_i(t) \supset K(b_i)$ und $L_i(t) \supset K(t)$ regulär (siehe Bild).

$$
\begin{tikzcd}[column sep=small]
 & & M_i \\
 & L_i(t) \arrow[ur, dash] & \\
L_i \arrow[ur, dash] & \arrow[r, phantom, "\text{l.d.}"] & F(t) \arrow[uu, dash, "A_n"'] \\
\arrow[r, phantom, "\text{l.d.}"] & K(b_i,t) \arrow[ur, dash] \arrow[uu, dash, "A_n"'] & \\
K(b_it) \arrow[ur, dash] \arrow[uu, dash, "A_n"] & \arrow[r, phantom, "\text{l.d.}"] & F \arrow[uu, dash] \\
\arrow[r, phantom, "\text{l.d.}"] & \left\{\begin{matrix} K(b_i) \\ K(t) \end{matrix}\right\} \arrow[ur, dash] \arrow[uu, dash] & \\
K \arrow[ur, dash] \arrow[uu, dash] & &
\end{tikzcd}
$$

reg. reg.

<u>Behauptung:</u> Für $i < |F|$ sind die Erweiterungen M_i linear disjunkt über $F(t)$.

Angenommen es gibt ein $i < |F|$ mit $M_i \underset{F(t)}{\not\perp^l} M_i^C$ für $M_i^C := \prod_{\substack{j<|F| \\ j\neq i}} M_j$; ohne Einschränkung sei $i = 0$. Da $M_0 \supset F(t)$ galoissch ist, ist dies wegen Bemerkung 1.5.5 äquivalent zu $M_0 \cap M_0^C \supsetneq F(t)$. Da $\mathrm{Gal}(M_i/F(t))$ einfach ist, folgt sogar $M_0 \subseteq M_0^C$ und erst recht $L_0(t) \subset M_0^C$.

Da für alle $j < |F|$ der Körper M_j in $K(b_j, t)^{\mathrm{a}}F$ liegt, gilt

$$M_0^C \subseteq \prod_{1\leq j<|F|} K(b_j,t)^{\mathrm{a}}F \subseteq K(t,(b_j)_{1\leq j<|F|})^{\mathrm{a}}F^{\mathrm{a}},$$

also auch $L_0(t) \subseteq (K(t,(b_j)_{1\leq j<|F|}))^{\mathrm{a}}F^{\mathrm{a}}$. Außerdem gilt $L_0(t) \subseteq (K(b_0,t))^{\mathrm{a}}$.

Da die Elemente t und $(b_j)_{j<|F|}$ algebraisch unabhängig über K sind, gilt

$$K(t,b_0) \underset{K}{\overset{a}{\perp}} K((b_j)_{1\leq j<|F|}),$$

und daher auch

$$K(t)^{\mathrm{a}}K(b_0)^{\mathrm{a}} \underset{K^{\mathrm{a}}}{\overset{a}{\perp}} K((b_j)_{1\leq j<|F|})^{\mathrm{a}}.$$

Wendet man Lemma 2.15 an (wobei K^{a}, $(K(t))^{\mathrm{a}}$, $(K(b_0))^{\mathrm{a}}$ und $(K((b_j)_{1\leq j<|F|}))^{\mathrm{a}}$ den Körpern K, A, B und C entsprechen), so erhält man

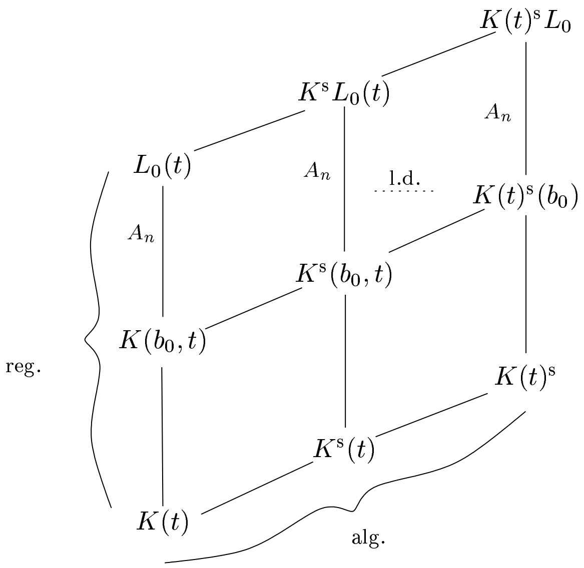
$$K(t,b_0)^{\mathrm{a}} \cap K(t,(b_j)_{1\leq j<|F|})^{\mathrm{a}}F^{\mathrm{a}} = K(t)^{\mathrm{a}}K(b_0)^{\mathrm{a}},$$

also ist $L_0(t) \subseteq (K(t))^{\mathrm{a}}(K(b_0))^{\mathrm{a}}$.

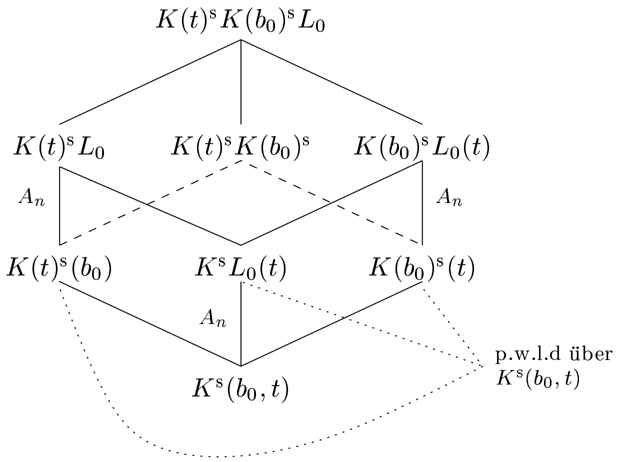
Nun ist $L_0(t) \supset K(t,b_0)$ separabel algebraisch, also in $K(t,b_0)^{\mathrm{s}}$ enthalten. Die Erweiterung $K(t,b_0)^{\mathrm{s}} \supseteq K(t)^{\mathrm{s}}K(b_0)^{\mathrm{s}}$ ist separabel. Dagegen ist die Erweiterung $K(t)^{\mathrm{a}}K(b_0)^{\mathrm{a}} \supseteq K(t)^{\mathrm{s}}K(b_0)^{\mathrm{s}}$ rein inseparabel, also ist $K(t,b_0)^{\mathrm{s}}$ linear disjunkt von $K(b_0)^{\mathrm{a}}K(t)^{\mathrm{a}}$ über $K(t)^{\mathrm{s}}K(b_0)^{\mathrm{s}}$. Demnach gilt sogar

$$\boxed{L_0(t) \subseteq K(t,b_0)^{\mathrm{s}} \cap K(b_0)^{\mathrm{a}}K(t)^{\mathrm{a}} = K(t)^{\mathrm{s}}K(b_0)^{\mathrm{s}} \qquad (*)}$$

Da $L_0(t) \supset K(t)$ regulär ist und $K(t)^{\mathrm{s}} \supset K(t)$ algebraisch, sind $L_0(t)$ und $K(t)^{\mathrm{s}}$ linear disjunkt über $K(t)$, wegen der Turmeigenschaft gilt also $K^{\mathrm{s}}L_0(t) \underset{K^{\mathrm{s}}(b_0,t)}{\overset{l}{\downarrow}} K(t)^{\mathrm{s}}(b_0)$ und es ist $\mathrm{Gal}(K^{\mathrm{s}}L_0(t)/K^{\mathrm{s}}(b_0,t)) \cong A_n$. Da auch $L_0(t) \supset K(b_0)$ regulär und $K(b_0)^{\mathrm{s}} \supset K(b_0)$ algebraisch ist, gilt auch $K^{\mathrm{s}}L_0(t) \underset{K^{\mathrm{s}}(b_0,t)}{\overset{l}{\downarrow}} K(b_0)^{\mathrm{s}}(t)$ (siehe Bild).



Außerdem sind $K(t)^{\mathrm{s}}(b_0)$ und $K(b_0)^{\mathrm{s}}(t)$ linear disjunkt über $K^{\mathrm{s}}(t,b_0)$, denn aus $K(t) \underset{K}{\overset{l}{\downarrow}} K(b_0)$ folgt mit der Bemerkung nach Lemma 1.16 auch $K(t)^{\mathrm{s}} \underset{K^{\mathrm{s}}}{\overset{l}{\downarrow}} K(b_0)^{\mathrm{s}}$ und mit der Turmeigenschaft $K(t)^{\mathrm{s}}(b_0) \underset{K^{\mathrm{s}}(t,b_0)}{\overset{l}{\downarrow}} K(b_0)^{\mathrm{s}}(t)$. Demnach sind $K^{\mathrm{s}}L_0(t)$, $K(b_0)^{\mathrm{s}}(t)$ und $K(t)^{\mathrm{s}}(b_0)$ paarweise linear disjunkt über $K^{\mathrm{s}}(b_0,t)$. Die Situation ist also wie folgt:



$\mathrm{Gal}(K^{\mathrm{s}}L_0(t)/K^{\mathrm{s}}(b_0,t)) \cong A_n$ ist nicht abelsch. Lemma 4.10 besagt dann aber, daß

L_i eine echte Erweiterung von $K(t)^{\mathrm{s}}K(b_i)^{\mathrm{s}}$ ist; dies ist ein Widerspruch zu $(*)$!
Also sind die Erweiterungen M_i $(i < |F|)$ linear disjunkt über $F(t)$. ■Beh.

Sei nun $M := \prod_{i<|F|} M_i$; dann ist mit Lemma 1.3

$$\mathrm{Gal}(M/F(t)) \cong \prod_{|F|} A_n.$$

Es bleibt also noch die Regularität von M über F zu zeigen (siehe nächstes Bild): Es ist klar, daß die Erweiterung separabel ist. Angenommen $M \supset F$ ist nicht primär, das heißt es ist $M \cap F^{\mathrm{s}} \supsetneq F$. Dann ist schon der Schnitt des Kompositums von endlich vielen M_i mit F^{s} eine echte Erweiterung von F; es sei also ohne Einschränkung $M_1 \cdots M_r \cap F^{\mathrm{s}} =: M' \supsetneq F$.

Es sei $\bar{M} := M_1 \cdots M_r$. Mit $M' \supsetneq F$ ist wegen $M' \underset{F}{\overset{l}{\smile}} F(t)$ auch $M'(t) \supsetneq F(t)$ eine echte Erweiterung. Da $M' \supset F$ normal ist, ist auch $M'(t) \supset F(t)$ normal. Also ist

$$N := \mathrm{Gal}(\bar{M}/M'(t)) \trianglelefteq \mathrm{Gal}(\bar{M}/F(t)) \overset{\varphi}{\cong} \prod_{r\text{- mal}} A_n$$

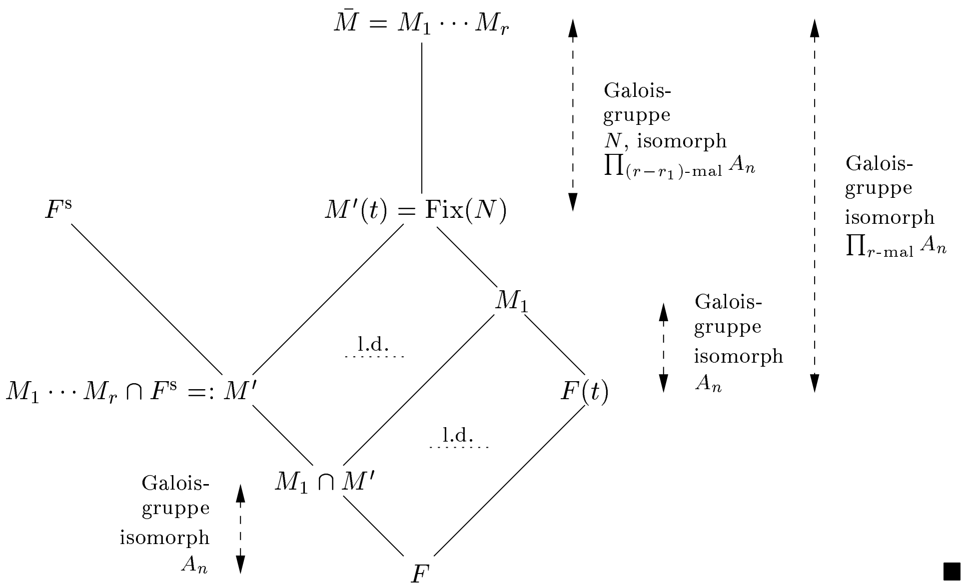
ein echter Normalteiler von $\mathrm{Gal}(\bar{M}/F(t))$. Nach Lemma 4.11 gilt dann ohne Einschränkung

$$\varphi|_N(N) = \underbrace{\{e\} \times \ldots \times \{e\}}_{\substack{r_1\text{-mal für ein } r_1 \\ \text{mit } 1 \leq r_1 \leq r}} \times \underbrace{A_n \times \ldots \times A_n}_{r-r_1\text{-mal}},$$

es ist also $M_1 \subseteq M'(t)$. Folglich ist

$$[M_1 : F(t)] = [M_1 \cap M' : F] = [M_1 \cap F^{\mathrm{s}} : F] = \frac{n!}{2} > 1,$$

das heißt $M_1 \supset F$ ist nicht primär und somit auch nicht regulär.



■

Jetzt ist schon ein großer Teil der Arbeit geschafft, und wir können langsam mit den Hauptgängen beginnen:

Fisch unter Kräuterkruste mit lauwarmem Ratatouille-Salat und Polenta-Talern

Fisch (pro Person): einen schönen Mittelmeerfisch (Knurrhahn eignet sich vortrefflich, Rotbarbe und Dorade auch) schuppen, waschen, trocknen, salzen und pfeffern. Aus je einem Eßlöffel gemischten gehackten Kräutern (Rosmarin, Thymian, Salbei, Basilikum...), Semmelbröseln, Butter, gehackten Oliven und geriebenem Parmesan mit etwas Zitronensaft eine Farce rühren. Fisch in eine feuerfeste Form legen, mit 2 bis auf das Fruchtfleisch geschälten Zitronenscheiben füllen und mit der Farce bedecken. Bei 180° C ca. 20-30 Minuten garen.

