01

Dienstag, 17. April 2018 22:21

Algebraische Zahlentheorie II.

Übungsblätter: Vorlesungshomepage.

01. Proendliche Gruppen

Why. · X Menge, Topologie auf X: $\mathcal{T} \subseteq \mathcal{P}(X)$ mit
(0) $\emptyset, X \in \mathcal{T}$ (1) $U, V \in \mathcal{T} \Rightarrow U \cap V \in \mathcal{T}$ (2) $(U_i)_{i \in I} \in \mathcal{T}^I \Rightarrow \bigcup_i U_i \in \mathcal{T}$

· $\mathcal{B} \subseteq \mathcal{T}$ heißt Basis $:\Leftrightarrow \forall U \in \mathcal{T}\ \exists (B_i)_{i \in I} \in \mathcal{B}^I: U = \bigcup_i B_i$

· $W \subseteq X$ heißt Umgebung (von $x \in X$) $:\Leftrightarrow \exists V \in \mathcal{T}: x \in V \subseteq W$.

Für $x \in X$ sei $\mathcal{U}(x)$ die Menge aller Umgebungen von x.

z.B.: (X, d) metrischer Raum $\Rightarrow \{B_\varepsilon(x) \mid x \in X, \varepsilon > 0\}$ ist Basis für X.

· $(X, \mathcal{T}_X) \xrightarrow{f} (Y, \mathcal{T}_Y)$ heißt stetig $:\Leftrightarrow f^{-1}(\mathcal{T}_Y) \subseteq \mathcal{T}_X$.

· Produkttopologie: Seien $((X_i, \mathcal{T}_i))_{i \in I}$ topologische Räume.

Basis der Produkttopologie auf $\prod_i X_i$: $\left\{\prod_i U_i \mid U_i \in \mathcal{T}_i, U_i = X_i \text{ f.f.a. } i \in I\right\}$

Satz von Tychonoff: Sind alle X_i kompakt, so auch $\prod_i X_i$

· Sei $X \xrightarrow{\pi} Y$ surjektiv, $(X, \mathcal{T})$ top. Raum.

$\{V \subseteq Y \mid \pi^{-1}(V) \in \mathcal{T}\}$ heißt Quotiententopologie.

Def. 1.1. (a) Eine topologische Gruppe $(G, e, \circ, \mathcal{T})$ besteht aus einer Gruppe $(G, e, \circ)$ und einem top. Raum $(G, \mathcal{T})$ so dass

$G \times G \xrightarrow{\mu} G$, $(g, h) \mapsto g \circ h$, $G \xrightarrow{i} G$, $g \mapsto g^{-1}$ stetig sind, wobei $G \times G$ die Produkttopologie trägt.

(b) Ein Morphismus topologischer Gruppen ist ein stetiger Gruppenhomomorphismus.

$\leadsto$ Man erhält die Kategorie topologischer Gruppen $\underline{\text{Top Grp}}$.

Bsp. (ü) K normierter Körper $\Rightarrow (K, +)$, $(K^\times, \cdot)$ sind topologische Gruppen.

Facts 1.2. Seien G, G' top. Grp., $G \xrightarrow{\phi} G'$ ein Gruppenhomomorphismus.

(i) $l_g : G \to G,\ h \mapsto g\circ h$, $\ r_g : G \to G,\ h \mapsto h\circ g$ sind Automorphismen (insb. Homöomorphismen)

(ii) ϕ ist stetig $\iff \forall\, W' \in \mathcal{U}(e') : \exists\, W \in \mathcal{U}(e) : \phi(W) \subseteq W'$

(iii) Eine offene Untergruppe $H \underset{\text{offen}}{\leq} G$ ist abgeschlossen.

(iv) Eine abgeschlossene Untergruppe $H \underset{\text{abg.}}{\leq} G$ mit $[G:H] < \infty$ ist offen.

(v) Ist G kompakt, $H \leq G$ offen, so gilt $[G:H] < \infty$.

(vi) Ist $H \leq G$ Untergruppe, so ist $(H, \tau_{G|H})$ eine topologische Untergruppe (Unterraumtop.)

(vii) Ist $U \underset{\text{offen}}{\subseteq} G$, so ist $U^{-1} \underset{\text{offen}}{\subseteq} G$ und $cl(U) = \overline{U} \subseteq UU^{-1}$

(viii) G ist regulär, d.h. $\forall g \in G : \exists\, U, V \in \mathcal{U}(g)$ offen s.d. $V \subseteq \overline{V} \subseteq U$

(ix) G ist hausdorffsch $\iff \{e\} \underset{\text{abg.}}{\subseteq} G$

(x) Ist $N \trianglelefteq G$ Normalteiler, so ist G/N topologische Gruppe mit Quotiententopologie.
Dabei ist G/N hausdorffsch, falls $N \underset{\text{abg.}}{\subseteq} G$.

(xi) Sind $(G_i)_{i\in I}$ top. Grp., so ist $\prod_i G_i$ top. Grp.

Beweis.

(i) $l_g = G \to \{g\} \times G \xrightarrow{\text{inkl.}} G \times G \xrightarrow{\mu} G$ ist stetig, $l_g \circ l_{g^{-1}} = id_G$

r_g analog.

(ii) "$\Rightarrow$": klar; "$\Leftarrow$": Sei $g \in G$, $g' := \phi(g)$, $W \in \mathcal{U}(g')$. Wähle $V \in \mathcal{U}(e)$ mit $\phi(V) \subseteq \underbrace{(g')^{-1}W}_{= l_{g'^{-1}}(W)}$

$\Rightarrow \phi(l_g(V)) \subseteq W$, also ist ϕ stetig.

(iii) $G = H \,\dot\cup\, \underbrace{\bigcup_{\substack{g \in G/H \\ g \neq 0}} gH}_{\text{offen, da } gH = l_g(H)}$

(iv) wie (iii): $G = H \,\dot\cup\, \underbrace{\bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{abg}}}_{\text{abg., da endliche Vereinigung wg. } [G:H] < \infty}$

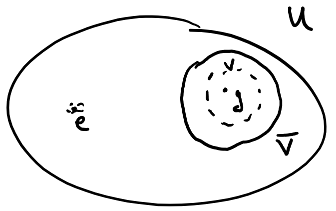
(v) $G = \bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{offen}}$ $\quad G$ kompakt $\Rightarrow [G:H] < \infty$

(vi), (vii): Übung.

(viii) oE $g = e$ wegen (i). Sei U offene Umgebung von e.

Beh. (ii) $\exists$ offene Umgb. V von e mit $V \cdot V \subseteq U$, $V = V^{-1}$. Nun verwende (vii).

(ix) z.z.: können e und $g \neq e$ trennen (wg. (i))



$$G \setminus \bar{V} \cap V = \emptyset$$

(x), (xi) Übung. ∎

Wdh. I sei teilgeordnete, filtrierte Menge, d.h. $\forall i,j \in I : \exists k \in I : i,j \leq k$.

Ein inverses System (von Gruppen) besteht aus einer Familie von Gruppen $(G_i)_{i \in I}$ zusammen mit Gruppenhomomorphismen $\phi_{ji} : G_j \to G_i$ $\forall i,j \in I$ mit $i \leq j$.

so dass: (i) $\phi_{ii} = id_{G_i}$ (ii) $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$ $\forall i \leq j \leq k$

Dann heißt $\varprojlim_{i \in I} G_i$ Limes des inversen Systems .... hat übliche universelle Eigenschaft.

· $\varprojlim_{i \in I} G_i$ existiert und ist gegeben durch $G := \{ (g_i)_{i \in I} \in \prod_i G_i \mid \phi_{ji}(g_j) = g_i \ \forall i \leq j \}$

Lemma 1.3. Sind alle G_i topologische Gruppen, so auch $\varprojlim G_i$ mit der Unterraumtop. von $\prod_i G_i$.
Sind alle G_i hausdorffsch (kompakt + hausdorffsch), so ist auch $\varprojlim G_i$ hausdorffsch (kpt. + hd.).

Beweis.

① $\prod_i G_i$ ist selbst $\varprojlim G_i$ für geeignet gewähltes inverses System I.

Alle G_i hausdorffsch $\Rightarrow$ $\prod_i G_i$ hausdorffsch (Produkte von Hausdorffräumen sind hausdorffsch)

Kompakt folgt mit dem Satz von Tychonoff.

② Allgemeiner Fall: Hausdorffsch überträgt sich auf Unterräume $\Rightarrow$ $\varprojlim G_i$ hd.

$$\varprojlim G_i = \bigcap_{i \leq j} \underbrace{\{ (g_k)_k \in \prod_k G_k \mid \phi_{ji}(g_j) = g_i \}}_{" = " \ \Gamma_{\phi_{ji}} \times \prod_{k \neq i,j} G_k \ \underset{\text{abg.}}{\subseteq} \ \prod_k G_k} \underset{\text{abg.}}{\subseteq} \prod_k G_k$$

$\left(\Gamma_{\phi_{ji}} \underset{\text{abg.}}{\subseteq} G_i \times G_j \text{ da } G_i \text{ hd.} \right)$

$\Rightarrow \varprojlim G_i$ kpt. da abg. Teilraum eines kpt. Raumes. ∎

Def. 1.4. Eine proendliche Gruppe ist ein inverser Limes $\varprojlim G_i$ endlicher, diskreter topologischer Grp. $(G_i)_{i \in I}$ mit der Topologie aus 1.3.