Ratatouille-Salat (für 4-6 Personen): Je 2 rote und 2 gelbe Paprikaschoten waschen, vierteln und im Ofen grillen, bis die Haut blasen wirft und sich abziehen läßt. 1-2 Auberginen in Alufolie gewickelt im Ofen garen. 400g Buschbohnen in mundgerechte Stücke teilen und in Salzwasser blanchieren. 1-2 junge Zuccini in Würfel schneiden, in Olivenöl andünsten. In Würfel geschnittene Auberginen und Paprika und die Bohnen dazugeben und einige Minuten mitbraten[10]. Vor dem Servieren 4 geschälte und entkernte Tomaten in Stücken zugeben und nach Geschmack 1 oder mehr gepresste Knoblauchzehen zugeben. Mit Salz, Pfeffer, Olivenöl und Aceto Balsamico abschmecken und mit reichlich Basilikum würzen.

Polenta-Taler: 300g Polenta kochen, nach Geschmack frisch geriebenen Parmesan dazugeben, zu einer Rolle formen und in Frischhaltefolie gewickelt kalt stellen. In ca. 1,5 cm dicke Scheiben schneiden und in Salbeibutter goldbraun braten.

[10] Wer mag, kann noch 1-2 in Stücke geschnittene, blanchierte Fenchelknollen hinzufügen.

5 Unbeschränkte PAC-Körper sind nicht einfach

Dieses Kapitel enthält den zentralen Teil dieser Arbeit: Wir zeigen, daß die Theorie eines unbeschränkten PAC-Körpers nicht einfach ist. Im ersten Abschnitt werden wir ein technisches Lemma beweisen, das eine Folgerung aus der Definition einfacher Theorien mittels des lokalen Charakters des Teilens ist; es wird im Beweis eine zentrale Rolle spielen. Im zweiten Teil beschäftigen wir uns mit dem Spezialfall eines PAC-Körpers der Charakteristik $p \neq 2$ mit unendlich vielen quadratischen Erweiterungen. Schließlich enthält der dritte Abschnitt den Beweis des allgemeinen Falls.

5.1 Ein Kriterium für nicht-einfache Theorien

Lemma 5.1. *Sei T eine abzählbare vollständige L-Theorie und $F \models T$. Für $i < \aleph_1$ seien $\varphi_i(x,y)$ $L(F)$-Formeln, so daß gilt:*

Es existiert ein Modell $K \succ F$ und es existieren Elemententupel $(c_i)_{i<\aleph_1}$ aus K, so daß gilt:

1) Die Formelmenge

$$\{\varphi_i(x,c_i) \mid i < \aleph_1\}$$

ist erfüllbar.

2) Für jedes $i < \aleph_1$ existiert $n_i \in \mathbb{N}$, so daß

$$\bigwedge_{0\leq j\leq n_i} \varphi_i(x,y_j) \wedge \bigwedge_{0\leq j<k\leq n_i} y_j \neq y_k$$

inkonsistent ist.

3) Für alle abzählbaren Mengen $B \subset K$ gibt es ein $i < \aleph_1$, so daß $c_i \notin \operatorname{acl}(FB)$ ist.

Dann ist T nicht einfach.

Bemerkung:

1) Das Lemma ist speziell für die Anwendung in der eq-Theorie einer Struktur konstruiert: Die Elemente c_i werden bei späteren Anwendungen fast immer Äquivalenzklassen einer $\emptyset$-definierbaren Äquivalenzrelation sein. Ohne den Übergang von Elementen der Heimsorte zu imaginären Elementen wäre oftmals statt der in 5.1.2 geforderten n_i-Inkonsistenz nur n_i-Konsistenz für paarweise nichtäquivalente Elemente erreichbar.
2) Da L abzählbar ist, muß das Modell F überabzählbar sein, damit man $L(F)$-Formeln $(\varphi_i)_{i<\aleph_1}$ finden kann. Die c_i können paarweise verschieden gewählt werden.
3) Äquivalent zur Existenz von L(F)-Formeln $\big(\varphi_i(x,y)\big)_{i<\aleph_1}$, so daß die Bedingungen aus 5.1 erfüllt sind, ist die Existenz von Tupeln $(d_i)_{i<\aleph_1}$ aus F und einer L-Formel $\varphi(x,y,z)$, so daß diese Bedingungen für $\varphi_i(x,y) = \varphi(x,y,d_i)$ erfüllt sind.

4) In 5.1.2 kann man anstelle der $n_i \in \mathbb{N}$ uniform für alle $i < \aleph_1$ die Existenz einer natürlichen Zahl n fordern, weil für überabzählbar viele $i < \aleph_1$ das gleiche n_i auftaucht.

Beweis: Wegen 5.1.1 existiert ein $a \in \mathbb{C}$ mit $\models \varphi_i(a, c_i)$ für $i < \aleph_1$. Ich zeige, daß $\mathrm{tp}(a/K)$ über jeder abzählbaren Menge teilt; wegen Theorem 2.10 ist $\mathrm{Th}(F)$ dann nicht einfach.

Sei $B \subset K$ abzählbar. Angenommen $\mathrm{tp}(a/K)$ teilt nicht über B; dann teilt $\mathrm{tp}(a/K)$ erst recht nicht über FB. Wegen 5.1.3 existiert ein $j < \aleph_1$ mit $c_j \notin \mathrm{acl}(FB)$, das heißt c_j hat unendlich viele Konjugierte $(c_j^l)_{l<\aleph_0}$ über FB.
Da $\mathrm{tp}(a/K)$ nicht-teilende Erweiterung von $\mathrm{tp}(a/FB)$ ist und $\varphi_j(x, c_j)$ in $\mathrm{tp}(a/K)$ liegt, ist für alle Folgen $(d_l)_{l<\aleph_1}$ in $\mathrm{tp}(c_j/FB)$ und für alle $k \in \mathbb{N}$ die Formelmenge $\{\varphi_j(x, d_l) \mid l < \aleph_0\}$ nicht k-inkonsistent.

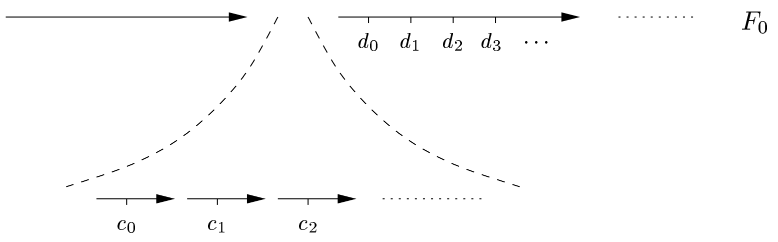
Für die Folge $(c_j^l)_{l<\aleph_0}$ ergibt sich daraus, daß für alle $k \in \mathbb{N}$ Indizes $l_0, \ldots, l_k$ existieren, so daß $\{\varphi(x, c_j^{l_0}), \ldots, \varphi(x, c_j^{l_k})\}$ konsistent ist; für $k = n_j$ ergibt sich damit ein Widerspruch zu 5.1.2. ■

Ein Beispiel für die Anwendung von 5.1 ist die Theorie der Arithmetik:

Beispiel: Es sei $T := \mathrm{Th}(\mathbb{N}, +, \cdot, 0, 1)$ und $F_0 \models T$ ein Modell mit paarweise verschiedenen Nichtstandartprimzahlen $(d_i)_{i<\aleph_1}$. Es sei $(F_i)_{i<\aleph_1}$ eine aufsteigende elementare Kette, so daß für $i < \aleph_1$ ein $c_i \in F_i$ existiert mit

$$c_i \models \{x < d_j \mid j < \aleph_1\} \cup \{x \neq f \mid f \in \bigcup_{j<i} F_j\}.$$

Zur Veranschaulichung:



Dann existiert für jede abzählbare Menge B ein $i < \aleph_1$ mit $c_i \notin \mathrm{acl}(FB)$; damit ist 5.1.3 erfüllt.
Es sei $K := \bigcup_{i<\aleph_1} F_i$. Wir betrachten nun die $\mathrm{L}(K)$-Formeln

$$\varphi_i(x, c_i) = \varphi(x, c_i, d_i) = \ (x \equiv c_i \bmod d_i) \wedge c_i < d_i.$$

Dann folgt aus dem chinesischen Restsatz, daß

$$\{\varphi_i(x, c_i) \mid i < \aleph_1\}$$

in K endlich erfüllbar, also erfüllbar in $\mathbb{C}$ ist. Außerdem folgt aus $\varphi_i(x, c) \wedge \varphi_i(x, c')$

$$c \equiv c' \bmod d_i,$$

was wegen $c < d_i$ und $c' < d_i$ schon $c = c'$ impliziert. Also gelten auch 5.1.1 und 5.1.2 , demnach ist T nicht einfach. ■Bsp.

Lemma 5.1 stellt ein hinreichendes Kriterium dafür dar, daß eine Theorie nicht einfach ist. Es handelt sich jedoch nicht um ein notwendiges Kriterium, wie das folgende Beispiel zeigt:

Beispiel 5.2. *Die Theorie T_{doO} dichter offener Ordnungen ist nicht einfach; dies läßt sich jedoch nicht mit dem Kriterium aus Lemma 5.1 zeigen.*

Beweis: Wie wir in Beispiel 2.11 gesehen haben, ist die Theorie dichter offener Ordnungen nicht einfach. Um zu zeigen, daß wir dies nicht mit dem Kriterium aus Lemma 5.1 beweisen können, benutzen wir das folgende Lemma:

Lemma 5.3. *Sei $L = \{<\}$, $Q \models T_{doO}$ und $\varphi(x, y_1, \ldots, y_n)$ eine L-Formel. Weiter sei*

$$\Phi(x, y_1, \ldots, y_n) := \{x < y_1, x \doteq y_1, y_1 < x < y_2, \ldots, y_{n-1} < x < y_n, x \doteq y_n, y_n < x\}.$$

Dann existiert ein $\Phi_0 \subseteq \Phi$ mit

$$Q \models \forall \bar{y}\Big(y_1 < \ldots < y_n \rightarrow \big(\varphi(x, \bar{y}) \leftrightarrow \bigvee \Phi_0(x, \bar{y})\big)\Big).$$

Beweisskizze: Da $\mathrm{T_{doO}}$ o-minimal ist, ist jede definierbare Menge $\varphi(x, \bar{a})^Q$ Vereinigung von Intervallen, deren Endpunkte, abgesehen von eventuell $\pm\infty$, in $\mathrm{dcl}(\bar{a}) = \bar{a}$ liegen. Daher existiert zu $a_1 < \ldots < a_n$ aus Q immer ein $\Phi_0 \subseteq \Phi$ mit

$$Q \models \varphi(x, \bar{a}) \leftrightarrow \bigvee \Phi_0(x, \bar{a}).$$

Ist nun $b_1 < \ldots < b_n$ ein weiteres geordnetes Tupel aus Q, so existiert ein $\alpha \in \mathrm{Aut}(\mathbb{C})$ mit $\alpha(\bar{a}) = \bar{b}$.

Also gilt

$$\varphi(x\bar{b})^Q = \alpha\big(\varphi(x, \bar{a})^Q\big) = \alpha\big(\Phi_0(x, \bar{a})^Q\big) = \Phi_0(x, \bar{b})^Q.$$

Dies zeigt, daß Φ_0 unabhängig vom geordneten Tupel $a_1 < \ldots < a_n$ ist. ■Lemma

Wir benutzen die in Teil 3) der Bemerkung hinter Theorem 5.1 angegebene Variante von Lemma 5.1.

Angenommen $\varphi(x, y, z)$ ist eine L-Formel,$(d_i)_{i<\aleph_1}$ sind Elemente aus F und $(c_i)_{i<\aleph_1}$ sind paarweise verschiedene Elemente aus einer elementaren Oberstruktur $K \succ F$, so daß 1) - 3) aus Lemma 5.1 gelten.

Die Bedingung 5.1.3 ist für paarweise verschiedene $(c_i)_{i<\aleph_1}$ stets erfüllt, da in dichten offenen Ordnungen der algebraische Abschluß trivial ist. Ist für ein $i < \aleph_1$ und ein $b \in \mathbb{C}$ die Erfüllungsmenge von $\varphi(x, b, d_i)$ unendlich, enthält also nach Lemma 5.3 ein ganzes Intervall, so bleibt die Formel auch nach „Rütteln" an einer Intervallgrenze noch konsistent, demnach ist 5.1.2 nicht erfüllt. Also ist die Erfüllungsmenge endlich.

Wieder wegen Lemma 5.3 existiert dann ein $I \subseteq \{1, \dots, r\}$ und ein $J \subseteq \{1, \dots, s\}$ mit

$$\varphi(x, c_i, d_i) \; = \; \bigvee_{k \in I} x \doteq c_i^k \vee \bigvee_{k \in J} x \doteq d_i^k.$$

Ist $J \neq \emptyset$, etwa $x \doteq d_i^1 \vdash \varphi(x, c_i, d_i)$, so gilt $\models \varphi(d_i^1, b, d_i)$ für beliebige b; also ist 2) aus 5.1 nicht erfüllt. Ist dagegen $|I| > 1$, etwa $x \doteq c_i^1 \vee x \doteq c_i^2 \vdash \varphi(x, c_i, d_i)$, so gilt $\models \varphi(c_i^1, b, d_i)$ für alle b mit $b^1 = c_i^1$, wieder ist 5.1.2 nicht erfüllt. Also ist ohne Einschränkung $\varphi(x, c_i, d_i) \; = \; x \doteq c_i^1$; dann ist aber

$$\{\varphi(x, c_i, d_i) \mid i < \aleph_1\}$$

inkonsistent und 5.1.1 ist nicht erfüllt. ■

Bemerkung: Da $\mathrm{T}_{\mathrm{doO}}$ Imaginärenelimination hat, läßt sich auch in $\mathrm{T}_{\mathrm{doO}}^{\mathrm{eq}}$ nicht mit Lemma 5.1 beweisen, daß dichte offene Ordnungen nicht einfach sind.

5.2 PAC-Körper mit unendlich vielen quadratischen Galoiserweiterungen

Bevor wir uns beliebigen unbeschränkten PAC-Körpern zuwenden, werden wir den beispielhaften Fall eines Körpers der Charakteristik ungleich 2 mit unendlich vielen quadratischen Erweiterungen betrachten. Dabei ist die Grundidee beim Beweis des allgemeinen Falls mit der des Beispiels identisch– nur die technische Durchführung wird komplizierter.