(insb.: alle G_i hausdorffsch und kompakt)

Def. 1.5. Ein topologischer Raum heißt total unzusammenhängend $:\Leftrightarrow$

Jedes $x \in X$ besitzt eine Umgebungsbasis aus offen-abgeschlossenen Mengen

$\underset{\ddot{u}}{\Leftrightarrow}$ Die Zusammenhangskomponente von x ist $\{x\}$

Proposition 1.6. (ü) Eine kpt., hd. top. Grp. ist total unzusammenhängend $\Leftrightarrow$

e besitzt eine Umgebungsbasis aus offen-abgeschlossenen Normalteilern von G. ☒

05

Freitag, 20. April 2018 09:17

Korrektur: X top. Raum.

X heißt **zusammenhängend** $:\Leftrightarrow$ $\emptyset, X$ sind die einzigen offen + abg. Teilmengen.

$x \sim_{zh} y \;:\Leftrightarrow\; \exists\, Y \subseteq X$ zshgd.: $x, y \in Y$. ist Äquivalenzrelation

Äquivalenzklassen unter $\sim_{zh}$ heißen **Zusammenhangskomponenten**.

Lemma. (Ribes-Zaleski, Lemma 1.1.11)
X kpt., hd. und $x \in X$. Dann ist die Zusammenhangskomp. die x enthält die Menge

$$[x]_{zh} = \bigcap \{ U \subseteq X \mid x \in U,\ U \text{ offen abg.} \}$$

Def. 1.5. Ein topologischer Raum X heißt **total-unzusammenhängend** $\Leftrightarrow$ alle Zshgskomp. von X sind 1-elementig.

Korollar. (aus Lemma) Sei X kompakt, hd. Dann gilt:
X total unzshgd $\Leftrightarrow$ Jedes $x \in X$ besitzt eine Umgebungsbasis aus offen-abg. Mengen.

Satz 1.7. Sei G eine topologische Gruppe. Dann sind äquivalent:
(i) G ist proendlich (ii) G ist kompakt, hausdorffsch und total unzusammenhängend.

Beweis.
(i) $\Rightarrow$ (ii): kompakt, hausdorffsch: letztes Mal.
g.z.z.: $e \in \prod G_i$ besitzt Umgebungsbasis aus offen abgeschlossenen Teilmengen.
Eine solche ist gegeben durch $\left\{ \prod_{i \in I_0} \{e_{i_0}\} \times \prod_{I \setminus I_0} G_i \;\middle|\; I_0 \subseteq I \text{ endlich} \right\} =: \mathcal{U}_e$ ← offen, abg. Normalteiler

letztes Mal: G kpt., hd., $H \leq G$ offene Untergrp. $\Rightarrow$ H abg.

Allgemeiner Fall: Schneide $\mathcal{U}_e$ mit $\varprojlim G_i$.

(ii) $\Rightarrow$ (i): Konsequenz aus dem folgenden Lemma. ∎

Lemma 1.8. Sei G kompakt, hausdorffsch, total unzshgd. und $\mathcal{U}$ eine Umgebungsbasis der Eins bestehend aus offen-abg. Normalteilern.
Dann ist

$$G \xrightarrow{\varphi} \varprojlim_{N \in \mathcal{U}} G/N, \quad g \longmapsto (gN)_{N \in \mathcal{U}}$$

ein Isomorphismus topologischer Gruppen. (G/N endl. diskret)

Beweis. φ stetig: "obvious".
betrachte $G \longrightarrow \prod_{N \in \mathcal{U}} G/N$ ← hat Umgebungsbasis $\mathcal{U}_e$ (s. 1.7).

Für $I_0 \subseteq \mathcal{U}_e$ endl. $\rightsquigarrow$ Umgebung $\prod_{N \in I_0} N/N \times \prod_{N \in \mathcal{U}_e \setminus I_0} G/N$

Urbild ist $\bigcap_{N \in I_0} N$ ist offen abg. Normalteiler in G $\Rightarrow$ stetig bei e $\Rightarrow$ stetig.

φ injektiv: $\varphi(g) = (e_N)_{N \in \mathcal{U}} \Rightarrow g \in N \;\; \forall N \in \mathcal{U}$.
Umgebungsbasis, G hausdorffsch.

$$\Rightarrow \bigcap_{\mathcal{U}_0} N = \{e\}, \text{ d.h. } g = e.$$

· φ surjektiv. Sei $(g_N \cdot N)_{N \in \mathfrak{U}} \in \varprojlim G/N$ $(N' \subseteq N \Rightarrow g_{N'} N = g_N N)$

gesucht:
$$g \in \underbrace{\bigcap_{N \in \mathfrak{U}} (g_N N)}_{\text{abg.}} \subseteq G \text{ kompakt}$$

Anm.:
rechte Seite leer $\Rightarrow \exists I_0 \subseteq \mathfrak{U}$ endlich: $\bigcap_{N \in I_0} gN = \emptyset$. $\mathfrak{U}$ Umgebungsbasis

$\Rightarrow \exists N' \subseteq \bigcap_{N \in I_0} N$

φ Homöomorphismus: φ bijektiv, stetig, G kompakt, $\varprojlim G/N$ hausdorffsch. ▨

Bem. 1.9. (i) 1.8 ist anwendbar, wenn G proendlich
(ii) analog zu 1.8 lassen sich auch beweisen: G proendlich, $\mathfrak{U}$ wie 1.8

(a) $\forall\ H \leq G$ abg. gilt: $H \xrightarrow{\sim} \varprojlim_{N \in \mathfrak{U}} H/N \cap H$

(b) $\forall\ H \trianglelefteq G$ abg. gilt $G/H \xrightarrow{\sim} \varprojlim_{N \in \mathfrak{U}} G/N \cdot H$

Lemma 1.10. Sei G proendlich, $H \leq G$ Untergruppe. Dann sind äquivalent:
(i) H ist abgeschlossen

(ii) $H = \bigcap \{ U \mid U \leq G \text{ offene Untergruppe mit } H \leq U \}$

Beweis.
"$\Leftarrow$": $U \leq G$ offen $\underset{G \text{ kpt.}}{\Rightarrow}$ U abg. Untergruppe $\Rightarrow \bigcap \{U \ldots\}$ ist abgeschlossen.

"$\Rightarrow$": Sei $V \in \mathfrak{U}$ ($\mathfrak{U}$ wie oben) $\Rightarrow \underbrace{H \cdot V}_{= \bigcup_{h \in H} hV}$ ist offene Untergruppe von G.

In Ü: $\underset{\text{Teilmenge}}{H \subseteq G}$ kompakt $\Rightarrow \bigcap_{V \in \mathfrak{U}} H \cdot V = H$. ▨

Def. 1.11. Eine pro-p Gruppe ist ein inverser Limes von endlichen p-Gruppen.
(Insb. proendlich)

Def. 1.12. Sei G eine diskrete (i.a. unendliche) Gruppe.
Die pro-p Komplettierung von G ist
proendliche

$$\hat{G}^p := \varprojlim \{ G/N \mid N \trianglelefteq G \text{ und } G/N \text{ ist endliche } p\text{-Grp.} \}$$
endliche

Bsp. $\hat{\mathbb{Z}}^p = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$

(man kann auch Ringe pro-p oder pro-endl. komplettieren)

Def. 1.13. Der Prüferring ist die proendliche Komplettierung von $\mathbb{Z}$, $\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$

($\{n\mathbb{Z} \mid n \in \mathbb{N}\}$ bzgl. Inklusion, d.h. Teilbarkeit geordnet)

Lemma. $\hat{\mathbb{Z}} \cong \prod_{p \text{ prim}} \mathbb{Z}_p$

Beweis. $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \underset{\text{CRS}}{\cong} \varprojlim_n \left(\prod_{p \text{ prim}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z} \right)$; $\prod_p \mathbb{Z}_p \overset{\text{pro endl.}}{=} \varprojlim_{U \in \mathcal{U}} \prod \mathbb{Z}_p/U = \varprojlim_n \prod \mathbb{Z}_p/U_n$

$$\mathcal{U} = \{ \underbrace{\prod_p (p^{v_p(n)} \mathbb{Z}_p)}_{=:U_n} \mid n \in \mathbb{N} \}$$

■

Def. 1.14 Eine Teilmenge $S \subseteq G$ heißt **topologisches Erzeugendensystem** (ES) $:\Leftrightarrow$ G ist der topologische Abschluss der von S erzeugten Untergrp.

Bsp. $\{1\}$ ist topologisches EZS von $\mathbb{Z}_p$ und $\hat{\mathbb{Z}}$

Def. 1.15 Eine topologische Gruppe G heißt **topologisch endlich erzeugt** $:\Leftrightarrow \exists\, S \subseteq G$ endlich s.d. S ist top. EZS von G

Bsp. Die proendl. bzw. pro-p Komplettierung der freien nicht-abelschen Gruppen mit endlich vielen Erzeugern

Satz 1.16. (**Burnside Basissatz**)
Sei G eine pro-p-Gruppe. Sei $\Phi(G)$ der topologische Abschluss der von $[G,G]$ und $G^p = \{g^p \mid g \in G\}$ erzeugten Untergruppe. ($\Phi(G)$ heißt **Frattini-Untergruppe** von G)

Dann: G ist topologisch endl. erz. $\Leftrightarrow$ $G/\Phi(G)$ ist endlicher $\mathbb{F}_p$-VR.