Beispiel 5.4. *Sei F ein PAC-Körper der Charakteristik $p \neq 2$ mit unendlich vielen Erweiterungen von Grad 2. Dann ist $\mathrm{Th}(F)$ nicht einfach.*

Beweis: Ohne Einschränkung hat F die Mächtigkeit $\aleph_1$, denn wegen Theorem 3.6 können wir zu einer elementaren Ober- oder Unterstruktur übergehen, die wieder PAC ist; wegen Korollar 2.5 und Lemma 2.6 hat diese wiederum unendlich viele quadratische Galoiserweiterungen. Es sei $(d_i)_{i<\aleph_1}$ eine Aufzählung von F. Die durch $\psi(u, v) \; = \; (\exists z \; u \doteq z^2 v)$ definierte Äquivalenzrelation auf $F^\times$ hat unendlich viele Äquivalenzklassen, da die Quadrate von zwei Elementen, die verschiedene quadratische Erweiterungen erzeugen, nicht äquivalent seien können. Wegen Theorem 2.13 können wir in T^{eq} arbeiten. Ich bezeichne die Variablen der Heimsorte mit $x, y, \dots$ und die Variablen in der zu ψ gehörigen Sorte mit $x^\psi, y^\psi, \dots$; für $a \in F$ sei a^ψ die Äquivalenzklasse von a, und es sei $F^\psi := \{a^\psi \mid a \in F\}$.

Schritt 1: Wir konstruieren eine Kette

$$F =: F_0 \prec F_1 \prec F_2 \prec \cdots \prec \bigcup_{i<\aleph_1} F_i =: K,$$

so daß für $i < \aleph_1$ ein $c_i^\psi \in F_i^\psi$ existiert, das eine in $\bigcup_{j<i} F_j^\psi$ noch nicht repräsentierte Äquivalenzklasse vertritt. Die Elemente c_i^ψ, die wir in diesem Schritt finden, werden später genau die Elemente c_i aus Lemma 5.1 sein.

Für c_0^ψ können wir die Äquivalenzklasse eines beliebigen Elementes aus F wählen. Für $j < i$ seien F_j und c_j^ψ bereits konstruiert. Zur Konstruktion von F_i:

Es sei $M := \bigcup_{j<i} F_j$; dann ist $M \succ F_j$ für alle $j < i$. Es sei weiter

$$\Phi_i := \{\neg x^\psi = m^\psi \mid m \in M\}.$$

Da in M unendlich viele verschiedene Äquivalenzklassen repräsentiert sind, ist Φ_i in M^{eq} endlich erfüllbar, also erfüllbar durch $c_i^\psi \in F_i^{\mathrm{eq}}$ für ein $F_i \succ M$. ■Schritt 1

Schritt 2: Wir wählen Formeln $\varphi_i(x, y)$, so daß für die Elemente $c_i \in K$ die Punkte 5.1.2 und 5.1.3 erfüllt sind.

Für die L(F)-Formel $\varphi_i(x, c_i)$ in Lemma 5.1 wählen wir die Formel

$$\varphi_i(x, c_i^\psi) \;=\; \varphi(x, c_i^\psi, d_i) \;=\; (x + d_i)^\psi \doteq c_i^\psi.$$

Dann ist für alle $i < \aleph_1$ die Formel

$$\varphi(x, y_1^\psi, d_i) \wedge \varphi(x, y_2^\psi, d_i) \wedge y_1^\psi \neq y_2^\psi$$

inkonsistent, denn aus $\models \varphi(a, b_1^\psi, d_i) \wedge \varphi(a, b_2^\psi, d_i)$ folgt $(a + d_i)^\psi = b_1^\psi$ und $(a + d_i)^\psi = b_2^\psi$, also $b_1^\psi = b_2^\psi$. Außerdem existiert für jedes abzählbare B in K ein $i < \aleph_1$ mit $B \subset F_i$ (denn $\aleph_1$ ist regulär), also ist $\mathrm{acl}(FB) \subseteq \mathrm{acl}(F_i) = F_i$; demnach ist $c_{i+1} \notin \mathrm{acl}(FB)$. ■Schritt 2

Schritt 3: Wir zeigen die Gültigkeit von 5.1.1.

Gesucht ist jetzt also ein Element $a \in \mathbb{C}$ mit $\models \varphi(a, c_i^\psi, d_i)$ für $i < \aleph_1$; ist das geschafft, so folgt mit Lemma 5.1, daß $\mathrm{Th}(F)$ nicht einfach ist.
Wegen der Äquivalenz

es ex. $a \in \mathbb{C}$ mit $\models \varphi(a, c_i^\psi, d_i)$	$\iff$	es ex. $a \in \mathbb{C}$, so daß für jedes $c_i \in c_i^\psi$ ein $b \in \mathbb{C}$ existiert mit $b^2(a + d_i) = c_i$
	$\iff$	es ex. $a \in \mathbb{C}$, so daß für ein $c_i \in c_i^\psi$ ein $b \in \mathbb{C}$ existiert mit $b^2(a + d_i) = c_i$

und aus Kompaktheitsgründen reicht es, zu jeder endlichen Teilmenge $I_0 \subset \aleph_1$, ohne Einschränkung $I_0 = \{1, \ldots, n\}$, eine Nullstelle des Ideals

$$I := \left(Z_i^2 \frac{X + d_i}{c_i} = 1 \,\middle|\, 1 \leq i \leq n \right)_{K[X, Z_1, \ldots, Z_n]}$$

in einer elementaren Oberstruktur von K zu finden; dabei sei $\{c_i \mid i < \aleph_1\}$ ein Repräsentantensystem von $\{c_i^\psi \mid i < \aleph_1\}$.

Nach Theorem 3.7 existiert für jede reguläre Erweiterung eines PAC-Körpers K eine elementare Oberstruktur von K, die die Erweiterung enthält. Es reicht also der Nachweis, daß ein rationaler Punkt von I existiert, dessen Adjunktion zu einer regulären Erweiterung von K führt.

Wir betrachten einen rationalen Punkt der Form $(a, b_1, \ldots, b_n)$, wobei a transzendent über K ist und b_i eine Quadratwurzel von $\frac{c_i}{a+d_i}$.
Zu zeigen ist die lineare Disjunktheit von K^{a} und $K(a, \overline{b})$ über K. Da $K^{\mathrm{a}} \supseteq K$ algebraisch ist und $K(a) \supseteq K$ rein transzendent, muß wegen der Turmeigenschaft nur $K(a, \overline{b}) \underset{K(a)}{\overset{l}{\perp}} K^{\mathrm{a}}(a)$ gezeigt werden. Wegen $\mathrm{char}(F) \neq 2$ ist $K(a, \bar{b}) \supseteq K(a)$ galoisch; also ist $K(a, \overline{b}) \underset{K(a)}{\overset{l}{\perp}} K^{\mathrm{a}}(a)$ äquivalent zu $[K(a, \overline{b}) : K(a)] = [K^{\mathrm{a}}(a, \overline{b}) : K^{\mathrm{a}}(a)]$. Es genügt also zu zeigen, daß der Grad $[K^{\mathrm{a}}(a, \overline{b}) : K^{\mathrm{a}}(a)]$ der maximal mögliche, das heißt 2^n, ist. Wir benutzen dazu das folgende

Theorem 5.5 (Kummer-Theorie). *Es sei M ein Körper, $m \in \mathbb{N}$ sei teilerfremd zu $\mathrm{char}(M)$, und es liege eine primitive m-te Einheitswurzel in M. Weiter sei B eine Untergruppe der multiplikativen Gruppe $M^{\times}$ von M, die $M^{\times m}$ enthält, es sei $B^{1/m} := \{b^{1/m} \mid b \in B\}$ und $M_B := M(B^{1/m})$.*
Dann ist $M_B \supseteq M$ galoissch; die Erweiterung $M_B \supseteq M$ ist genau dann endlich, wenn der Index $(B : M^{\times m})$ endlich ist. In diesem Fall gilt

$$[M_B : M] = (B : M^{\times m}).$$

Beweis: siehe [La1, Kapitel 6, Theorem 8.1]

Setze nun $m := 2$ und $M := K^{\mathrm{a}}(a)$; dann ist $M^{\times 2} = (K^{\mathrm{a}}(a)^{\times})^2$. Für

$$B = \left\langle (K^{\mathrm{a}}(a)^{\times})^2, b_i^2 \mid 1 \leq i \leq n \right\rangle_{K^{\mathrm{a}}(a)}$$

folgt dann $M_B = K^{\mathrm{a}}(a, \overline{b})$. Mit -1 enthält $K^{\mathrm{a}}(a)$ eine primitive Quadratwurzel der 1, außerdem ist $[K^{\mathrm{a}}(a, \overline{b}) : K^{\mathrm{a}}(a)]$ endlich. Wir zeigen also

$$(B : M^{\times m}) = \left(\left\langle (K^{\mathrm{a}}(a)^{\times})^2, b_i^2 \mid 1 \leq i \leq n \right\rangle_{K^{\mathrm{a}}(a)} : (K^{\mathrm{a}}(a)^{\times})^2 \right) \overset{!}{=} 2^n.$$

Behauptung: Die Elemente

$$\Big\{ \prod_{j \in J_0} b_j^2 \mid J_0 \subseteq \{1, \ldots, n\} \Big\},$$

das heißt die Elemente

$$\Big\{ \prod_{j \in J_0} \frac{c_j}{a + d_j} \mid J_0 \subseteq \{1, \ldots, n\} \Big\},$$

sind multiplikativ unabhängig über $(K^{\mathrm{a}}(a)^{\times})^2$.

Ist das gezeigt, so sind wir fertig!
BEWEIS: Angenommen nicht. Dann existieren $J_0, J_1 \subseteq \{1, \dots, n\}$, ohne Einschränkung $J_0 \cap J_1 = \emptyset$, und teilerfremde $p, q \in K^{\mathrm{a}}[X]$, $p, q \neq 0$ mit

$$\prod_{i \in J_0} \frac{c_i}{a + d_i} = \left(\frac{p(a)}{q(a)}\right)^2 \prod_{i \in J_1} \frac{c_i}{a + d_i}, \text{ also}$$

$$q(a)^2 \prod_{i \in J_1} (a + d_i) = rp(a)^2 \prod_{i \in J_0} (a + d_i) \text{ für } r := \frac{\prod_{i \in J_1} c_i}{\prod_{i \in J_0} c_i} \in K.$$

Vergleich der Koeffizienten vor den höchsten Potenzen von a auf der rechten und der linken Seite ergibt $r \in K^2$, also ohne Einschränkung $r = 1$. Also gilt:

$$\begin{aligned} q(a)^2 \cdot \prod_{i \in J_1} (a + d_i) = p(a)^2 \cdot \prod_{i \in J_0} (a + d_i) &\Longrightarrow \prod_{i \in J_1} (a + d_i) \text{ teilt } p^2 \\ &\Longrightarrow \Big(\prod_{i \in J_1} (a + d_i)\Big)^2 \text{ teilt } p^2 \\ &\Longrightarrow \prod_{i \in J_1} (a + d_i) \text{ teilt } q \\ &\Longrightarrow p, q \text{ sind nicht teilerfremd.} \end{aligned}$$

Widerspruch! Also gilt $\Big(\big\langle (K^{\mathrm{a}}(a)^{\times})^2, b_i^2 \mid 1 \leq i \leq n \big\rangle_{K^{\mathrm{a}}(a)} : (K^{\mathrm{a}}(a)^{\times})^2\Big) = 2^n$ und $K(a, \overline{b})$ ist eine reguläre Erweiterung von K; es gibt also ein $a \in \mathbb{C}$ mit $\varphi(a, c_i^{\psi}, d_i)$ für $i < \aleph_1$. ■Schritt 3

■

5.3 Der Satz

Wir beginnen jetzt mit den Vorbereitungen für den Beweis des allgemeinen Falls:

Lemma 5.6. *Es sei G eine Gruppe der Ordnung n und $m \geq 2n$. Dann existiert eine Einbettung von G in die alternierende Gruppe A_m.*

BEWEIS: G operiert durch Rechtsmultiplikation auf sich selbst; dies liefert eine Einbettung von G in die S_n. Durch Verknüpfung mit der Abbildung $S_n \to A_{2n}$, $(i, i+1) \mapsto (i, i+1)(i+n, i+n+1)$ erhält man eine Einbettung in die A_{2n}. Schließlich kann man die A_{2n} für jedes $m \geq 2n$ in die A_m einbetten: Operiert die A_m etwa auf $\Omega = \{\omega_1, \dots, \omega_m\}$, so ist die A_{2n} isomorph zu $\mathrm{Stab}(\{\omega_{2n+1}, \dots, \omega_m\}) \subseteq A_m$. Insgesamt erhält man für $m \geq 2n$ eine Einbettung von G nach A_m. ■

Lemma 5.7. *Sei F ein unbeschränkter Körper. Dann existiert eine endliche separable Erweiterung F_* von F, die für ein $n > 1$ und eine einfache Gruppe G der Ordnung n paarweise linear disjunkte Galoiserweiterungen $(M_i)_{i \in \aleph_0}$ mit $\mathrm{Gal}(M_i/F_*) \cong G$ besitzt.*

Beweis: Es sei $m > 1$ so, daß F paarweise verschiedene Galoiserweiterungen $(B_i)_{i<\aleph_0}$ von Grad m besitzt. Ohne Einschränkung sei m minimal gewählt.
Aus der Minimalitätsannahme für m folgt, daß die Menge $\{B_i \cap B_j \mid i, j \in \aleph_0\}$ endlich ist. Mit dem Satz von Ramsey erhält man nun, daß unendlich viele der B_i den gemeinsamen Schnitt F_* haben. Dabei ist F_* eine endliche separable Erweiterung von F. Wir können also ohne Einschränkung annehmen, daß alle B_i über F_* paarweise linear disjunkt sind. Der Grad der B_i über F_* sei r.
Da es nur endlich viele Gruppen der Ordnung r gibt, haben unendlich viele der B_i über F_* isomorphe Galoisgruppe G'. Existiert nun noch ein Normalteiler $N \trianglelefteq G'$, so geht man von B_i über zum Fixkörper B_i' des entsprechenden Normalteilers N_i in $\mathrm{Gal}(B_i/F_*)$; nach endlich vielen Schritten erhält man Erweiterungen $M_i \supset F_*$ mit einfacher Galoisgruppe. ■

Im folgenden sei $\aleph_1^* := \{*\} \cup \aleph_1$ und für $i \in \aleph_1$ sei $i^* := \{*\} \cup i$.

Lemma 5.8. *Es sei F ein unbeschränkter Körper. Dann existiert eine endliche separable Erweiterung F_* von F, ein $n > 1$, eine (einfache) Gruppe G der Ordnung n und eine elementare Kette $F_* \prec F_0 \prec F_1 \prec \cdots \prec \bigcup_{i\in\aleph_1} F_i =: K$, so daß für $i \in \aleph_1$ Galoiserweiterungen $E_i \supset F_i$ existieren mit $\mathrm{Gal}(E_i/F_i) \cong G$ und $E_i \underset{F_j}{\overset{l}{\perp}} F_j^s$ für alle $j \in i^*$.*
Die Erweiterungen $L_i := KE_i$ sind dann linear disjunkt über K, und für $L := \prod_{i\in\aleph_1} L_i = \prod_{i\in\aleph_1} E_i$ ist $\mathrm{Gal}(L/K) \cong \prod_{i\in\aleph_1} G$ und die Erweiterung $L \supseteq F_*$ ist regulär.

Beweis: Nach Lemma 5.7 existiert eine endliche separable Erweiterung F_* von F, ein $n \in \mathbb{N}$ und eine einfache Gruppe G der Ordnung n, so daß F_* paarweise linear disjunkte Galoiserweiterungen $(B_k)_{k\in\aleph_0}$ mit $\mathrm{Gal}(B_k/F_*) \cong G$ besitzt.

Zur Konstruktion der Kette $F_* \prec F_0 \prec F_1 \prec \cdots \prec \bigcup_{i\in\aleph_1} F_i$:

Die Kette sei für $j \in i^*$ bereits konstruiert. Zur Konstruktion von F_i:
Es sei $M := \bigcup_{j\in i^*} F_j$; dann ist M elementare Oberstruktur von F_j für $j \in i^*$. Es sei

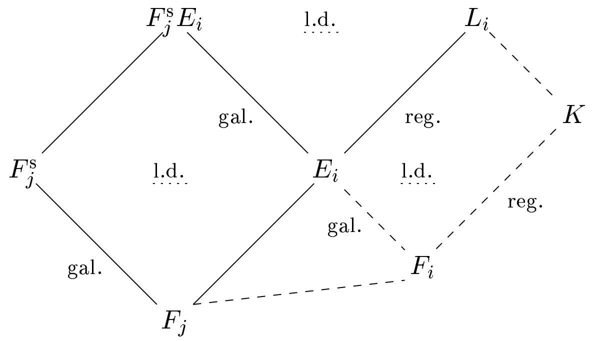
$$\Phi := \{\psi_{\mathrm{G}}(\bar{x_k}) \mid j < |M|^+\} \cup \{\neg\psi_{\mathrm{glErw}}(\bar{x_k}, \bar{x_l}) \mid k, l < |M|^+,\ k \neq l\};$$

dabei seien ψ_{G} und ψ_{glErw} die in Korollar 2.5 bzw. Lemma 2.6 definierten Formeln. Φ ist in M endlich erfüllbar, denn sonst hätte mit M auch F_* nur endlich viele Galoiserweiterungen mit Galoisgruppe G. Es sei also $F_i \succ M$ eine elementare Oberstruktur von M, und es seien $(R_j \supseteq F_i)_{j<|M|^+}$ Galoiserweiterungen mit Galoisgruppe G. Da G einfach ist, gilt für jedes $j < |M|^+$ entweder $R_j \subseteq M^{\mathrm{s}}F_i$ oder $R_j \cap M^{\mathrm{s}}F_i = F_i$.
Nun hat $M^{\mathrm{s}} \supseteq M$ und damit auch $M^{\mathrm{s}}F_i \supseteq F_i$ jedoch höchstens $|M|$-viele Teilerweiterungen von Grad n; es können also nicht alle R_j in $M^{\mathrm{s}}F_i$ enthalten sein. Also existiert ein $R_{j_0} =: E_i$ mit $E_i \cap M^{\mathrm{s}}F_i = F_i$, also $E_i \underset{F_i}{\overset{l}{\perp}} M^{\mathrm{s}}F_i$. Mit der Turmeigenschaft folgt dann $E_i \underset{F_j}{\overset{l}{\perp}} F_j^{\mathrm{s}}$ für alle $j \in i^*$.

Sei $K := \bigcup_{i\in\aleph_1} F_i$. Für alle $i \in \aleph_1$ gilt $K \succ F_i$, also ist $K \supset F_i$ regulär und daher gilt $\mathrm{Gal}(L_i/K) \cong G$. Weiter ist $\prod_{i\in\aleph_1} E_i = L$, denn es gilt $K = \prod_{i\in\aleph_1^*} F_i \subset \prod_{i\in\aleph_1} E_i$.

<u>Behauptung 1):</u> Die Körper $(L_i)_{i\in\aleph_1}$ sind linear disjunkt über K.

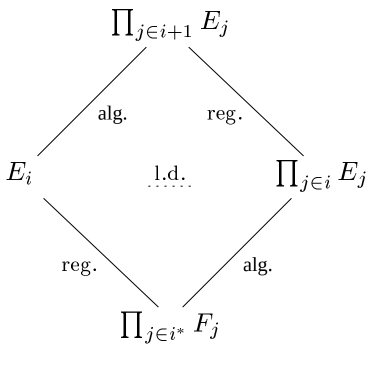
Es reicht für alle $i \in \aleph_1$ zu zeigen, daß $L_i \underset{K}{\overset{l}{\downarrow}} \prod_{j\in i} L_j$ ist. Das folgende Bild dient der Veranschaulichung:



Da E_i und K linear disjunkt über F_i sind, folgt aus der Regularität von $K \supset F_i$ auch die Regularität von $L_i \supset E_i$. Für $j \in i^*$ ist also L_i linear disjunkt von $F_j^{\mathrm{s}} E_i$ über E_i. Zusammen mit $E_i \underset{F_j}{\overset{l}{\downarrow}} F_j^{\mathrm{s}}$ folgt mit der Turmeigenschaft $F_j^{\mathrm{s}} \underset{F_j}{\overset{l}{\downarrow}} L_i$, und wiederum wegen der Turmeigenschaft auch $F_j^{\mathrm{s}} K \underset{K}{\overset{l}{\downarrow}} L_i$. Aus dem endlichen Charakter linearer Disjunktheit folgt dann auch $\prod_{j\in i^*} F_j^{\mathrm{s}} K \underset{K}{\overset{l}{\downarrow}} L_i$. Wegen $\prod_{j\in i} L_j \subseteq \prod_{j\in i^*} F_j^{\mathrm{s}} K$ folgt die Behauptung. ■Beh.1)

<u>Behauptung 2):</u> L ist eine reguläre Erweiterung von F.

Das folgende Bild illustriert den Beweis:



Die Erweiterungen $E_i \supset F_j$ sind für $j \in i^*$ separabel und wegen $E_i \underset{F_j}{\overset{l}{\downarrow}} F_j^{\mathrm{s}}$ primär, also regulär. Wegen des endlichen Charakters der linearen Disjunktheit folgt hieraus auch die Regularität von $E_i \supset \prod_{j\in i^*} F_j$. Andererseits ist $\prod_{j\in i} E_j \supseteq \prod_{j\in i^*} F_j$ algebraisch, demnach ist $E_i \underset{\prod_{j\in i^*} F_j}{\overset{l}{\downarrow}} \prod_{j\in i} E_j$. Also ist auch $\prod_{j\in i\cup\{i\}} E_j \supset \prod_{j\in i} E_j$ regulär.

Ist $(M_i)_{i<\kappa}$ eine aufsteigende Kette, so daß die Erweiterungen $M_i \supseteq \prod_{j<i} M_j$ regulär sind, so zeigt man leicht durch Induktion über κ, daß die Vereinigung $\prod_{i<\kappa} M_i$ eine reguläre Erweiterung von M_0 ist.

Für $\kappa = \aleph_1$, $M_0 := F_*$ und $M_i := \prod_{j<i} E_j$ für $i > 1$, also für die Kette

$$\begin{array}{ccccccccccccc} F_* & \overset{\text{reg.}}{\subset} & E_1 & \overset{\text{reg.}}{\subset} & E_1E_2 & \overset{\text{reg.}}{\subset} \cdots \overset{\text{reg.}}{\subset} & \prod_{i<\aleph_0} E_i & \overset{\text{reg.}}{\subset} \cdots \overset{\text{reg.}}{\subset} & \prod_{i<\aleph_1} E_i & = L \\ \| & & \| & & \| & & \| & & \| & \\ M_0 & & M_1 & & M_2 & & M_{\aleph_0} & & M_{\aleph_1} & \end{array}$$

heißt dies gerade, daß $L \supset F$ regulär ist. ■Beh.2)

■

Bemerkung: Wir werden später an keiner Stelle benutzen, daß es sich bei G um eine einfache Gruppe handelt. In Lemma 5.8 muß man dann aber bei der Konstruktion der Kette fordern, daß die $(R^j_{i+1})_{j\in|F_i|^+}$ paarweise disjunkt sind. Dies ist möglich (denn es läßt sich ausdrücken, daß zwei Erweiterungen keinen gemeinsamen Schnitt haben), erfordert aber einige Überlegungen zur Formulierbarkeit; mir erscheint es daher eleganter, stattdessen mit einer einfacher Gruppe zu arbeiten.

Nun also zum zentralen Satz dieser Arbeit:

Theorem 5.9.
Es sei F ein unbeschränkter PAC-Körper. Dann ist die Theorie von F nicht einfach.

Beweis: Wieder hat F ohne Einschränkung die Mächtigkeit $\aleph_1$. Wir finden mit Lemma 5.8 ein $n > 1$, eine endliche Gruppe G der Ordnung n, eine endliche Erweiterung F_* von F, eine elementare Kette $F_* \prec F_0 \prec F_1 \prec \cdots \prec \prod_{i<\aleph_1} F_i =: K$ und Galoiserweiterungen $E_i \supset F_i$ mit $\mathrm{Gal}(E_i/F_i) \cong G$ und $E_i \underset{F_j}{\overset{l}{\downarrow}} F_j^{\mathrm{s}}$ für alle $j < i^*$. Da F_* als endliche algebraische Erweiterung von F wieder ein einfacher PAC-Körper ist, können wir ohne Einschränkung $F_* = F$ annehmen.

Wie in Lemma 5.8 sei $L_i := KE_i$ und $L := \prod_{i<\aleph_1} L_i = \prod_{i<\aleph_1} E_i$; die Erweiterungen L_i sind dann linear disjunkt über K, es ist $\mathrm{Gal}(L/K) \cong \prod_{i<\aleph_1} G$ und die Erweiterung $L \supseteq F$ ist regulär.

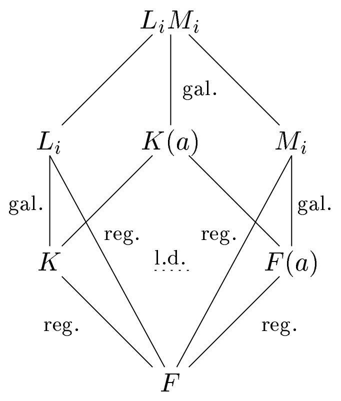
Ist $\mathrm{char}(F) =: p \neq 2$, so wählen wir ein $m \in \mathbb{N}, m > 4$ so, daß $p \nmid m(m-1)$ gilt; andernfalls sei $m := 2n$.
Sei nun a transzendent über K. Nach Theorem 4.1 existieren für $i < \aleph_1$ über $F(a)$ linear disjunkte Galoiserweiterungen $M_i \supset F(a)$, so daß $\mathrm{Gal}(M_i/F(a)) \cong A_m$ und $M := \prod_{i<\aleph_1} M_i \supset F$ regulär ist. Zur Erinnerung: Nur falls $p = 2$ ist, benötigen wir an dieser Stelle, daß F ein PAC-Körper ist!

Zur Beweisidee: Wir wollen Lemma 5.1 anwenden. Dabei ist K die in 5.1 auftauchende elementare Oberstruktur $K \succ F$.

- In Teil 1 des Beweises konstruieren wir eine elementare Oberstruktur $K^* \succ K$, für die $K^*L_i = K^*M_i$ gilt.
- In Teil 2 des Beweises zeigen wir, daß die Erweiterung $K^*M_i \supseteq K^*$ mit Parametern $d_i \in F$ und a interpretierbar ist. Ist nun $c_i \in K$ so, daß $K^*L_i = K^*_{c_i}$ gilt, so gibt es eine Formel $\varphi_i(x, c_i^X) = \varphi_i(x, c_i^X, d_i)$, welche die Gleichheit von $K^*_{c_i}$ und K^*M_i beschreibt und die alle Bedingungen aus 5.1 erfüllt.

Teil 1:

Wir betrachten das folgende Diagramm:



Mit Lemma 1.16 erhalten wir für alle $i < \aleph_1$ zum einen $L_i \underset{F}{\overset{l}{\downarrow}} M_i$ und weiter

$$\mathrm{Gal}(L_iM_i/K(a)) \overset{f_i}{\cong} \mathrm{Gal}(L_i/K) \times \mathrm{Gal}(M_i/F(a)).$$

Dabei sind die f_i jeweils die Produkte der Restriktionsabbildungen.

Sei $\varphi_i : \mathrm{Gal}(L_i/K) \hookrightarrow \mathrm{Gal}(M_i/F(a))$ eine Einbettung von $\mathrm{Gal}(L_i/K) \cong G$ in $\mathrm{Gal}(M_i/F(a)) \cong A_m$ wie in Lemma 5.6 beschrieben. Weiter sei

$$H_i := f_i^{-1}(\underbrace{\{(g, \varphi_i(g)) \mid g \in \mathrm{Gal}(L_i/K)\}}_{\subseteq \mathrm{Gal}(L_i/K) \times \mathrm{Gal}(M_i/F(a))}) \subseteq \mathrm{Gal}(L_iM_i/K(a))$$

die „Diagonale“ in $\mathrm{Gal}(L_iM_i/K(a))$ und

$$N_i := \mathrm{Fix}(H_i).$$

Dann ist $H_i = \mathrm{Gal}(L_iM_i/N_i)$. Es gilt $L_iM_i = L_iN_i = M_iN_i$, denn es ist

$$\begin{aligned} L_iN_i &= \mathrm{Fix}\Big(f_i^{-1}\big(\{e\} \times \mathrm{Gal}\big(M_i/F(a)\big)\big)\Big)\mathrm{Fix}(H_i) \\ &= \mathrm{Fix}\Big(f_i^{-1}\big(\{e\} \times \mathrm{Gal}\big(M_i/F(a)\big)\big) \cap H_i\Big) \end{aligned}$$

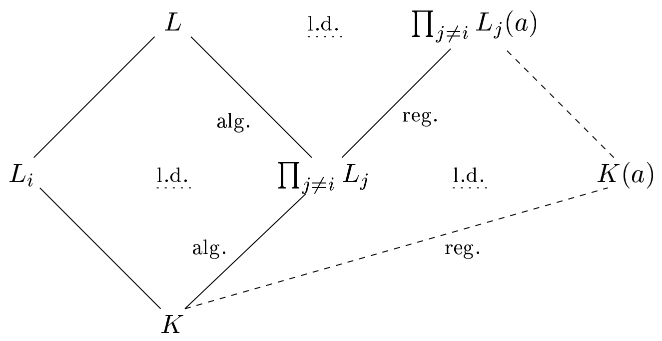
$$
\begin{aligned}
&= \mathrm{Fix}\Big(f_i^{-1}\Big(\big(\{e\} \times \mathrm{Gal}\big(M_i/F(a)\big)\big) \cap \Big\{(g, \varphi_i(g)) \mid g \in \mathrm{Gal}(L_i/K)\Big\}\Big)\Big) \\
&= \mathrm{Fix}\big(\{\mathrm{id}\}\big) \\
&= L_i M_i \\
&= \mathrm{Fix}\Big(f_i^{-1}\Big(\mathrm{Gal}\big(L_i/K\big) \times \{e\}\Big) \cap H_i\Big) \\
&= M_i N_i
\end{aligned}
$$

Also gilt mit $N := \prod_{i<\aleph_1} N_i$ auch $LM = LN = MN$.