Bilden $\overline{b_1}, \dots, \overline{b_n}$ eine Basis von $G/\Phi(G)$, dann ist $\{b_1, \dots, b_n\}$ ein <u>minimales</u> EZS.

Beweis. (ü).

■

<u>Bem.</u> 1) $G/\overline{[G,G]}$ ist abelsche, hausdorff. topol. Grp.

$\rightarrow$ $G/\overline{[G,G]G^p}$ ist abelsche p-Torsionsgruppe (d.h. $\mathbb{F}_p$-VR)

(— " — heißt **p-elementar abelsch**)

2) Sei G eine abelsche pro-p-Gruppe.

(a) Dann ist G ein $\mathbb{Z}_p$-Modul!, d.h. haben stetige $\mathbb{Z}_p$-Operation $\mathbb{Z}_p \times G \to G$

$$\underbrace{\alpha}_{\in \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}} \cdot \underbrace{g}_{= (g_i)_i \in \varprojlim \underline{G_i}} := \underbrace{(\alpha \bmod \underbrace{\# G_i}_{p\text{-Potenz}} \cdot g_i)_{i \in I}}_{= \alpha \bmod \operatorname{ord}(g_i) \cdot g_i} \in \varprojlim_I G_i = G.$$

(G_i:) endl. abelsche p-Grp.

(<u>wohldef</u>? $\pi_{ji}: \begin{cases} G_j \to G_i \\ g_j \mapsto g_i \end{cases}$ $\pi_{ji}(\alpha \bmod \operatorname{ord}(g_j) \cdot g_j) = (\alpha \bmod \operatorname{ord}(g_i) \cdot g_i)$)

$\operatorname{ord}(g_i) \mid \operatorname{ord}(g_j)$

z.B. $$(1 + p\mathbb{Z}_p, \cdot) = \varprojlim_n \underbrace{\left(1+p\mathbb{Z}_p / 1+p^n\mathbb{Z}_p \right)}_{= \{ \beta \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid \beta \equiv 1 \ (p) \} = \langle 1+p \rangle \cong \mathbb{Z}/p^{n-1}}$$

■

$\beta \in 1+p\mathbb{Z}_p$, $\alpha \in \mathbb{Z}_p$ $\rightsquigarrow$ $\beta^\alpha \in 1 + p\mathbb{Z}_p$

(b) G topol. endlich erzeugt $\underset{ü}{\Longleftrightarrow}$ G ist endl. erz. als $\mathbb{Z}_p$-Modul

In diesem Fall kann man den Strukturssatz für endl. erz. Moduln über HI-Ringen anwenden
$\Rightarrow G \simeq \mathbb{Z}_p^r \times \prod_{i=1}^{t} \mathbb{Z}/p^{n_i}$ ...

02. Galoistheorie und unendliche Galoiserweiterungen

Whg. $L|K$ algebraische Erweiterung von Körpern

$L|K$ normal $\Longleftrightarrow \forall \alpha \in L$: $\mathrm{mipo}_K(\alpha) \in K[X]$ zerfällt über L in Linearfaktoren
$L|K$ separabel $\Longleftrightarrow \forall \alpha \in L$: $\mathrm{mipo}_K(\alpha)$ besitzt nur einfache Nullstellen in K^{alg}.
$L|K$ galoissch $:\Longleftrightarrow$ $L|K$ normal + separabel

Definiere dann: $\mathrm{Gal}(L/K) := G_{L|K} := \{ \sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K \}$

Fakt: Ist $L|F|K$ ein Zwischenkp., so ist $L|F$ galoissch.

Hauptsatz der endlichen Galoistheorie: $L|K$ endlich $\Rightarrow$ Die Abbildungen

$$\{ H \leq \mathrm{Gal}(L|K) \text{ UG} \} \underset{\mathrm{Gal}(L|F) \leftarrow F}{\overset{H \mapsto L^H}{\longleftrightarrow}} \{ L|F|K \text{ Zwischenkp.} \}$$

definiert eine Bijektion.

$$\{ H \trianglelefteq G \text{ NT} \} \overset{1:1}{\longleftrightarrow} \{ F \text{ Zwkp.} \mid F|K \text{ galoissch} \}$$

Was geht schief, wenn $L|K$ unendlich?
Man hat zu viele Untergruppen!

Proposition 2.1. Sei $L|K$ galoissch. Sei $\Sigma := \{ E|L \text{ Unterkörper} \mid E|K \text{ endlich galoissch} \}$, geordnet mit $\subseteq$, $\rightsquigarrow (\Sigma, \subseteq) \longrightarrow \mathrm{Grp}$, $E \longmapsto \mathrm{Gal}(E|K)$ ist ein inverses System.

Dann ist
$$\mathrm{Gal}(L|K) \xrightarrow{\rho} \varprojlim_{E \in \Sigma} \mathrm{Gal}(E/K), \quad \sigma \mapsto (\sigma|_E)_{E\in\Sigma}$$
ein Gruppenisomorphismus.

Beweis.

- Homomorphismus nach Konstruktion.
- Injektiv: $\rho(\sigma) = \mathrm{id} \iff \sigma|_E = \mathrm{id}_E \; \forall E \in \Sigma \implies \sigma = \mathrm{id}_L$
- Surjektiv: Sei $(\sigma_E)_{E\in\Sigma} \in \varprojlim_{E\in\Sigma} \mathrm{Gal}(E/K) \subseteq \prod_{E\in\Sigma} \mathrm{Gal}(E/K)$

$$\underline{\text{d.h.:}} \quad E'/E \in \Sigma \implies \sigma_{E'}|_E = \sigma_E$$

Wegen $L = \bigcup_{E\in\Sigma} E$, definiere $\sigma : L \longrightarrow L$, $\alpha \longmapsto \sigma_E(\alpha)$ falls $\alpha \in E \in \Sigma$

(wohldefiniert, da $(\sigma_E)_E$ kompatibel)

$$\implies \sigma \in \mathrm{Gal}(L/K) \text{ mit } \rho(\sigma) = (\sigma_E)_E$$

(Automorphismus da $\sigma|_E$ Automorphismus)

$\square$

Def. 2.2. Die **Krulltopologie** auf $\mathrm{Gal}(L|K)$ ist die Topologie für welche ρ ein Isomorphismus topologischer Gruppen wird. (mit der proendl. Topologie auf $\varprojlim_{\Sigma} \mathrm{Gal}(E/K)$)

<u>Konkret</u>: Umgebungsbasis der Eins in $\mathrm{Gal}(L|K)$ ist $\{ \underbrace{\mathrm{Gal}(L/E)}_{= \ker(\mathrm{Gal}(L|K) \to \mathrm{Gal}(E|K))} \mid E \in \Sigma \}$ $\leftarrow$ Umgebungsbasis offen-abg. Normalteiler von $\mathrm{Gal}(L|K)$

Lemma 2.3. Sei $L|K$ galoissch. Dann sind die offenen Untergruppen von $\mathrm{Gal}(L|K)$ gerade die Untergruppen $\mathrm{Gal}(L|F)$ mit $F|K$ endlich.

Beweis. Sei $H \leq \mathrm{Gal}(L|K)$ offene Untergruppe. Wähle $E \in \Sigma$ mit $\mathrm{Gal}(L|E) \subseteq H$.

$$\implies \overline{H} = \text{Bild von } H \text{ in } \mathrm{Gal}(E/K) = \{ \sigma|_E \mid \sigma \in H \} \quad \left(= \mathrm{Gal}(L|K) / \mathrm{Gal}(L/E) \right)$$

$$\begin{array}{c} L \\ | \\ E \\ | \\ F \\ | \\ K \end{array} \quad \text{endlich}, \; \overline{H}$$

Sei $F = E^{\overline{H}}$ ... Prüfe: $H = \mathrm{Gal}(L/F)$.

Umgekehrt: $F|K$ endl. Erweiterung in $L \rightsquigarrow$ Sei E der Galoisabschluss von $F|K$

$$\implies [E:K] < \infty \implies \underbrace{\mathrm{Gal}(L|E)}_{\text{offen}} \subseteq \mathrm{Gal}(L|F).$$

$$\implies \underbrace{\mathrm{Gal}(L|F) = \bigcup_{g \in \mathrm{Gal}(L|F)/\mathrm{Gal}(L|E)} g\, \mathrm{Gal}(L|E)}_{} \underset{\text{offen}}{\subseteq} \mathrm{Gal}(L|K)$$

$\square$

Korollar 2.4. Sei L wie in 2.3. Dann gilt:
$$\{H \leq Gal(L|K) \mid H \text{ abg.}\} = \{Gal(L|F) \mid L|F|K\}$$

Beweis.
"$\supseteq$": Schreibe $F = \bigcup_{i\in I} F_i$, I Menge, $F_i|K$ endl. Erw.

Dann:
$$\underset{\sigma|_F = id_F}{Gal(L|F)} = \bigcap_{i\in I} \underbrace{\underset{\sigma|_{F_i} = id_{F_i}}{Gal(L|F_i)}}_{\text{offen-abgeschlossen}}$$

"$\subseteq$": Jede abg. Untergruppe einer proendlichen Gruppe ist der Durchschnitt offener Untergruppen (1.10)

$$H = \bigcap_{i\in I} U_i \qquad U_i: \text{ offene Untergruppe in } G, \quad U_i = Gal(L|F_i) \text{ nach 2.3}$$

$$\underset{F=K[F_i|i\in I]}{\longrightarrow} \quad = \bigcap_{i\in I} Gal(L|F_i) = Gal(L|F)$$

$\square$

Satz 2.5. Sei $L|K$ galoisch. Dann sind die Abbildungen

$$\{H \leq Gal(L|K) \mid H \text{ abg.}\} \underset{Gal(L/F) \longleftarrow F}{\overset{H \longmapsto L^H}{\rightleftarrows}} \{F \subseteq L \mid F|K \text{ Körpererweiterung}\}$$

zueinander inverse Bijektionen (ordnungsumkehrend). Die Restriktionen der Abbildungen definieren Bijektion:

$$\{H \trianglelefteq Gal(L|K) \mid H \text{ abg. Normalteiler}\} \rightleftarrows \{E \subseteq L \mid E|K \text{ Galoiserweiterung}\}$$

Dabei gilt (topologisch):
$$Gal(L/K)/N \xrightarrow{\sim} Gal(L^N/K)$$

Beweis. Reduktion auf den endlichen Fall. – Sharifi 8.3.6.

$\square$

Bezeichnung: K ein beliebiger Körper.

K^{alg} bezeichne einen algebraischen Abschluss

$\underset{\text{ist galoisch über } K}{K^{sep}} \subseteq K^{alg}$ bezeichne einen separablen Abschluss $\quad (K^{sep} = \{\alpha \in K^{alg} \mid K(\alpha)|K \text{ separabel}\})$

$$\rightsquigarrow \quad G_K := Gal(K^{sep}/K) \text{ die absolute Galoisgruppe von } K$$

$$\left(\begin{array}{l} Aut_K(K^{alg}) \longrightarrow G_K \\ \quad \sigma \longmapsto \sigma|_{K^{sep}} \end{array} \text{ ist ein Isomorphismus} \right)$$

Bsp. • $G_{\mathbb{F}_q} \simeq \hat{\mathbb{Z}}$ $\quad (\mathbb{F}_q$ perfekt $\Rightarrow \mathbb{F}_q^{alg} = \mathbb{F}_q^{sep})$

$\mathbb{F}_{q^n} = \{\alpha \in \mathbb{F}_q^{alg} \mid \alpha^{q^n} = \alpha\} \mid \mathbb{F}_q$ galoissch mit $Gal(\mathbb{F}_{q^n} / \mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$

$(\sigma_q : \alpha \mapsto \alpha^q) \longleftrightarrow 1$

und $\mathbb{F}_q^{alg} = \bigcup_n \mathbb{F}_{q^n} \Rightarrow G_{\mathbb{F}_q} \cong \varprojlim_{(\mathbb{N},|)} Gal(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \cong \hat{\mathbb{Z}}$

• $\zeta_n := e^{\frac{2\pi i}{n}} \in \mathbb{C} \Rightarrow \mathbb{Q}_p(\zeta_{p^\infty}) := \bigcup_{n \in \mathbb{N}} \mathbb{Q}_p(\zeta_{p^n})$

$$\Rightarrow Gal(\mathbb{Q}_p(\zeta_{p^\infty}) / \mathbb{Q}_p) = \varprojlim Gal(\mathbb{Q}_p(\zeta_{p^n}) / \mathbb{Q}_p) = \varprojlim (\mathbb{Z}/p^n)^\times$$

$$= \mathbb{Z}_p^\times$$

($\zeta_n \in K^{alg}$ primitive n-te EW sofern $\operatorname{char} K \nmid n$ und falls $n \mid n'$ $(\operatorname{char} K \nmid n')$ wollen $\zeta_n = (\zeta_{n'})$)

Bezeichnung: $G_{\mathbb{Q}_p} \xrightarrow[\text{Projektion}]{\text{kanonische}} Gal(\mathbb{Q}_p(\zeta_{p^\infty}) / \mathbb{Q}_p) \xrightarrow[\text{isom.}]{\text{obiger}} \mathbb{Z}_p^\times$

heißt p-adischer Kreisteilungscharakter.

Analog: $\tilde{\mathbb{Q}} = \bigcup_n \mathbb{Q}(\zeta_n)$ (alle n) wissen $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \prod_{p \text{ PZ}} Gal(\mathbb{Q}(\zeta_{p^{v_p(n)}})/\mathbb{Q})$

$$Gal(\tilde{\mathbb{Q}} / \mathbb{Q}) \cong \varprojlim Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_{p \text{ PZ}} Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \prod_p \mathbb{Z}_p^\times = (\hat{\mathbb{Z}})^\times$$

Satz (Kronecker-Weber)

$\tilde{\mathbb{Q}} = \mathbb{Q}^{ab}$ wobei $K^{ab} = \bigcup \{E \mid K$ galoissch $\mid Gal(E/K)$ abelsch$\}$

u: $Gal(K^{ab} / K) \simeq G_K^{ab} = G_K / \overline{[G_K, G_K]}$ ∎

Bemerkung. $G_{\mathbb{Q}_p}$ für $p > 2$ ist beschrieben durch Koch-Jansen-Wingberg. (~ 1985)

$(\widehat{G}_K^p$, K lokal: $\sim 1967)$

03. Weitere Eigenschaften lokaler Körper

Sei K ein nicht-archimedischer lokaler Körper. Sei $\mathcal{O} = \mathcal{O}_K$ Bewertungsring, $v = v_K : K^\times \to \mathbb{Z}$ normalisierte Bewertung.

$k := k_K$ (endl.!) Restklassenkörper, $\pi \in \mathcal{O}$ Primelement (Uniformisierer von K)

$p = \operatorname{char} k$, $q = \# k$, $f = [k : \mathbb{F}_p]$, $e := \begin{cases} e(K/\mathbb{Q}_p), & K \mid \mathbb{Q}_p \\ 0, & \text{sonst} \end{cases}$

A. Die multiplikative Gruppe von K

Def. 3.1. Für $i \in \mathbb{N}_0$ sei $\mathcal{U}_i := \mathcal{U}_i(K)$ definiert als $\mathcal{U}_0 := \mathcal{O}^\times$, $\mathcal{U}_i = 1 + \pi^i \mathcal{O}$ für $i \geq 1$.
Sei $\mu^{(p)}(K) = \{ \zeta \in K^\times \mid \exists\, n \in \mathbb{N} : \zeta^n = 1 \text{ und } p \nmid n \} \subseteq \mathcal{O}^\times$ endliche Untergruppe

Lemma 3.2. $\mu^{(p)}(K) \longrightarrow k^\times$, $\zeta \longmapsto \zeta \bmod \pi$ ist Gruppeniso. (ü)

Proposition 3.3. Die kanonische Abbildung $\pi^{\mathbb{Z}} \times \mu^{(p)}(K) \times \mathcal{U}_1 \longrightarrow K^\times$ ist ein topologischer Isomorphismus
(ANT I, topologisch: ü)

Lemma 3.4. $\forall i \in \mathbb{N}_0$: $\mathcal{U}_i / \mathcal{U}_{i+1} \xrightarrow{\sim} (k, +)$, $1 + a\pi^i \longmapsto a \bmod \pi$ ist Gruppenisomorphismus.

Beweis.
$$(1 + a\pi^i)(1 + b\pi^i) = 1 + (a + b(1 + \pi^i a))\pi^i \qquad (i \geq 1)$$
$$\in (1 + (a+b)\pi^i)\, \mathcal{U}_{i+1}$$

$\Rightarrow$ $\mathcal{U}_i \to (k, +)$, $1 + a\pi^i \mapsto a \bmod \pi$ ist Gruppenhomomorphismus

mit Kern $\mathcal{U}_{i+1}$.

$\boxtimes$

Korollar 3.5. $\forall i \in \mathbb{N}_{\geq 1}$: $\mathcal{U}_i \xrightarrow{\sim} \varprojlim_{j \geq i} \mathcal{U}_i / \mathcal{U}_j$ ($\rightsquigarrow \mathcal{U}_i$ ist pro-p Gruppe)

Beweis.
<u>injektiv</u>: ✓
<u>surjektiv</u>: Sei $\overline{\alpha_j} \in \mathcal{U}_i / \mathcal{U}_j$ kompatible Familie. Wähle $\alpha_j \in \mathcal{U}_i$ mit Reduktion $\overline{\alpha_j}$.

$\Rightarrow$ $(\alpha_j)_j$ bilden CF in $\mathcal{O}^\times \subseteq \mathcal{O}$ $\underset{\substack{\mathcal{U}_i \text{ kpt.} \\ (\mathcal{O} \text{ kpt.!})}}{\Longrightarrow}$ $\alpha := \lim_j \alpha_j$ existiert in $\mathcal{U}_i$.

$\rightsquigarrow$ $\alpha \longmapsto (\overline{\alpha_j})_j$.