Behauptung: $N \supset K$ ist regulär.

Schritt 1: Ich zeige für alle $i < \aleph_1$, daß $L_i M_i \underset{K(a)}{\overset{l}{\smile}} \prod\limits_{i \neq j} L_j M_j$ gilt.

Da die L_i linear disjunkt über K sind und die Erweiterung $\prod\limits_{j\neq i} L_j(a) \supset \prod\limits_{j\neq i} L_j$ regulär ist, die Erweiterung $L \supset \prod\limits_{j\neq i} L_j$ dagegen algebraisch, folgt mit der Turmeigenschaft $\prod\limits_{j\neq i} L_j(a) \underset{K}{\overset{l}{\smile}} L_i$. Dies wird durch das folgende Bild illustriert:



Wiederum mit der Turmeigenschaft folgt dann

$$\prod_{j\neq i} L_j(a) \underset{K(a)}{\overset{l}{\smile}} L_i(a).$$

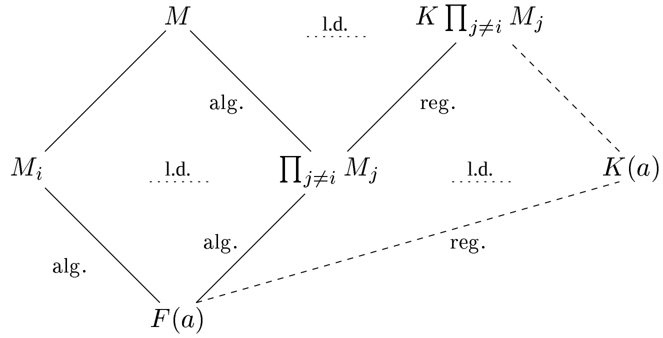
Außerdem folgt mit der Turmeigenschaft aus $M \underset{F}{\overset{l}{\smile}} L$ auch $MK \underset{K}{\overset{l}{\smile}} L$, hieraus dann $MK \underset{K(a)}{\overset{l}{\smile}} L(a)$ und schließlich

$$M \prod_{j\neq i} L_j \underset{\prod_{j\neq i} L_j(a)}{\overset{l}{\smile}} L(a).$$

Aus $\prod\limits_{j\neq i} L_j(a) \underset{K(a)}{\overset{l}{\smile}} L_i(a)$ und $M \prod\limits_{j\neq i} L_j \underset{\prod_{j\neq i} L_j(a)}{\overset{l}{\smile}} L(a)$ folgt dann mit der Turmeigenschaft auch $M \prod\limits_{j\neq i} L_j \underset{K(a)}{\overset{l}{\smile}} L_i(a)$ und dann natürlich erst recht

$$\boxed{\prod_{j \neq i} L_j M_j \overset{l}{\underset{K(a)}{\smile\!\!\!\!\!\!\vert\;}} L_i(a).} \qquad (*)$$

Ähnlich wie zuvor $\prod\limits_{j \neq i} L_j(a) \overset{l}{\underset{K(a)}{\smile\!\!\!\!\!\!\vert\;}} L_i(a)$ erhält man auch $K \prod\limits_{j \neq i} M_j \overset{l}{\underset{K(a)}{\smile\!\!\!\!\!\!\vert\;}} M_i K$; das folgende Bild veranschaulicht dies:



Weiter folgt aus $M \overset{l}{\underset{F}{\smile\!\!\!\!\!\!\vert\;}} L$ wieder mit der Turmeigenschaft $MK \overset{l}{\underset{K \prod\limits_{j \neq i} M_j}{\smile\!\!\!\!\!\!\vert\;}} L \prod\limits_{j \neq i} M_j$. Zusammen mit $K \prod\limits_{j \neq i} M_j \overset{l}{\underset{K(a)}{\smile\!\!\!\!\!\!\vert\;}} M_i K$ erhält man mit der Turmeigenschaft

$$L \prod_{j \neq i} M_j \overset{l}{\underset{K(a)}{\smile\!\!\!\!\!\!\vert\;}} M_i K$$

und dann auch

$$\boxed{L \prod_{j \neq i} M_j \overset{l}{\underset{L_i(a)}{\smile\!\!\!\!\!\!\vert\;}} L_i M_i.} \qquad (**)$$

Aus $(*)$ und $(**)$ folgt dann mit der Turmeigenschaft insgesamt $L_i M_i \overset{l}{\underset{K(a)}{\smile\!\!\!\!\!\!\vert\;}} \prod\limits_{j \neq i} L_j M_j$.

■Schritt 1

<u>Schritt 2:</u> Es ist $\mathrm{Gal}(LM/N) \cong \mathrm{Gal}(L/K)$ via Restriktion.

Das folgende Diagramm dient der Erläuterung. Da nach Schritt 1 die Erweiterungen $L_i M_i$ linear disjunkt über $K(a)$ sind, folgt mit der Turmeigenschaft auch die lineare Disjunktheit der $L_i M_i N$ über N. Also gilt

$$\mathrm{Gal}(LM/N) \cong \prod_{i < \aleph_1} \mathrm{Gal}(L_i M_i N/N)$$

via Restriktion. Wegen $L_i M_i \overset{l}{\underset{N_i}{\smile\!\!\!\!\!\!\vert\;}} N$ gilt ebenfalls via Restriktion

$$\prod_{i < \aleph_1} \mathrm{Gal}(L_i M_i N/N) \cong \prod_{i < \aleph_1} \mathrm{Gal}(L_i M_i/N_i) = \prod_{i < \aleph_1} H_i.$$

$$
\begin{tikzcd}[column sep=small]
 & & LM \arrow[dl, dash] \arrow[dr, dash] & & \\
 & L_iM_iN \arrow[dl, dash] \arrow[dr, dash] \arrow[rr, phantom, "\text{l.d.}"] & & N\prod_{j\neq i} L_jM_j \arrow[dl, dash] \arrow[dr, dash] & \\
L_iM_i \arrow[dr, dash] \arrow[rr, phantom, "\text{l.d.}"] & & N \arrow[dl, dash] \arrow[dr, dash] \arrow[rr, phantom, "\text{l.d.}"] & & \prod_{j\neq i} L_jM_j \arrow[dl, dash] \\
 & N_i \arrow[dr, dash] \arrow[rr, phantom, "\text{l.d.}"] & & \prod_{j\neq i} N_j \arrow[dl, dash] & \\
 & & K(a) & &
\end{tikzcd}
$$

Mit der weiter oben definierten Abbildung $\varphi_i : \mathrm{Gal}(L_i/K) \to \mathrm{Gal}(M_i/F(a))$ und der Restriktion $f_i : \mathrm{Gal}(L_iM_i/K(a)) \cong \mathrm{Gal}(L_i/K) \times \mathrm{Gal}(M_i/F(a))$ gilt

$$\prod_{i<\aleph_0} H_i \overset{\Pi\left(f_i|_{H_i}\right)}{\cong} \prod_{i<\aleph_1} \{(g, \varphi_i(g) \mid g \in \mathrm{Gal}(L_i/K)\} \subseteq \mathrm{Gal}(L_i/K) \times \mathrm{Gal}(M_i/F(a)).$$

Weiter gilt via Restriktion

$$\prod_{i<\aleph_1} \{(g, \varphi_i(g) \mid g \in \mathrm{Gal}(L_i/K)\} \cong \prod_{i<\aleph_1} \mathrm{Gal}(L_i/K).$$

Insgesamt ist also die Restriktionsabbildung $res : \mathrm{Gal}(LM/N) \cong \prod_{i<\aleph_1}(L_i/K)$ ein Isomorphismus.

Des weiteren ist ebenfalls via Restriktion

$$\mathrm{Gal}(L/K) \cong \prod_{i<\aleph_1} \mathrm{Gal}(L_i/K).$$

Dies zeigt, daß mittels der Restriktionsabbildung $\mathrm{Gal}(LM/N) \cong \mathrm{Gal}(L/K)$ gilt.

■Schritt2

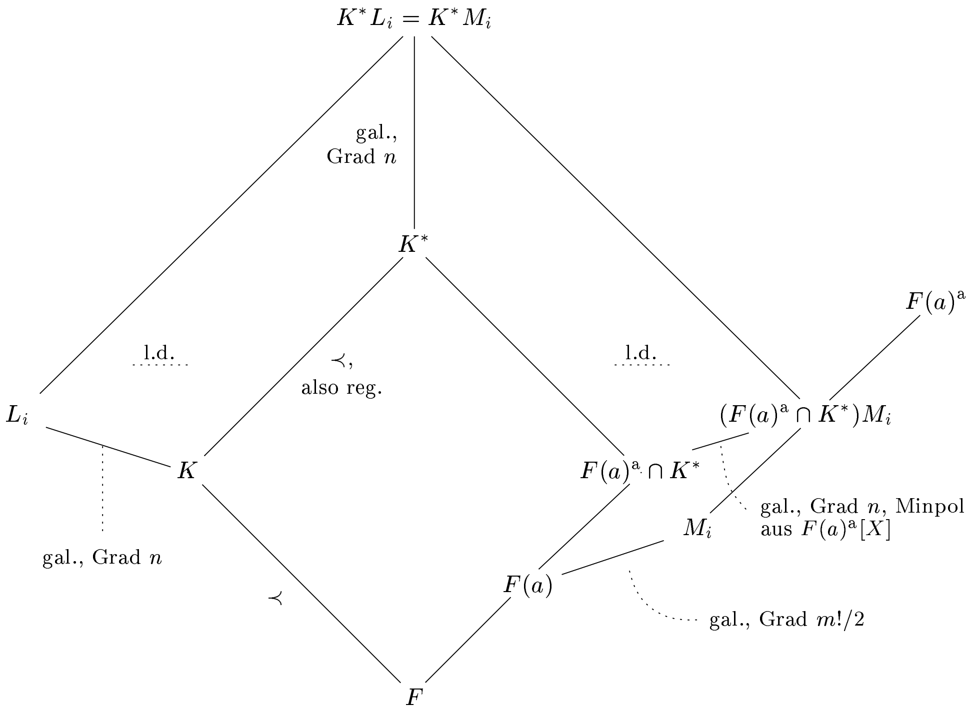
Wegen Bemerkung 1.5.5 ist dies äquivalent dazu, daß L und N linear disjunkt über K sind. Da L und M linear disjunkt über F sind, ist mit $M \supset F$ auch $LM \supset L$ regulär, das heißt es ist $L^{\mathrm{a}} \underset{L}{\overset{l}{\downarrow}} LM$. Wegen $LM = LN$ folgt aus $L^{\mathrm{a}} \underset{L}{\overset{l}{\downarrow}} LM$ und $L \underset{K}{\overset{l}{\downarrow}} N$ mit der Turmeigenschaft $L^{\mathrm{a}} \underset{K}{\overset{l}{\downarrow}} N$ und dann $K^{\mathrm{a}} \underset{K}{\overset{l}{\downarrow}} N$. Also ist $N \supset K$ regulär. ■Beh.

Da die Erweiterung $N \supset K$ regulär und K pseudo-algebraisch abgeschlossen ist, existiert nach 3.7 eine elementare Oberstruktur K^* von K, die N enthält. Ist $p \neq 2$, so ist dies die einzige Stelle im Beweis, an der die pseudo-algebraische Abgeschlossenheit eingeht!

K^* ist natürlich auch eine elementare Oberstruktur von F. Da N in K^* enthalten ist, gilt $K^* L_i = K^* M_i$.

Teil 2:

Wir fixieren nun ein $i < \aleph_1$. Die Situation wird durch das folgende Bild illustriert:



Es sei α_i ein primitives Element für die Erweiterung $M_i \supset F(a)$. Der Körper $F(a)^{\mathrm{a}} \cap K^*$ ist in K^* relativ algebraisch abgeschlossen, also erst recht separabel abgeschlossen. Da $(F(a)^{\mathrm{a}} \cap K^*) M_i \supset F(a)^{\mathrm{a}} \cap K^*$ galoissch ist, folgt mit Bemerkung 1.5.5 schon die lineare Disjunktheit von $(F(a)^{\mathrm{a}} \cap K^*) M_i$ und K^* über $F(a)^{\mathrm{a}} \cap K^*$. Also hat α_i über K^* das gleiche Minimalpolynom $\mathrm{Irr}(\alpha_i, K^*) = \sum_{k=0}^{n} b_{i,k} x^k$ wie über $F(a)^{\mathrm{a}} \cap K^*$; ohne Einschränkung sei $\mathrm{Irr}(\alpha_i, K^*)$ normiert, es sei also $b_{i,n} = 1$. Der Grad dieses Minimalpolynoms ist n, denn es ist $[K^* M_i : K^*] = [K^* L_i : K^*] = [L_i : K] = n$.

Die Koeffizienten $\bar{b}_i = (b_{i,0}, \ldots, b_{i,n-1})$ liegen in $F(a)^{\mathrm{a}}$; sei $q_{i,k} \in F(a)[X]$ das Minimalpolynom von $b_{i,k}$ über $F(a)$. Die Koeffizienten von $q_{i,k}$ sind definierbar über F und a; sei $\bar{d}_i \in F$ so, daß sie in $\mathrm{dcl}(a, \bar{d}_i)$ liegen.