$\boxtimes$

Lemma 3.6. Sei K p-adisch, $i \geq 1$. Dann:

(0) $(1+\pi^i a)^p \equiv 1 + p\pi^i a + \pi^{pi} a^p \mod \pi^{e+2i}\mathcal{O}$ $\qquad e = e(K/\mathbb{Q}_p) = v_K(p)$ $\quad (p \mathrel{\hat{=}} \pi^e)$

(1) $(1+\pi^i a)^p \equiv 1 + a^p \pi^{ip} \mod \pi^{ip+1}$, falls $i < \frac{e}{p-1}$

(2) $(1+\pi^i a)^p \equiv 1 + p\pi^i a \mod \pi^{i+e+1}$, falls $i > \frac{e}{p-1}$

(3) $(1+\pi^i a)^p \equiv 1 \mod \pi^{i+e}$, falls $i = \frac{e}{p-1}$

Beweis. (0): Binomischer Lehrsatz und $p \mid \binom{p}{j}$ für $j = 1 \dots p-1$

und $v(\pi^{2i} p) = 2i + e$

(1)–(3): $v(p\pi^i) > v(\pi^{pi}) \iff e + i > pi \iff \frac{e}{p-1} > i$, etc. $\blacksquare$

Korollar 3.7. Sei K p-adisch. $\mathcal{O}^\times \xrightarrow{\varphi} \mathcal{O}^\times$, $\alpha \mapsto \alpha^p$. Dann gilt:

(1) $\forall i > \frac{e}{p-1}$: $\forall k \geq 1$: φ induziert Isomorphismus $U_i / U_{i+k} \xrightarrow{\sim} U_{i+e} / U_{i+e+k}$

(2) $\forall i > \frac{e}{p-1}$: φ induziert Isomorphismus $U_i \xrightarrow{\sim} U_{i+e}$

Beweis.
(1) $\underline{k=1}$:

$$\begin{tikzcd} U_i/U_{i+1} \arrow[r] \arrow[d, phantom, "\cong"] & U_{i+e}/U_{i+e+1} \arrow[d, phantom, "\cong"] \\ (k,+) & (k,+) \end{tikzcd} \qquad \begin{tikzcd} (1+a\pi^i)\,U_{i+1} \arrow[r, mapsto, "3.6"'] \arrow[d, mapsto] & (1+pa\pi^i)\,U_{i+e+1} \arrow[d, mapsto] \\ a \mod \pi & a \cdot \underbrace{\frac{p}{\pi^e}}_{\text{Einheit}} \mod \pi \end{tikzcd}$$

(aus 3.6. Isomorphismus!)

Induktion:

$$\begin{tikzcd} 1 \arrow[r] & U_{i+1}/U_{i+k+1} \arrow[r] \arrow[d, "\cong", "\mathrm{IV}"'] & U_i/U_{i+k+1} \arrow[r] \arrow[d, "\cong"] & U_{i+k}/U_{i+k+1} \arrow[r] \arrow[d, "\cong \ \mathrm{IV}"] & 1 \\ 1 \arrow[r] & U_{i+e+1}/U_{i+e+k+1} \arrow[r] & U_{i+e}/U_{i+e+k+1} \arrow[r] & U_{i+e+k}/U_{i+e+k+1} \arrow[r] & 1 \end{tikzcd}$$

$\cong$: Schlangenlemma.

(2) verwendet

$$\begin{tikzcd} U_i \arrow[r, "\sim"] \arrow[d, "\cong"] & \varprojlim_{j \geq i} U_i/U_j \arrow[d, "\cong \ \varphi \bmod \dots"] \\ U_{i+e} \arrow[r] & \varprojlim_{j \geq i} U_{i+e}/U_{j+e} \end{tikzcd}$$

rechts Isomorphismus wegen (1). $\blacksquare$

(2) alternativ:

$$\begin{array}{ccc} \underbrace{(1+\pi^i\mathcal{O},\cdot)}_{=\mathcal{U}_i} & \underset{\exp}{\overset{\log}{\rightleftarrows}} & (\pi^i\mathcal{O},+) \\ \downarrow \varphi & = & \downarrow p\cdot - \quad \text{ist Isomorphismus} \\ (\mathcal{U}_{i+e},\cdot) & \underset{\exp}{\overset{\log}{\rightleftarrows}} & (\pi^{i+e}\mathcal{O},+) \end{array}$$

$\boxtimes$

27.04.18

Satz 3.8. K sei p-adischer Körper. Dann:

(1) $\mathcal{U}_1(K) \cong \mu_{p^\infty}(K) \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ als topologische Gruppen.

(2) $K^\times \cong \pi^{\mathbb{Z}} \times \mu^{(p)}(K) \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ als topologische Gruppen.

Dabei:

- $\mu_{p^\infty}(K) = \{\zeta\in K^\times \mid \exists n>0: \ \zeta^{p^n}=1\}$
- $\#\mu_{p^\infty}(K) < \infty$: $[K:\mathbb{Q}_p]<\infty$ und $[\mathbb{Q}_p(\zeta_{p^n}):\mathbb{Q}_p] = \phi(p^n)$
  $p^{n-1}(p-1) \xrightarrow[n\to\infty]{} \infty$

Bemerkung: · $\mathcal{U}_1(K)$ ist abelsche pro-p-Gruppe, d.h. $\mathbb{Z}_p$-Modul. (letztes mal)

· $\mathcal{U}_1(K)_{tors} \cong \mu_{p^\infty}(K)$ und $\mathcal{U}_1(K)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p \cong \mathbb{Q}_p^{[K:\mathbb{Q}_p]}$

Beweis. (2) folgt aus (1) und 3.3.

(1) $\mathcal{U}_1(K)$ ist abelsche pro-p-Gruppe.

$$\mathcal{U}_1(K)_{tors} = \{x\in\mathcal{U}_1(K) \mid \exists n\in\mathbb{N}: \ x^{p^n}=1\} = \mu_{p^\infty}(K) \ (<\infty)$$

Beh. $\mathcal{U}_1(K)$ topol. endl. erz. $\Big[\Rightarrow \mathcal{U}_1(K)$ endl. erz. $\mathbb{Z}_p$-Modul
$\Rightarrow \mathcal{U}_1(K) \cong \mathcal{U}_1(K)_{tors}\times\mathbb{Z}_p^r$ für ein $r\in\mathbb{N}_0$

Dazu: (Burnside Basissatz) z.z. $\mathcal{U}_1(K)/\mathcal{U}_1(K)^p$ endlich

dazu: $\mathcal{U}_1(K)^p \supseteq \mathcal{U}_{i_0}(K)^p \underset{3.7.}{=} \mathcal{U}_{i_0+e}(K)$ für $i_0 = \left\lceil \frac{e}{p-1} \right\rceil$

$\Rightarrow \mathcal{U}_1(K)/\mathcal{U}_1(K)^p$ ist Quotient von $\mathcal{U}_1(K)/\mathcal{U}_{i_0+e}(K)$ ← endliche p-Gruppe
$(\mathcal{U}_i/\mathcal{U}_{i+1} \cong (k,+)$ endl.$)$

$\Rightarrow$ Behauptung gezeigt.

Behauptung: $r = [K:\mathbb{Q}_p]$ $\quad \mathcal{U}_1/\mathcal{U}_i$ endl. $\forall i\geq 1$

$\Rightarrow \operatorname{rang}_{\mathbb{Z}_p}\mathcal{U}_1 = \operatorname{rang}_{\mathbb{Z}_p}\mathcal{U}_{i_0}$

wegen log, exp: $U_{i_0} \underset{\log}{\cong} \pi^{i_0}\mathcal{O}_K$ als $\mathbb{Z}_p$-Modul (als pro-p-Gruppe)

$$\mathrm{rang}_{\mathbb{Z}_p} \mathcal{O}_K = \mathrm{rang}_{\mathbb{Q}_p} \mathcal{O}_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \dim_{\mathbb{Q}_p} K = [K:\mathbb{Q}_p]$$

Alternativ: U_{i_0} ist p-torsionsfrei, denn $x \mapsto x^p$ ist Isomorphismus $U_{i_0} \to U_{i_0+e}$

$\Rightarrow U_{i_0}$ ist freier $\mathbb{Z}_p$-Modul (von endl. Rang)

$$\underset{\text{Nakayama}}{\Longrightarrow} \mathrm{rang}_{\mathbb{Z}_p} U_{i_0} = \mathrm{rang}_{\mathbb{F}_p} U_{i_0}/U_{i_0}^p = \mathrm{rang}_{\mathbb{F}_p} U_{i_0}/U_{i_0+e} = \log_p(\# U_{i_0}/U_{i_0+e})$$

$$= \log_p((\underbrace{\# k}_{=p^f})^e) = ef = [K:\mathbb{Q}_p]$$

Satz 3.9. (ohne Beweis, s. Ü)

Für $K \cong \mathbb{F}_q((\pi))$ gilt $U_1(K) \cong \mathbb{Z}_p^{\mathbb{N}}$

Abb. $\mathbb{Z}_p^{\mathbb{N}} \to U_1$: Sei $b_1, \dots, b_f$ Basis von k über $\mathbb{F}_p$.

Behauptung: $\prod_{\substack{n \in \mathbb{N} \\ p \nmid n}} \prod_{j=1}^{f} \mathbb{Z}_p \longrightarrow U_1(K)$, $(a_{nj})_{n,j} \longmapsto \prod_{n,j} (1 + b_j \pi^n)^{a_{nj}}$

B. Zahm verzweigte Erweiterungen (ζ_n primitive n-te EW)

Proposition 3.10. $L|K$ lokale Körper, $n \in \mathbb{N}$ mit $p \nmid n$.

(a) $K(\zeta_n)$ ist unverzweigt über K

(b) Für $m := \# k_L^{\times}$ gilt $K(\zeta_m) \subseteq L$ und $K(\zeta_m)$ ist größte unverzweigte Erweiterung von K in L. ($\Rightarrow L|K(\zeta_m)$ ist total verzweigt)

(c) Zu $\in \mathbb{N}$ $\exists!$ unverzweigte Erweiterung K_ℓ von K mit $[K_\ell : K] =$, nämlich $K = K(\zeta_{q^\ell - 1})$, $K_\ell | K$ ist galoissch und

$$\mathrm{Gal}(K_\ell | K) \xrightarrow{\sim} \mathrm{Gal}(k(\zeta_{q^\ell - 1})/k) \cong \mathbb{Z}/\ell\mathbb{Z}$$

Beweis. (vgl. ANT I)

(a) Man betrachtet $X^m - 1$ ($p \nmid m$ und wendet Hensels Lemma an. $\Rightarrow [K(\zeta_n):K] = [k(\zeta_n):k]$

$\Rightarrow f(K(\zeta_n)|K) = [K(\zeta_n):K]$

(Hensel: $\deg \mathrm{mipo}_K \zeta_m = \deg \mathrm{mipo}_k \zeta_m$). Hensel zeigt auch $K(\zeta_m) \subseteq L$ und $k_L = k_K(\zeta_m)$

($\Rightarrow L|K(\zeta_m)$ voll verzweigt) $\Rightarrow$ (a), (b), (c).

Hatten in ANT I gezeigt. $\exists$ kanonische Surjektion $\rho_{L|K}: \mathrm{Gal}(L|K) \to \mathrm{Gal}(k_L|k)$ falls $L|K$ galoissch.

Für $L|K$ algebraisch ($L \subseteq K^{alg}$, $K \subseteq L$) sei

$$\mathcal{F}_{L|K} := \{ F \subseteq L \mid F|K \text{ endl. Körpererweiterung} \}$$

Def. 3.11.

(1) $L|K$ heißt unverzweigt $:\Leftrightarrow$ alle $F \in \mathcal{F}_{L|K}$ sind unverzweigt über K.

(2) $L|K$ heißt total verzweigt $:\Leftrightarrow$ alle $F \in \mathcal{F}_{L|K}$ sind total verzweigt über K.

(3) $K^{ur} := \bigcup \{ F \in \mathcal{F}_{K^{sep}|K} \mid F/K \text{ unverzweigt} \}$ $(= \varinjlim \dots)$

(die max. unverzweigte Erweiterung von K (in K^{alg}))

(4) Für $F \subseteq F'$ in $\mathcal{F}_{L|K}$ haben kanonische Inklusion $k_F \hookrightarrow k_{F'}$

Sei $k_L = \bigcup \{ k_F \mid F \in \mathcal{F}_{L|K} \}$ $(= \varinjlim \dots)$

(Bem.: $k_L \xleftarrow{\sim} \mathcal{O}_L / m_L$; Bewertung auf K setzt sich eind. auf L fort)

Bem. (a) $K^{ur} = \bigcup_m K(\zeta_{q^m - 1})$ $(= \varinjlim \dots)$

(b) $K^{ur} \cap L$ für bel. L ist die maximale unverzweigte Erweiterung von K in L.

Def. 3.12. $L|K$ galoissch.

(i) Erhalten kanonischen Homomorphismus $\rho_{L|K} : Gal(L|K) \longrightarrow Gal(k_L|k)$

(als $\varprojlim \rho_{E|K} : \varprojlim_{\substack{E \in \mathcal{F}_{L|K} \\ E|K \text{ galoissch}}} (Gal(E|K) \longrightarrow Gal(k_E/k))$)

(ii) $I_{L|K} := \ker(\rho_{L|K})$, $I_K := I_{K^{sep}/K}$

(iii) Haben $\sigma : k_L \to k_L$, $\alpha \mapsto \alpha^q$ in $Gal(k_L/k)$ (topol. Erz.) $q = \# k$

Nenne $Fr \in Gal(L|K)$ einen Frobeniusautomorphismus $:\Leftrightarrow \rho_{L|K}(Fr) = \sigma$

Bem. (1) Haben "wieder" kurze exakte Sequenzen $1 \to I_{K/L} \to Gal(L|K) \xrightarrow{\rho_{L|K}} Gal(k_L/k) \to 1$

als inverser Limes analoger Sequenzen für $E \in \mathcal{F}_{L|K}$ mit $E|K$ galoissch.

(2) Fr ist eindeutig $\Leftrightarrow$ $\rho_{L|K}$ ist Isomorphismus $\Leftrightarrow$ $L|K$ ist unverzweigt (d.h. $I_{L|K} = \{1\}$)

Für $L = K^{ur}$: $Gal(K^{ur}/K) \xrightarrow{\sim} Gal(k^{alg}/k) \cong \hat{\mathbb{Z}}$.

Def. 3.13. (a) Gilt $[L:K] < \infty$, so heißt $L|K$ zahm verzweigt $:\Leftrightarrow p \nmid e(L|K)$ ($= \operatorname{char} k$)

(b) $L|K$ heißt zahm verzweigt $:\Leftrightarrow$ alle $F \in \mathcal{F}_{L|K}$ sind zahm verzweigt über K

(c) $L|K$ heißt wild verzweigt $:\Leftrightarrow$ $L|K$ ist nicht zahm verzweigt.
($p \mid e(F|K)$ für ein $F \in \mathcal{F}_{L|K}$)

Bsp. (a) $e \in \mathbb{Z}_{\geq 2}$ mit $p \nmid e \Rightarrow L = K(\sqrt[e]{\pi})$ zahm verzweigt (und total unverzweigt)

(b) $p = \operatorname{char} k$, $L|K$ inseparabel $\rightarrow$ $L|K$ wild verzweigt

(c) $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ zahm, total verzweigt. $(e = \phi(p) = p-1)$

$\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ wild verzweigt für $n \geq 2$ $(e = \phi(p^n))$

Proposition 3.14. Sei $L|K$ zahm verzweigt, $[L:K] < \infty$, $E = L \cap K^{ur}$, $e = e(L|K)$. Dann:

(a) $L = E(\sqrt[e]{\pi_E})$ für π_E geeignetes Primelement von E.

(b) $E' := E(\zeta_{e \cdot \# k_E^\times})$, $L' := LE'$ $\Rightarrow L' = E'(\sqrt[e]{\underset{=\pi_K}{\pi}})$

und $E'|K$ unverzweigt, $L'|L$ unverzweigt --- ($L'|K$ galoissch)

Beweis.

(a) Sei π_L Primelement von $\mathcal{O}_L \Rightarrow \pi\mathcal{O}_L = \pi_L^e \mathcal{O}_L$, d.h. $\alpha \in \mathcal{O}_L^\times$: $\pi = \pi_L^e \alpha$

wissen $\mathcal{O}_L^\times = \mu^{(p)}(L) \times U_1(L)$ $\Rightarrow \underset{\text{in}}{\alpha} = \zeta \cdot u$ (mit $\zeta \in \mu^{(p)}(L)$, $u \in U_1(L)$) $\Big\}$ $U_1(L)$ ist (endl. erz.) $\mathbb{Z}_p$-Modul, $e \in \mathbb{Z}_p^\times$ $\Rightarrow \exists\, u' \in U_1(L): (u')^e = u$.

$\Rightarrow \zeta^{-1}\pi = (\pi_L \cdot u')^e$

beachte: $\mu^{(p)}(L) = \mu^{(p)}(E)$ da $k_L = k_E$ $\Big\}$ $\Rightarrow \pi_E := \zeta^{-1}\pi$ Primelement von $\mathcal{O}_E$ und $L = E(\sqrt[e]{\pi_E})$

(denn: $L = E(\pi_L)$, da $[L:E] = e(L|E) = e(L|K) = e$)

(b) wähle $\xi \in \mu^{(p)}(E)$ mit $\xi^e = \zeta$ $(\zeta^{\# k_E^\times} = 1)$

Dann: $\pi = (\pi_L \cdot u' \xi)^e \Rightarrow L' = E'(\sqrt[e]{\pi})$.

Bsp. (ii) $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{\pi'})$ für geeigneten Uniformisierer in $\mathbb{Q}_p$.

Bch.: $\pi = -p$ tut's!

Def. G pro-endlich abelsch. $\Rightarrow$ G ist $\hat{\mathbb{Z}}$-Modul.

Modulstruktur: $\hat{\mathbb{Z}} \times G \longrightarrow G, \ (\alpha, g) \longmapsto \underbrace{\alpha \cdot g}_{?}$

$n \in \mathbb{Z} \Rightarrow n \cdot g := g^n$

Für $\hat{a} \in \hat{\mathbb{Z}}$ beliebig: schreibe $\hat{a} = (a_n)_n \in \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$ $(a_n \in \mathbb{Z})$

prüfe: (g^{a_n}) "konvergieren" $((g^{a_n})$ hat end. Häufungspunkt!)

Proposition 3.15.