Also gibt es eine L(F)-Formel $\psi_i(x, \bar{z}) = \psi_i(x, \bar{z}, \bar{d}_i)$ mit

1) für alle $\bar{b} = (b_0, \ldots, b_{n-1})$ gilt

$$\models \psi_i(a, \bar{b}) \iff b_k \text{ ist Nullstelle von } q_{i,k}(x) \text{ für } 0 \leq k \leq n-1$$

2) $\models \forall x\, \exists^{\leq n_i} \bar{z}\, \psi_i(x, \bar{z})$, wobei $n_i := \prod_{k=0}^{n} \deg(q_{i,k})$ ist.

Da ohne Einschränkung keines der $q_{i,k}$ das Nullpolynom ist, gibt es höchstens n_i-viele $(n+1)$-Tupel $\bar{b}$, so daß b_k Nullstelle von $q_{i,k}$ ist; ein solches Tupel ist $\bar{b}_i$. Also gilt

$$\models \psi_i(a, \bar{b}_i).$$

Betrachte nun die auf K^{*n} definierbare Äquivalenzrelation

$$\bar{a}E\bar{b} :\Longleftrightarrow \models \chi_{\text{ÄR},n}(\bar{a}, \bar{b}).$$

Zur Erinnerung: Es gilt $\models \chi_{\text{ÄR},n}(\bar{a}, \bar{b})$ genau dann, wenn entweder Adjunktion einer Nullstelle von $p_{\bar{a}}$ die gleiche Galoiserweiterung erzeugt wie Adjunktion einer Nullstelle von $p_{\bar{b}}$, oder aber wenn beide Erweiterungen keine Galoiserweiterungen von Grad n sind; siehe 2.7.

Es seien $\bar{a}^\chi, \bar{b}^\chi, \ldots$ und $\bar{x}^\chi, \bar{y}^\chi, \ldots$ die Elemente bzw. Variablen der zu $\chi_{\text{ÄR}}$ gehörigen Sorte von $K^{*\text{eq}}$. Weiter sei $c_i \in F_i^{n+1}$ das Tupel mit $K_{c_i} = L_i$; da $K^* \succ K$ regulär ist, gilt dann auch $K^*_{c_i} = K^* L_i$.

Betrachte die Formel

$$\varphi_i(a, c_i^\chi, \bar{d}_i) \ = \ \exists \bar{z} \left(\psi_i(a, \bar{z}) \wedge \bar{z}^\chi \doteq c_i^\chi \right).$$

Es gilt:

1) Für alle $i < \aleph_1$ ist
$$K^* \models \varphi_i(a, c_i^\chi),$$
denn es gilt $K^* \models \psi_i(a, \bar{b}_i)$ und wegen $K^* M_i = K^* L_i$ auch $\bar{b}_i^\chi = c_i^\chi$.
2) Für alle $i < \aleph_1$ ist
$$\bigwedge_{0 \le j \le n_i} \varphi_i(x, y_j^\chi) \ \wedge \bigwedge_{0 \le j < k \le n_i} y_j^\chi \neq y_k^\chi$$
inkonsistent, da $\models \forall x \, \exists^{\le n_i} \bar{z} \, \psi_i(x, \bar{z})$ gilt.
3) Für alle abzählbaren Mengen $B \subset K$ existiert ein $j < \aleph_1$ mit $c_j^\chi \notin \operatorname{acl}^{\text{eq}} FB$, denn jedes abzählbare B ist schon in einem Modell F_j enthalten und es ist $F_j^{\text{eq}} = \operatorname{acl}^{\text{eq}}(F_j)$.

Damit sind die Bedingungen für Lemma 5.1 erfüllt, die Theorie von F ist also nicht einfach. ■Satz

So, damit wäre der Hauptteil der Arbeit geschafft. Zur Belohnung:

Schwarzer Hase

für 4 Personen; Rezept siehe [e&t, S. 180]

1 küchenfertigen Hasen (in Stücken, mit Leber und Niere) über Nacht mit 200g in Scheiben geschnittenen Zwiebeln, 2 getrockneten und zerdrückten roten Chilischoten, 1 Eßlöffel Rosmarinnadeln, 15 Pfefferkörnern, 5 Lorbeerblättern, $\frac{1}{4}$ l trockenem

Rotwein und $\frac{1}{8}$ l Rotweinessig kühl gestellt marinieren; dabei einmal wenden. Am nächsten Tag Fleisch abtrocknen, in 100g Schweineschmalz in einem Bräter anbraten und die Marinade dazugeben. Im vorgeheizten Backofen bei 225° C zugedeckt 45 Minuten schmoren.
Inzwischen 5 Eßlöffel Olivenöl erhitzen, je 50g feingewürfelten durchwachsenen Speck und Pinienkerne darin bräunen. 2 Knoblauchzehen dazupressen. Saft und Schale einer unbehandelten Orange und 50g Sultaninen zugeben, kurz durchkochen und vom Herd nehmen. 30g Bitterschokolade fein hacken, zu der Soße geben und noch einmal kurz aufkochen.
Fleisch weitere 10 Minuten ohne Deckel garen. Mit den Zwiebeln auf einer Platte anrichten und warm halten. Den Schmorfond durch ein Sieb in die Schokoladensoße gießen und aufkochen. Leber und Nieren würfeln, in etwas Butter anbraten und mit einem Teil der Soße zu dem Fleisch geben; den Rest der Soße getrennt servieren.

Dazu passen selbst gemachte Nudeln.

Anhang: Der modelltheoretische algebraische Abschluß in PAC-Körpern

Dieser Abschnitt ist eine Ausarbeitung von Lemma 4.4 und Proposition 4.5 aus [ChP]; in diesen wird der modelltheoretische algebraische Abschluß eines PAC-Körpers bestimmt.
Z. Chatzidakis benutzt in [Ch1] zum Beweis von Theorem 5.9 die Ergebnisse aus [ChP]. In dieser Arbeit haben wir diese Ergebnisse nicht benötigt; da die Beschreibung des modelltheoretischen algebraischen Abschluß es eines PAC-Körpers jedoch auch für sich genommen interessant ist, folgt hier eine Darstellung von [ChP, Lemma 4.4, Proposition 4.5].

Eine proendliche Gruppe G heißt **projektiv**, wenn zu jeder proendlichen Gruppe H und zu jedem stetigen Epimorphismus $f : H \to G$ eine abgeschlossene Untergruppe H_1 von H existiert, so daß die Restriktion von f auf H_1 ein Isomorphismus auf G ist:

$$\begin{tikzcd}
H \arrow[rr, two heads, "f"] \arrow[d, phantom, "\cup\!\mid"] & & G \\
! \ H_1 \arrow[urr, dash, "f|_{H_1}", "\cong"'] & &
\end{tikzcd}$$

abgeschlossen

Wir benötigen in diesem Kapitel noch die folgenden Eigenschaften von PAC-Körpern:

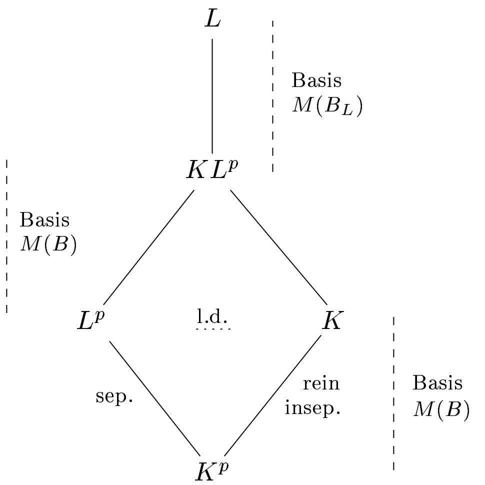
Theorem A.10. *1) (18.7 in [FJ]) Es seien $F \supseteq K$ zwei PAC-Körper von gleichem Imperfektionsgrad. Die Erweiterung $F \supseteq K$ sei separabel; außerdem sei die Restriktionsabbildung $res : G(F) \to G(K)$ ein Isomorphismus. Dann ist F eine elementare Erweiterung von K.*
2) (10.17 in [FJ]) Ist F PAC, so ist $G(F)$ projektiv.
3) (12.11 in [FJ]) Jeder Körper hat eine reguläre Erweiterung, die PAC ist.

Um den modelltheoretischen algebraischen Abschluß in PAC-Körpern beschreiben zu können, müssen wir zunächst eine ganze Reihe von Vorüberlegungen[11] machen:

Lemma A.11. *L sei eine separable Erweiterung von K, B sei eine p-Basis von K und B_L eine p-Basis von L über L^pK. Dann ist $B \,\dot\cup\, B_L$ eine p-Basis von L; dies heißt insbesondere, daß $M(B)$ eine Vektorraumbasis von KL^p über L^p ist.*

Beweis:

[11] Die Aussagen dieses Kapitels über p-Basen sind nur im Fall $p > 0$ interessant und werden für den Fall eines Körpers K der Charakteristik 0 mit den Konventionen aus Kapitel 2 trivial.



Mit $L \supseteq K$ ist auch $L^p \supseteq K^p$ eine separable Erweiterung. Also ist $L^p \underset{K^p}{\overset{l}{\smile}} K$, demnach bleibt $M(B)$ auch in KL^p linear unabhängig. Außerdem ist $M(B)$ Erzeugendensystem von KL^p über L^p, bildet also eine Vektorraumbasis von KL^p über L^p. Nach Voraussetzung ist $M(B_L)$ eine Vektorraumbasis von L über L^pK. Also ist

$$\{m_B m_{B_L} \mid m_B \in M(B), m_{B_L} \in M(B_L)\}$$

eine Basis von L über L^p, daß heißt $B \mathbin{\dot\cup} B_L$ ist eine p-Basis von L. ■

Korollar A.12. *Ist $L \supseteq K$ eine separabel algebraische Erweiterung, so ist eine p-Basis von K auch eine p-Basis von L.*

Beweis: Ist $L \supseteq K$ eine separabel algebraische Erweiterung, so gilt $L = L^pK$ (siehe [La1, 6.10]); mit A.11 folgt das Gewünschte. ■

Lemma A.13. *Es seien L_1 und L_2 zwei seperable Erweiterungen des Körpers K mit $L_1 \underset{K}{\overset{l}{\smile}} L_2$. Weiter sei B ein p-Basis von K, es sei $B \mathbin{\dot\cup} B_1$ eine p-Basis von L_1 und $K \mathbin{\dot\cup} B_2$ eine p-Basis von L_2. Dann ist $B \mathbin{\dot\cup} B_1 \mathbin{\dot\cup} B_2$ eine p-Basis von L_1L_2.*

Beweis: Wir betrachten den Körperturm

$$L_1^pL_2^p \subseteq L_1^pL_2^pK \subseteq L_1L_2^p \subseteq L_1L_2$$

und zeigen, daß $M(B_2)$ eine Vektorraumbasis von $L_1L_2 \supseteq L_1L_2^p$, $M(B_1)$ eine Vektorraumbasis von $L_1L_2^p \supseteq L_1^pL_2^pK$ und $M(B)$ eine Vektorraumbasis von $L_1^pL_2^pK \subseteq L_1^pL_2^p$ ist. Dies ist gleichbedeutend damit, daß $B \mathbin{\dot\cup} B_1 \mathbin{\dot\cup} B_2$ eine p-Basis von L_1L_2 ist.

<u>Schritt 1:</u> $M(B)$ ist eine Basis von $L_1^pL_2^pK$ über $L_1^pL_2^p$:

Wegen $L_1 \underset{K}{\overset{l}{\smile}} L_2$ und der Separabilität von $L_1 \supseteq K$ und $L_2 \supseteq K$ ist auch $L_1L_2 \supseteq K$ separabel. Gemäß A.11 ist daher $M(B)$ eine Basis von $L_1^pL_2^pK$ über $L_1^pL_2^p$. ■Schritt 1

<u>Schritt 2:</u> $M(B_1)$ ist eine Basis von $L_1L_2^p$ über $L_1^pL_2^pK$:

Aus $L_1 \underset{K}{\overset{l}{\smile}} L_2$ folgt mit der Turmeigenschaft und mit der Monotonie linearer Disjunktheit auch $L_1 \underset{L_1^pK}{\overset{l}{\smile}} L_1^pL_2^pK$. Da $M(B_1)$ eine Basis von L_1 über L_1^pK ist, bildet $M(B_1)$ dann auch eine Basis von $L_1L_2^p$ über $L_1^pL_2^pK$. ■Schritt 2

<u>Schritt 3:</u> $M(B_2)$ ist eine Basis von L_1L_2 über $L_1L_2^p$:

Wie in Schritt 2 zeigt man, daß $M(B_2)$ eine Basis von $L_1^pL_2$ über $L_1^pL_2^pK$ ist. Mit der Turmeigenschaft folgt aus $L_1 \underset{K}{\overset{l}{\smile}} L_2$ auch $L_1L_2^p \underset{L_1^pL_2^pK}{\overset{l}{\smile}} L_2L_1^p$, also ist $M(B_2)$ auch eine Basis von L_1L_2 über $L_1L_2^p$. ■Schritt 3

■

Lemma A.14. *Ist L ein Körper und ist $B \dot\cup C$ p-unabhängig in L, so ist $L^p(B)$ linear unabhängig von $L^p(\{\sqrt[p^i]{c} \mid i \in \mathbb{N}, c \in C\})$ über L^p.*

Beweis: Die Idee des Beweises ist einfach: Gäbe es für ein $n > 1$ eine nichttriviale Linearkombination von p-Monomen in B und in p^0-ten bis p^n-ten Wurzeln von Elementen aus C, so ergäbe Exponentiation mit p^n eine nichttriviale Linearkombination der p-Monome in C. Wem das als Erklärung nicht genügt, muß sich die folgende technische Ausführung anschauen.