(a) Sind L, L' zahm verzweigt über K, so auch LL' ($\Rightarrow \exists$ größte zahm verzw. Erw. K^{tr} von L in K^{sep})

(b) Die maximal zahm verzweigte Erweiterung von K in K^{alg} ist

$$K^{tr} = \bigcup_{p \nmid n} K^{ur}(\sqrt[n]{\pi})$$

(c) K^{tr}/K^{ur} ist galoissch und $\mathrm{Gal}(K^{tr}/K^{ur}) \underset{\text{kan.}}{\cong} \underbrace{\prod_{\substack{\ell \neq p \\ \ell \text{ prim}}} \mathbb{Z}_\ell}_{= \hat{\mathbb{Z}}/\mathbb{Z}_p} =: \hat{\mathbb{Z}}^{(p)}$

(d) $K^{tr}|K$ ist galoissch mit $\mathrm{Gal}(K^{tr}/K) \cong \hat{\mathbb{Z}}^{(p)} \rtimes \hat{\mathbb{Z}}$ so dass für geeignete topologische Erzeuger $t \in \hat{\mathbb{Z}}^{(p)}$ und $s \in \hat{\mathbb{Z}}$ gilt:

$$sts^{-1} = t^q \quad (q = \# k)$$

Beweis.

(a) Für $L, L' | K$ endl: $e(LL'/K) \mid e(L|K)\, e(L'|K)$ (aus ANT 1) oder 3.14

(b) Folgt aus 3.14 (b)

(c) $\mathrm{Gal}(K^{ur}(\sqrt[n]{\pi}) \mid K^{ur}) \cong \mathbb{Z}/n\mathbb{Z}$ (nach Kummertheorie)

$(p \nmid n)$ Galoiskonjugierten von $\sqrt[n]{\pi}$ sind $(\zeta_n^i \sqrt[n]{\pi})_{i=1}^n$ (Algebra I)

$\varprojlim(\ldots) = \varprojlim_{p \nmid n}(\quad) \cong \hat{\mathbb{Z}}^{(p)}$

(d) (ii) Sei $K(n) := K(\zeta_{q^n-1}, \sqrt[q^n-1]{\pi})$; Beh.: $K(n)|K$ galoissch mit $\mathrm{Gal}(K(n)|K) \cong \underbrace{\mathbb{Z}/_{q^n-1}\mathbb{Z}}_{\substack{t=1 \\ \text{zahm total verzweigt}}} \rtimes \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\substack{s=1 \\ \text{unverzweigt } \mathrm{Gal}(K(\zeta_{q^n-1})|K)}}$

$\underline{\underline{\text{und}}}$: $sts^{-1} = t^q$

▨

04. Höhere Verzweigungsgruppen.

Sei K ein lokaler Körper. Seien $\mathcal{O}, \pi, k = k_K, v = v_K, q$ wie in 03.

Sei $L|K$ endlich galoissch mit $G = Gal(L|K)$. Seien $\mathcal{O}_L, \pi_L, k_L, v_L$ wie für K.

(v_L normalisiert, keine Fortsetzung von v_K)

Wdhg. ANT 1: $\exists x \in \mathcal{O}_L$ mit $\mathcal{O}_K[x] = \mathcal{O}_L$ ($L|K$ total verzweigt $\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\pi_L]$)

Lemma 4.1. Für $\sigma \in G$ und $i \in \mathbb{Z}_{\geq -1}$ sind äquivalent:

a) σ operiert trivial auf $\mathcal{O}_L / \pi_L^{i+1} \mathcal{O}_L$

b) $v_L(\sigma(a) - a) \geq i+1 \quad \forall a \in \mathcal{O}_L$

c) $v_L(\sigma(x) - x) \geq i+1$ für x wie oben.

Beweis.

a) $\Leftrightarrow$ b) $\Rightarrow$ c): klar.

c) $\Rightarrow$ b): $\sigma(\sum_i a_i x^i) - \sum_i a_i x^i = (\sigma x - x) \sum_i a_i \underbrace{\frac{(\sigma x)^i - x^i}{\sigma x - x}}_{\in \mathcal{O}_L}$, $a_i \in \mathcal{O}_K$

$$v_L(\ldots) = v_L(\sigma x - x) + \underbrace{?}_{\geq 0} \geq i+1$$

∎

Def. 4.2.

(i) $i_{L|K}(\sigma) := v_L(\sigma x - x) \quad \forall \sigma \in G$

(ii) Für $i \geq -1$ sei $G_i := \{\sigma \in G \mid i_{L|K}(\sigma) \geq i+1\}$ die i-te höhere Verzweigungsgruppe.

Bemerkung 4.3.

(0) $G_i = \bigcap_{\bar{x} \in \mathcal{O}_L / \pi^{i+1} \mathcal{O}_L} Stab_G(\bar{x}) \Rightarrow G_i$ Untergruppe.

(1) $G_{-1} = G$, $G_i = \{id\}$ für $i \gg 1$ ($\sigma \neq id \Rightarrow \sigma x - x \neq 0 \ldots$)

$G_0 \underset{4.1}{=} \{\sigma \in G \mid \sigma x \equiv x \mod \pi\} = I_{L|K} = \ker(G \longrightarrow Gal(k_L | k_K))$

(2) $H \leq G$ Untergruppe zum Zwischenkörper $E = L^H$ (beachte $\mathcal{O}_L = \mathcal{O}_E[x]$)

Dann: $H_i = H \cap G_i$ ($i_{L|E}(\sigma) = i_{L|K}(\sigma)$ für $\sigma \in H$)

z.B. $H = G_0 \Rightarrow L^H = L \cap K^{ur}$ und $G_i = (G_0)_i = H_i \quad \forall i \geq 0$

(3) $i_{L|K}$ ist unabhängig von der Wahl von x (wegen 4.1)

(4) $i_{L|K}: G \longrightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$

Lemma 4.4. Es gilt $G_i \trianglelefteq G \quad \forall i \geq -1$

Beweis.

$$G_i = \ker\left(G \longrightarrow \operatorname{Aut}\left(\mathcal{O}_L / \pi^{i+1}\mathcal{O}_L\right)\right).$$

$\blacksquare$

Korollar 4.5. Seien $\sigma, \tau \in G_0$. Dann gelten:

(i) $i_{L|K}(\sigma\tau\sigma^{-1}) = i_{L|K}(\tau)$

(ii) $i_{L|K}(\sigma\tau) \geq \min\left(i_{L|K}(\sigma), i_{L|K}(\tau)\right)$ mit Gleichheit falls $i_{L|K}(\sigma) \neq i_{L|K}(\tau)$.

Beweis. (i) wegen 4.4.

(ii)
$$\underbrace{v_{L|K}(\sigma\tau x - x)}_{i_{L|K}(\sigma\tau)} \geq \min\Big(\underbrace{v_{L|K}(\sigma(\tau x) - \tau x)}_{\substack{= i_{L|K}(\sigma),\text{ da} \\ \text{auch } \mathcal{O}_L = \mathcal{O}_K[\tau x] \\ \text{nach } 4.3\ (3)}}, \underbrace{v_{L|K}(\tau x - x)}_{i_{L|K}(\tau)}\Big)$$

Gleichheitsaussage wegen "analoger" Eigenschaft von v_L.

$\blacksquare$

Lemma 4.6. Für $\sigma \in G_0$ und $i \geq 0$ gelten:

$$\sigma \in G_i \underset{(i)}{\iff} v_L(\sigma\pi_L - \pi_L) \geq i+1 \underset{(ii)}{\iff} \frac{\sigma\pi_L}{\pi_L} \in U_i(L)$$

Beweis. (i) o.E.: $L|K$ voll verzweigt (ersetze K durch $K^{ur} \cap L$)

dann: klar wegen Wiederholung ANT 1 + 4.3. (3).

(ii) $v_L(\pi_L) = 1 \implies \Big(v_L(\sigma\pi_L - \pi_L) \geq i+1 \iff v_L\left(\frac{\sigma\pi_L}{\pi_L} - 1\right) \geq i$

$$\iff \frac{\sigma\pi_L}{\pi_L} \in U_i(L).$$

$\blacksquare$

1. Anwendung: $v_L(\mathcal{D}_{L|K})$!

$$\mathcal{D}_{L|K}^{-1} = \left\{\alpha \in L \mid Tr_{L|K}(\alpha\beta) \in \mathcal{O}_K \quad \forall \beta \in \mathcal{O}_L\right\}$$

und (Da $\mathcal{O}_L = \mathcal{O}_K[x]$) ist $\mu_x \in \mathcal{O}_K[X]$ das Mipo von x, so gilt $\mathcal{D}_{L|K} = \mu_x'(x)\,\mathcal{O}_L$.