Ohne Einschränkung sind $B := \{b_1, \dots, b_r\}$ und $C := \{c_1, \dots, c_s\}$ endlich. Es sei $\sqrt[p^i]{C} := \{\sqrt[p^i]{c_1}, \dots \sqrt[p^i]{c_s}\}$; weiter sei $(M_i(X_1, \dots, X_r))_{0 \leq i \leq p^r-1}$ eine Aufzählung der p-Monome in $X_1, \dots, X_r$ und $(N_j(Y_1, \dots, Y_s))_{0 \leq j \leq p^s-1}$ eine Aufzählung der p-Monome in $Y_1, \dots, Y_s$.
Es reicht zu zeigen, daß $L^p(B) \underset{L^p}{\overset{l}{\downarrow}} L^p(\sqrt[p^n]{C})$ für alle $n \in \mathbb{N}$ gilt. Die Elemente $M_i(B)$ für $0 \leq i \leq p^r - 1$ bilden eine Vektorraumbasis von $L^p(B)$ über L^p; die Elemente $N_{j_0}(C) \cdot N_{j_1}(\sqrt[p]{C}) \cdot \dots \cdot N_{j_n}(\sqrt[p^n]{C})$ für $0 \leq j_1, \dots, j_n \leq p^s - 1$ bilden eine Vektorraumbasis von $L^p(\sqrt[p^n]{C})$ über L^p. Es genügt also zu zeigen,daß die Elemente

$$M_i(B)N_{j_0}(C)N_{j_1}(\sqrt[p]{C}) \cdot \dots \cdot N_{j_n}(\sqrt[p^n]{C})$$

für $0 \leq i \leq p^r - 1$ und $0 \leq j_1, \dots, j_n \leq p^s - 1$ unabhängig über L^p sind. Wir beweisen dies via Induktion über n:

Ist $n = 0$, so folgt die Behauptung direkt aus der p-Unabhängigkeit von $B \dot\cup C$. Die Aussage sei für $m < n$ bereits gezeigt.
Angenommen die Elemente $M_i(B)N_{j_0}(C)N_{j_1}(\sqrt[p]{C}) \cdot \dots \cdot N_{j_n}(\sqrt[p^n]{C})$ mit $0 \leq i \leq p^r - 1$ und $0 \leq j_1, \dots, j_n \leq p^s - 1$ sind abhängig über L^p. Dann existiert eine nichttriviale Linearkombination

$$\sum_{\substack{0 \leq i \leq p^r-1 \\ 0 \leq j_0, \dots, j_n \leq p^s-1}} l^p_{ij_0 \dots j_n} M_i(B)N_{j_0}(C)N_{j_1}(\sqrt[p]{C}) \cdot \dots \cdot N_{j_n}(\sqrt[p^n]{C}) = 0$$

mit $l_{ij_0 \dots j_n}$ aus L.

Exponentiation mit p^n ergibt

$$0 = \sum_{0 \leq j_n \leq p^s-1} \underbrace{\Bigg(\sum_{\substack{0 \leq i \leq p^r-1 \\ 0 \leq j_0, \dots, j_{n-1} \leq p^s-1}} l^p_{ij_0 \dots j_n} M_i(B)N_{j_0}(C) \cdot \dots \cdot N_{j_{n-1}}(\sqrt[p^{n-1}]{C}) \Bigg)^{p^n}}_{\in L^p} N_{j_n}(C)$$

Dies ist eine Linearkombination von $N_{j_n}(C)$ über L^p. Da nicht alle $l_{ij_0 \dots j_n}$ gleich 0 sind, folgt mit der Induktionsvorraussetzung, daß die Linearkombination nicht trivial ist. Also ist C nicht p-unabhängig in L. Widerspruch! ■

Lemma A.15. *L sei ein Körper mit p-Basis $B \dot\cup C$, weiter sei $M := L(\{\sqrt[p^i]{c} \mid i \in \mathbb{N}, c \in C\})$. Dann ist B eine p-Basis von M.*

Beweis: Offensichtlich ist B ein p-Erzeugendensystem von M, denn es ist

$$M^p(B) = L^p(\{B, \sqrt[p^i]{c} \mid i \in \mathbb{N}, c \in C\}) = L(\{\sqrt[p^i]{c} \mid i \in \mathbb{N}, c \in C\}) = M.$$

Aus A.14 folgt

$$L^p(B) \underset{L^p}{\overset{l}{\perp}} L^p(\{\sqrt[p^i]{c} \mid i \in \mathbb{N}, c \in C\}) = M^p,$$

also ist B auch p-unabhängig in M. ■

Lemma A.16. *L sei ein Körper mit p-Basis $A \dot\cup \{b_j \mid j \in J\} \dot\cup \{c_j \mid j \in J\}$, weiter sei $M := L(\{\sqrt[p^i]{\frac{c_j}{b_j}} \mid i \in \mathbb{N}, j \in J\})$. Dann sind sowohl $A \dot\cup \{b_j \mid j \in J\}$ als auch $A \dot\cup \{c_j \mid j \in J\}$ p-Basen von M.*

Beweis: Es sei $B := \{b_j \mid j \in J\}$, $C := \{c_j \mid j \in J\}$ und $\frac{C}{B} := \{\frac{c_j}{b_j} \mid j \in J\}$. Offensichtlich sind für beliebige Teilmengen $A_0 \subseteq A$ und $J_0 \subseteq J$, für $B_0 := \{b_j \mid j \in J_0\}$, $C_0 := \{c_j \mid j \in J_0\}$ und $\frac{C_0}{B_0} := \{\frac{c_j}{b_j} \mid j \in J_0\}$ die p-Monome $M(A_0, B_0, \frac{C_0}{B_0})$ ein Erzeugendensystem von $L^p(A_0, B_0, C_0)$ über L^p.
Für endliche Teilmengen A_0 und J_0 ergibt sich daraus ergibt aus Kardinalitätsgründen die p-Unabhängigkeit von $A_0 \dot\cup B_0 \dot\cup \frac{C_0}{B_0}$ über L^p. Daraus folgt die p-Unabhängigkeit von $A \dot\cup B \dot\cup \frac{C}{B}$ über L^p; also ist $A \dot\cup B \dot\cup \frac{C}{B}$ eine p-Basis von L.
Nach A.15 ist also $A \dot\cup B$ eine p-Basis von M. Wegen $M = L(\{\sqrt[p^i]{\frac{c_j}{b_j}} \mid i \in \mathbb{N}, j \in J\}) = L(\{\sqrt[p^i]{\frac{b_j}{c_j}} \mid i \in \mathbb{N}, j \in J\})$ ist dann auch $A \dot\cup C$ eine p-Basis von M. ■

Lemma A.17. *Es sei L eine reguläre Erweiterungen des Körpers K. Dann existiert eine K-isomorphe Kopie L' von L mit $L \underset{K}{\overset{l}{\perp}} L'$ und ein K^s-Isomorphismus $\varphi : L^s \cong L'^s$.*

Beweis: Es sei $\{t_i \mid i \in I\}$ eine Transzendenzbasis von L über K und $\{t'_i \mid i \in I\}$ algebraisch unabhängig über $K(\{t_i \mid i \in I\})$. Dann sind $\{t_i \mid i \in I\}$ und $\{t'_i \mid i \in I\}$ auch algebraisch unabhängig über K^{a}. Also ist $K^{\mathrm{a}}(\{t_i \mid i \in I\}) \cong K^{\mathrm{a}}(\{t'_i \mid i \in I\})$ durch die Abbildung $t_i \mapsto t'_i$. Wir setzen diesen Isomorphismus auf $K(\{t_i \mid i \in I\})^{\mathrm{a}}$ fort (dies ist wegen der Eindeutigkeit des algebraischen Abschlusses möglich); das Bild der Restriktion auf L ist das gesuchte L', die Restriktion auf L^{s} ist der gesuchte K^{s}-Isomorphismus φ. Es bleibt nur noch zu zeigen, daß L und L' linear disjunkt über K sind (siehe nächstes Bild):
Die Elemente $\{t_i \mid i \in I\}$ sind auch über $K(\{t'_i \mid i \in I\})^{\mathrm{a}}$ algebraisch unabhängig. Da $K(\{t_i \mid i \in I\}) \supseteq K$ regulär ist, folgt daraus mit Lemma 1.11.3 schon die lineare Disjunktheit von $K(\{t_i \mid i \in I\})$ und $K(\{t'_i \mid i \in I\})^{\mathrm{a}}$ über K, mit der Turmeigenschaft also $K(\{t_i \mid i \in I\}) \underset{K}{\overset{l}{\perp}} L'$.
Also ist auch $L'(\{t_i \mid i \in I\}) \supseteq K(\{t_i \mid i \in I\})$ regulär; die Erweiterung $L \supseteq$

$K(\{t_i \mid i \in I\})$ ist dagegen algebraisch, also ist $L \underset{K(\{t_i|i\in I\})}{\overset{l}{\smile}} L'(\{t_i \mid i \in I\})$. Mit der Turmeigenschaft ergibt sich die lineare Disjunktheit von L und L' über K.

$$\begin{tikzcd}[column sep=small]
 & L(\{t'_i \mid i \in I\}) \arrow[dl, dash] \arrow[dr, dash] & & & \\
L \arrow[dr, dash, "\text{alg.}"] \arrow[rr, phantom, "\text{l.d.}"] & & L'(\{t_i \mid i \in I\}) \arrow[dl, dash, "\text{reg.}"] \arrow[dr, dash] & & K(\{t'_i \mid i \in I\})^{\mathrm{a}} \arrow[dl, dash] \\
 & K(\{t_i \mid i \in I\}) \arrow[dr, dash, "\text{reg.}"] \arrow[rr, phantom, "\text{l.d.}"] & & L' \arrow[dl, dash, "\text{reg.}"] & \\
 & & K & &
\end{tikzcd}$$

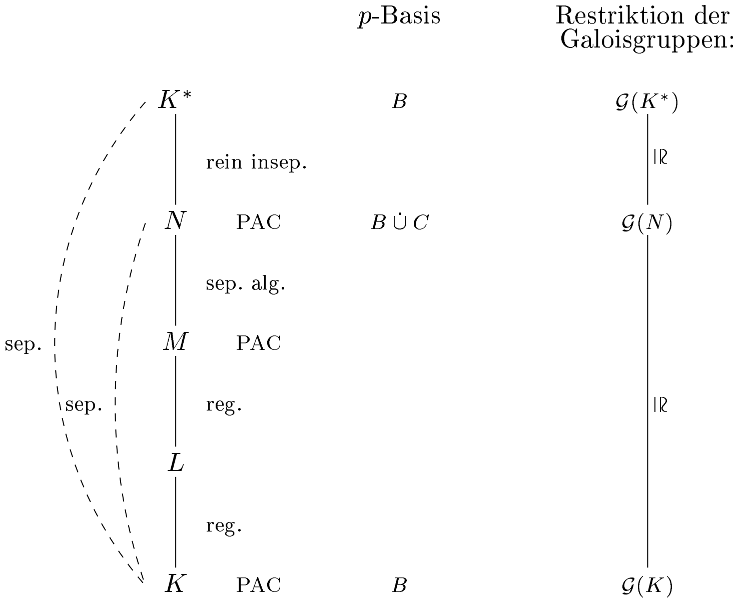
■

Lemma A.18. *Sei K ein PAC-Körper und und L eine reguläre Erweiterung von K. Dann existiert eine elementare Erweiterung K^* von K die L enthält, so daß die Restriktion $res : G(K^*) \to G(K)$ ein Isomorphismus ist. Man kann K^* so wählen, daß jede p-Basis von K auch eine p-Basis von K^* ist.*

Beweis: Ziel ist es, einen PAC-Oberkörper mit gleicher p-Basis und isomorpher Galoisgruppe wie K zu konstruieren, der eine separable Erweiterung von K ist; nach A.10.1 ist dieser dann schon eine elementare Erweiterung. Das nächste Bild illustriert den Beweis.

Wähle mit A.10.3 einen PAC-Körper $M \supseteq L$, so daß $M \supseteq L$ regulär ist. Aus der Regularität von $L \supseteq K$ und $M \supseteq L$ folgt dann die Regularität von $M \supseteq K$, also (siehe 1.10.4) ist die Restriktion $\mathcal{G}(M) \to \mathcal{G}(K)$ surjektiv. Wegen A.10.2 ist $\mathcal{G}(K)$ projektiv, also folgt per Definition die Existenz einer abgeschlossenen Untergruppe $\mathcal{G}_1$ von $\mathcal{G}(M)$, die isomorph zu $\mathcal{G}(K)$ ist. Sei $N \subseteq M^{\mathrm{s}}$ der Fixkörper von $\mathcal{G}_1$. Dann ist $res : \mathcal{G}(N) \to \mathcal{G}(K)$ ein Isomorphismus, N ist als algebraische Erweiterung von M wieder PAC (siehe 3.5) und $N \supseteq K$ ist separabel. Hat K die Charakteristik 0, so sind wir fertig. Andernfalls sei B eine p-Basis von K; wir ergänzen diese zu einer p-Basis $B \,\dot{\cup}\, C$ von N.

Betrachte die rein inseparable Erweiterung K^*, die durch Adjunktion aller p^n-ten Wurzeln von Elementen aus C entsteht. Nach A.15 ist dann B eine p-Basis von K^*, $K^* \supseteq K$ ist also separabel; weiter ist K^* als algebraische Erweiterung von N ein PAC-Körper. Da $K^* \supseteq N$ rein inseparabel ist, ist $\mathcal{G}(K^*) \cong \mathcal{G}(N) \cong \mathcal{G}(K)$ via Restriktion; also ist $K \prec K^*$. Da für jede p-Basis B' von K auch $B' \,\dot{\cup}\, C$ eine p-Basis von N ist, ist jede p-Basis von K auch eine p-Basis von K^*.



■

Lemma A.19. *Sei L ein PAC-Körper und $K \subseteq L$. Dann gilt:*

$$\mathrm{acl}_L(K) = K \iff L \supseteq K \text{ ist regulär.}$$

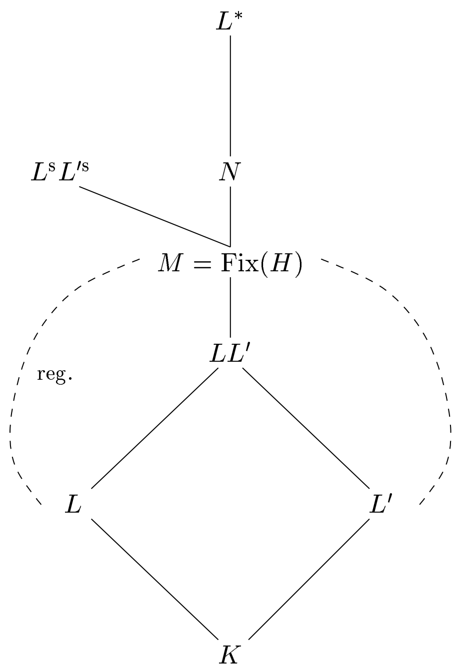
Beweis: Wir wir in Theorem 2.16 gesehen haben, gilt „$\Rightarrow$“ für beliebige Körper L. Also zur Rückrichtung:
Wie in A.17 sei $L' \supseteq K$ eine über K zu L linear disjunkte Kopie von L und $\varphi : L^{\mathrm{s}} \cong_{K^{\mathrm{s}}} L'^{\mathrm{s}}$; weiter sei $\Phi : \mathcal{G}(L) \to \mathcal{G}(L')$ der zugehörige Isomorphismus der Galoisgruppen. B sei eine p-Basis von K und $B \dot\cup C$ eine p-Basis von L; dann ist $B \dot\cup \varphi(C)$ eine p-Basis von L' und $B \dot\cup C \dot\cup \varphi(C)$ eine p-Basis von LL'.
Ziel ist es, einen Körper L^* zu konstruieren, der elementare Oberstruktur von L und von L' ist; dann ist $\mathrm{acl}_L(K) = \mathrm{acl}_{L^*}(K) = \mathrm{acl}_{L'}(K)$, es ist also $\mathrm{acl}_L(K) \subseteq L \cap L' = K$. Wegen 1.16 gilt $L^{\mathrm{s}} \underset{K^{\mathrm{s}}}{\overset{l}{\downarrow}} L'^{\mathrm{s}}$ und $\mathrm{Gal}(L^{\mathrm{s}}L'^{\mathrm{s}}/LL') \cong \mathcal{G}(L) \times_{K^{\mathrm{s}}} \mathcal{G}(L')$. Es sei

$$H' := \{(g, \Phi(g)) \mid g \in \mathcal{G}(L)\} \subseteq \mathcal{G}(L) \times_{K^{\mathrm{s}}} \mathcal{G}(L').$$

Für $\psi : \mathcal{G}(L) \times_{K^{\mathrm{s}}} \mathcal{G}(L') \to \mathcal{G}(L')$, $(g_1, g_2) \mapsto \Phi(g_1)g_2^{-1}$ gilt dann $H' = \psi^{-1}(\{1\})$, also ist H' eine abgeschlossene Untergruppe. Es sei H die H' entsprechende abgeschlossene Untergruppe in $\mathrm{Gal}(L^{\mathrm{s}}L'^{\mathrm{s}}/LL')$.

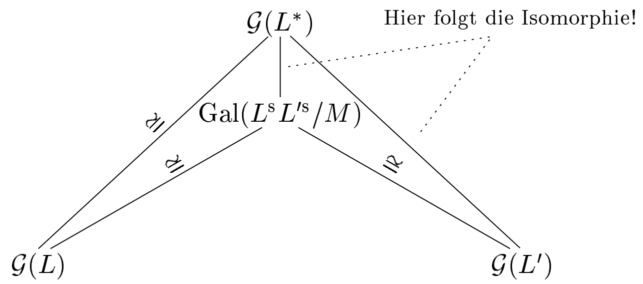
Das Bild auf der nächsten Seite illustriert die folgende Konstruktion.
Wir betrachten nun $M := \mathrm{Fix}(H) \subseteq L^{\mathrm{s}}L'^{\mathrm{s}} \subseteq LL'^{\mathrm{s}}$. Dann ist $\mathrm{Gal}(L^{\mathrm{s}}L'^{\mathrm{s}}/M)$ via Restriktion isomorph zu $\mathcal{G}(L)$ und zu $\mathcal{G}(L')$; insbesondere sind die Restriktionen $\mathcal{G}(M) \to \mathcal{G}(L)$ und $\mathcal{G}(M) \to \mathcal{G}(L')$ jeweils surjektiv. Da $M \supset L$ und $M \supseteq L'$ jeweils separabel sind, folgt hieraus die Regularität von $M \supseteq L$ und $M \supseteq L'$. Wegen A.12 ist $B \dot\cup C \dot\cup \varphi(C)$ auch eine p-Basis von M.
Es sei $N := M(\{ \sqrt[p^i]{\frac{c}{\varphi(c)}} \mid i \in \mathbb{N}, c \in C\})$. Dann ist auch N eine reguläre Erweiterung von L und von L': Denn $B \dot\cup C$ und $B \dot\cup \varphi(C)$ sind jeweils p-Basen von N, also sind

$N \supseteq L$ und $N \supseteq L'$ separabel. Da $N \supseteq M$ rein inseparabel ist, gilt $\mathcal{G}(N) \cong \mathcal{G}(M)$ via Restriktion; die Restriktionen $\mathcal{G}(N) \twoheadrightarrow \mathcal{G}(L)$ und $\mathcal{G}(N) \twoheadrightarrow \mathcal{G}(L')$ sind also wie die Restriktionen $\mathcal{G}(N) \twoheadrightarrow \mathcal{G}(L)$ und $\mathcal{G}(N) \twoheadrightarrow \mathcal{G}(L')$ surjektiv.
Mit Hilfe von A.18 finden wir eine elementare Oberstruktur L^* von L mit p-Basis $B \dot\cup C$, die N enthält, und für die die Restriktion $\mathcal{G}(L^*) \to \mathcal{G}(L)$ ein Isomorphismus ist.



Auch $B \dot\cup \varphi(C)$ ist eine p-Basis von L^*: Da $B \dot\cup C$ in L^* p-unabhängig bleibt, ist $L^* \supseteq N$ separabel; also bleibt auch $B \dot\cup \varphi(C)$ p-unabhängig in L^*. Wegen $\{ \sqrt[p^i]{\frac{c}{\varphi(c)}} \mid i \in \mathbb{N}, c \in C\} \subseteq L^*$ ist weiter klar, daß $L^{*p}[B \dot\cup \varphi(C)] = L^{*p}[B \dot\cup C] = L^*$ ist; also ist $B \dot\cup \varphi(C)$ auch ein p-Erzeugendensystem von L^*.
Also ist $L^* \supseteq L'$ eine separable Erweiterung, und der Imperfektionsgrad von L^* und von L' ist der Gleiche.

Es ist $\mathcal{G}(L^*) \cong \mathcal{G}(L)$ via Restriktion, ebenso ist die Restriktionsabbildung ein Isomorphismus von $\mathrm{Gal}(L^{\mathrm{s}}L'^{\mathrm{s}}/M)$ auf $\mathcal{G}(L)$. Also ist die Restriktion auf $L^{\mathrm{s}}L'^{\mathrm{s}}$ ein Isomorphismus von $\mathcal{G}(L^*)$ auf $\mathrm{Gal}(L^{\mathrm{s}}L'^{\mathrm{s}}/M)$; da auch $\mathrm{Gal}(L^{\mathrm{s}}L'^{\mathrm{s}}/M)$ und $\mathcal{G}(L')$ via Restriktion isomorph sind, erhält man insgesamt, daß $\mathcal{G}(L^*)$ und $\mathcal{G}(L')$ via Restriktion isomorph sind. Zur Veranschaulichung dient das folgende Bild; dabei sind alle Isomorphismen die entsprechenden Restriktionsabbildungen.



Also folgt aus A.10.1, daß L^* auch eine elementare Oberstruktur von L' ist. ■

Korollar A.20. *Sei L ein PAC-Körper und $K \subseteq L$. Dann gilt:*

$$\mathrm{acl}_L(K) = \mathrm{cl}_{\lambda_L}(K)^a \cap L$$

Beweis: „$\supseteq$" ist klar, da der Abschluß von K unter den λ-Funktionen von L sogar in $\mathrm{dcl}(K)$ enthalten ist, und im körpertheoretischen Sinne algebraische Elemente immer auch im modelltheoretischen algebraischen Abschluß liegen.
Zu „$\subseteq$" : Es reicht zu zeigen, daß $L \supseteq \mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L$ regulär ist.
$L \supseteq \mathrm{cl}_{\lambda_L}(K)$ ist separabel, also auch $\mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L \supseteq \mathrm{cl}_{\lambda_L}(K)$. Da $\mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L \supseteq \mathrm{cl}_{\lambda_L}(K)$ algebraisch ist, haben $\mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L$ und $\mathrm{cl}_{\lambda_L}(K)$ die gleichen p-Basen. Da $L \supseteq \mathrm{cl}_{\lambda_L}(K)$ separabel ist, bleibt jede p-Basis von $\mathrm{cl}_{\lambda_L}(K)$, und damit jede p-Basis von $\mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L$, in L p-unabhängig. Also ist $L \supseteq \mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L$ separabel.
Da $\mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L$ relativ algebraisch abgeschlossen in L ist, ist $L \supseteq \mathrm{cl}_{\lambda_L}(K)^{\mathrm{a}} \cap L$ auch primär und insgesamt regulär. ■

Zum Abschluß noch etwas Süßes:

Karamel-Apfel-Pudding mit Vanillesosse

für 4 Personen

Pudding: 4 Eier trennen. Das Eigelb mit 1 Packet Vanillinzucker schaumig schlagen. 3 Eßlöffel Zucker karamelisieren lassen, 50g gehackte Walnüsse dazugeben. Walnußkrokant abkühlen lassen und hacken. 50g Butter erhitzen, bis sie leicht gebräunt ist; etwas abkühlen lassen und zusammen mit dem Walnußkrokant und 3 gehäuften Eßlöffeln Mehl unter das Eigelb rühren. Weitere 2 Eßlöffel Zucker karamelisieren, mit 10 Eßlöffeln Sahne ablöschen und kochen, bis der Karamel sich gelöst hat (eventuell noch etwas Wasser zugeben). Unter die Eigelbmasse rühren. Einen kleinen in Stücke geschnittenen Apfel dazugeben. Die 4 Eiweiß steif schlagen und unterheben. Eine Puddingform buttern und mit Semmelbröseln ausstreuen; die Masse einfüllen und die Form verschließen. In einem Topf im Wasserbad ca. 60 Minuten garen (die Puddingform sollte zu ungefähr $\frac{2}{3}$ im Wasser stehen).

Soße: 4 Eigelb mit dem Mark einer Vanilleschote, einem Becher Sahne und Zucker nach Geschmack unter Rühren im Wasserbad aufschlagen, bis eine schaumige Créme entsteht.

Literatur

[Ax] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239-271

[Bou] E. Bouscaren, *Model Theory and Algebraic Geometry*, Lecture Notes in Mathematics 1696, Springer Verlag, 1998

[CDM] G. Cherlin, L. van den Dries, A. Macintyre, *Decedability and Undecidability Theorems for PAC-fields*, Bull. AMS 4 (1981), 101-104

[Ch1] Z. Chatzidakis, *Simplicity and Independence for Pseudo-algebraically closed fields*, Models and computability (Leeds, 1997), 41–61, London Math. Soc. Lecture Note Ser., 259, Cambridge Univ. Press, Cambridge, 1999

[Ch2] Z. Chatzidakis, *Properties of forking in ω-free pseudo-algebraically closed fields*, J. Symbolic Logic 67 (2002), Nr. 3, 957-996

[ChP] Z. Chatzidakis, A. Pillay, *Generic structures and simple theories*, Ann. Pure Appl. Logic 95 (1998), no. 1-3, 71-92.

[CK] C. C. Chang, H. J. Keisler, *Model Theory* Studies in Logic and the Foundations of Mathematics, North-Holland Publishing Company, 1973

[CS] G. Cherlin, S. Shelah, *Superstable fields and groups*, Ann. Math. Logic 18 (1980), 227-270

[Du] J. L. Duret, *Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance*, Model Theory of Algebra and Arithmetic, Lecture Notes in Mathematics 834, Springer Verlag, 1980

[E1] Yu. L. Ershov, *Regularly closed fields*, Dokl. Akad. Naud SSSR 268 (1980), Nr. 1, 16-20

[E2] Yu. L. Ershov, *Undecidability of regularly closed fields*, Algebra i Logika 20 (1981) Nr. 4, 389-394, 484

[En] O. Endler, *Valuation Theory*, Springer-Verlag, 1972

[e&t] Das große Italien Kochbuch – herausgegeben von der Zeitschrift Essen & Trinken, erschienen im Naumann & Göbel Verlag, 1991

[FJ] M. D. Fried, M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 11, Springer-Verlag, 1986

[Ho] W. Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1993

[Hr] E. Hrushovski, *Pseudofinite fields and related structures*, Preprint (1992)

[Hu] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften, Band 134, Springer Verlag, 1967

[Ja] M. Jarden, *The elementary theory of ω-free Ax fields*, Inv. Math. 38 (1976), 187-206

[JK] M. Jarden, U. Kiehne, *The elementary theory of algebraic fields of finite corank*, Inv. Math. 30 (1975), 275-294

[K1] B. Kim, *Simple first order theories*, PhD thesis, University of Notre Dame, Notre Dame, USA, 1996

[K2] B. Kim, *Forking in simple unstable theories*, J. London Math. Soc. 57 (1998), 257-267

[KP1] B. Kim, A. Pillay, *Simple theories*, Ann. Pure Appl. Logic 88 (1997), 149-164

[KP2] B. Kim, A. Pillay, *From stability to simplicity*, Bull. Symbolic Logic 4 (1998), 17-26

[La1] S. Lang, *Algebra*, Addison-Wesley Publishing Company, Inc., 1993

[La2] S. Lang, *Introduction to algebraic geometry*, Addison-Wesley Publishing Company, Inc., 1973

[Las] D. Lascar, *Stability in Model Theory*, Longman Scientific & Technical, 1987

[Mc] A. Macintyre, *On ω_1-categorical theories of fields*, Fund. Math. 71 (1971), Nr. 1, 1-25

[Mo] M. Morley, *Cateroricity in power*, Trans. AMS 114 (1965), 514-538

[Poi1] B. Poizat, *Cours de Théorie des Modèles*, NUR AL-MANTIQ WAL-MA'RIFAH, 1985

[Poi2] B. Poizat, *Groupes stables*, NUR AL-MANTIQ WAL-MA'RIFAH, 1987

[Pop] F. Pop, *Embedding Problems over large fields*, Ann. of Math. (2) 144 (1996) no.1, 1-34

[R] F. Rowbottom, *The Los conjecture for uncountable theories*, Notices of the AMS 11 (1964), 248

[Sch] H. Scheuermann, *Unabhängigkeitsrelationen*, Diplomarbeit, Albert-Ludwigs-Universität Freiburg, Deutschland, 1996

[Sh1] S. Shelah, *Classification Theory and the number of non-isomorphic models*, Revised Edition, North-Holland Publishing Company, 1990

[Sh2] S. Shelah, *Simple unstable Theories*, Annals of Math. Logic 19 (1980), 177-203

[St] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993

[Wa] F. O. Wagner, *Simple Theories*, Mathematics and Its Applications, Kluwer Academic Publishers, 2000

[Wae] B.L. van der Waerden, *Algebra I*, Springer-Verlag, 1993

[W] C. Wood, *Notes on the stability of separably closed fields*, J. Symb. Logic 44 (1979), Nr. 3, 412-416

Verzeichnis der verwendeten Symbole:

Index

Ich versichere hiermit, diese Arbeit selbständig und nur unter Zuhilfenahme der angegebenen Mittel und Quellen angefertigt zu haben.