Satz 4.7. $v_L(\underbrace{\mathcal{D}_{L|K}}_{=v_L(\mu_x'(x))}) = \sum_{\sigma \in G \setminus \{id\}} i_{L|K}(\sigma) = \sum_{i=0}^{\infty} (\# G_i - 1)$

(Bem.: weiter unten: $L|K$ zahm verzweigt $\Longleftrightarrow G_1 = \{1\}$
$\Downarrow v_L(\mathcal{D}_{L|K}) = \# G_0 - 1 = e(L|K) - 1$)

Beweis.
$$\mu_x(X) = \prod_{\sigma \in G} (X - \sigma x) \Longrightarrow \mu_x'(x) = \prod_{\sigma \in G \setminus \{1\}} (x - \sigma x)$$

$$\Longrightarrow v_L(\mathcal{D}_{L|K}) = \sum_{\sigma \in G \setminus \{1\}} v_L(x - \sigma x) = \sum_{\sigma \in G \setminus \{1\}} \underbrace{i_{L|K}(\sigma)}_{\in \mathbb{Z}_{\geq 0}}.$$

$$= \sum_{i=0}^{\infty} i \Big(\sum_{\substack{\sigma \in G \setminus \{1\} \\ i_{L|K}(\sigma) = i}} 1 \Big) = \sum_{i=1}^{\infty} i \,(\# G_{i-1} - \underbrace{\# G_i}_{=: g_i})$$

$$\underset{\substack{\text{Abel-}\\\text{summation}}}{=} \sum_{i=0}^{\infty} (\# G_i - 1)$$

$$0 \cdot (g_{-1} - g_0) + 1(g_0 - g_1) + 2(g_1 - g_2) + 3(g_2 - g_3) + \dots + n(g_{n-1} - \underbrace{g_n}_{=1}) + 0$$

$$= g_0 + g_1 + g_2 + \dots + g_{n-1} - n$$

$$= \sum_{k=0}^{n-1} (g_0 - 1)$$

∎

Korollar 4.8. (Ü) Sei $E|K$ endl. separable Erweiterung mit Galoishülle L und $H = \mathrm{Gal}(L/E)$. Dann: $v_{E|K}(\mathcal{D}_{E|K}) = \frac{1}{e(L/E)} \sum_{\sigma \in G \setminus H} i_{L|K}(\sigma)$

Die Gruppen G_i / G_{i+1}:

Lemma 4.9. $\forall i \geq 0$ ist die Abbildung $\theta_i : G_i / G_{i+1} \longrightarrow U_i(L) / U_{i+1}(L)$, $\sigma G_{i+1} \longmapsto \frac{\sigma(\pi_L)}{\pi_L} U_{i+1}(L)$ wohldefiniert, unabhängig von π_L und ein injektiver Gruppenhomomorphismus.

(Erinnerung: $\mathcal{U}_0(L)/\mathcal{U}_1(L) \cong (k_L^\times, \cdot) \cong \mathbb{Z}/(q_L-1)$, $\quad \mathcal{U}_i(L)/\mathcal{U}_{i+1}(L) \cong (k_L,+) \cong \mathbb{F}_p^{[k_L:\mathbb{F}_p]}$)

Beweis. • unabhängig von π_L: Gelte $\pi' = u\pi_L$ für ein $u \in \mathcal{O}_L^\times$.

$$4.1 \underset{\sigma\in G_i}{\Longrightarrow} \sigma u \equiv u \mod \pi_L^{i+1}, \text{ d.h. } \frac{\sigma u}{u} \equiv 1 \mod \pi_L^{i+1}$$

$$\Rightarrow \frac{\sigma\pi'}{\pi'} = \frac{\sigma u}{u}\,\frac{\sigma\pi_L}{\pi_L} \equiv \frac{\sigma\pi_L}{\pi_L} \mod \mathcal{U}_{i+1}(L)$$

• $\tilde{\theta}_i : G_i \longrightarrow \mathcal{U}_i(L)/\mathcal{U}_{i+1}(L)$, $\sigma \longmapsto \frac{\sigma(\pi_L)}{\pi_L} \mod \mathcal{U}_{i+1}(L)$ ist wohldef. Gruppenhomomorph.

$$\frac{\sigma\pi_L}{\pi_L} \underset{4.6}{\in} \mathcal{U}_i(L) \Rightarrow \text{wohldefiniert.}$$

Homomorphismus: $$\tilde{\theta}_i(\sigma\tau) = \frac{\sigma\tau(\pi_L)}{\pi_L} = \frac{\sigma(\tau\pi_L)}{\tau\pi_L}\cdot\frac{\tau(\pi_L)}{\pi_L} \underset{v_L(\tau\pi_L)=1}{\overset{\text{unabh. von } \pi_L}{\equiv}} \frac{\sigma\pi_L}{\pi_L}\cdot\frac{\tau\pi_L}{\pi_L}$$

inj., wohldefiniert:

$$\ker\tilde{\theta}_i = G_{i+1} \text{ nach Lemma 4.6.}$$

∎

Korollar 4.10. (i) G_0/G_1 ist endl. zykl. Grp. von Ordnung teilerfremd zu p.

(ii) G_1 ist eine p-Gruppe

(iii) L^{G_1} ist der max. zahm verzweigte Unterkörper von L über K

(iv) G ist auflösbar. (sogar "überauflösbar")

Beweis. (i), (ii): klar nach 4.9.

(iv): benötigt zusätzlich: $Gal(k_L/k)$ auflösbar ist.

(iii)

$$\begin{tikzcd}[column sep=small] L \arrow[d, dash, "\text{total verzweigt}"] & \\ L^{G_1} \arrow[d, dash] \arrow[dr, dash, "\text{zahm verzweigt, da } p \nmid \# G_0/G_1"] & \\ K \arrow[r, dash, "\text{unverzweigt}"'] & K^{G_0} \end{tikzcd}$$

$\Rightarrow L^{G_1}$ größte zahm verzweigte Untererweiterung von K in L

∎

Ü: $G_0 \simeq G_1 \rtimes G_0/G_1$ (Schur – Zassenhaus, … lieber elementar)

Def. 4.11. $G_1 \trianglelefteq G$ heißt wilde Verzweigungsgruppe von G.

Bsp 4.12. (Ü)
Sei $L_i = \mathbb{Q}_p(\zeta_{p^i}) \quad i \geq 0$

$$\mathrm{Gal}(L_n \mid \mathbb{Q}_p)_i = \begin{cases} G, & -1 \leq i \leq 0 \\ \mathrm{Gal}(L_n / L_k), & p^{k-1} \leq i \leq p^k - 1 \quad k \in \{1, \ldots, n-1\} \\ \{1\}, & i \geq p^{n-1} \end{cases}$$

Bemerkung 4.13 (siehe Serre) $\sigma \in G_i,\ \tau \in G_j,\ i,j \geq 1$

$\Longrightarrow \sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j+1}$

Der Satz von Herbrand.

Für $u \in \mathbb{R}_{\geq -1}$ setze $G_u := G_{\lceil u \rceil}$

$(\sigma \in G_u \Longleftrightarrow i_{L|K}(\sigma) \geq u+1)$

Def. 4.14. (Herbrand Funktion)

$$\phi = \phi_{L|K} : [-1, \infty) \longrightarrow [-1, \infty), \quad t \longmapsto \int_{s=0}^{t} \frac{1}{[G_0 : G_s]}\, ds$$

beachte: $s \longmapsto [G_0 : G_s]^{-1}$ ist monoton ~~wachsend~~ fallend in s und $\frac{1}{[G_0 : G_s]} \geq \frac{1}{\# G_0}$

Prop. 4.15. (Ü)

(i) ϕ ist stetig, stückweise linear (auf $(i, i+1)$) streng monoton wachsend und konkav.

(ii) $\phi(0) = 0$, Steigung 1 auf $-1 \leq t \leq 0$

(iii) Für $u \in \mathbb{R}_{\geq 1} \setminus \mathbb{Z}$: $\phi'(u) = \frac{1}{[G_0 : G_u]} \geq \frac{1}{\# G_0}$

(iv) $\phi : [-1, \infty) \longrightarrow [-1, \infty)$ ist bijektiv.

Sei $\psi = \psi_{L|K} = \phi^{-1} : [-1, \infty) \longrightarrow [-1, \infty)$

Korollar 4.16. (Ü) (i) ψ ist stetig, stückweise linear, streng monoton wachsend, konvex

(ii), (iv) wie für ϕ

(iii) Sei $v = \phi(u)$, $u \notin \mathbb{Z} \Rightarrow \psi'(v) = [G_0 : G_u]$ $(\in \mathbb{N})$ | (v) $u \in \mathbb{Z}_{\geq 1} \Rightarrow u = \psi(v) \in \mathbb{Z}_{\geq 1}$.

Beweis.

(v) OE $v \geq 1$. ($v=0$, $v=-1$ klar wegen ii)

$\exists i: \quad i \leq v \leq i+1$ $\qquad [G_0 : G_u] = \dfrac{\# G_0}{\# G_u}$

$$\underset{v=\phi(u)}{\Longrightarrow} \quad \underbrace{\# G_0 \; v}_{\substack{\text{teile durch} \\ \# G_{i+1}}} = \underset{[0,1]}{\# G_1} + \underset{[1,2]}{\# G_2} + \dots + \underset{[i-1,i)}{\# G_i}$$

$$\underset{v \in \mathbb{Z}}{\Longrightarrow} \quad u - i \in \mathbb{Z} \Rightarrow u = i.$$

$\square$

Def. 4.17. $\quad G^v := G_{\psi(v)}$ (Verzweigungsgruppen in oberer Nummerierung!)

Satz 4.18. (Herbrand) Für $N \trianglelefteq G$ Normalteiler gilt:

$$\left(G/N\right)^v = G^v N / N \qquad \forall v \in \mathbb{R}_{\geq -1}$$

08.05.18

Bem. zu 4.17.

i) $G^v = \{1\}$ für $v \gg 0$

ii) $G^0 = G_0$ $(\psi(0)=0)$; $G^{-1} = G$

iii) Ü: $\psi(v) = \int_{w=0}^{v} [G^0 : G^w] \, dw$

Übung: Die Abbildung $\phi = \phi_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}$ (mit Inverser ψ) erfüllt:

$$\phi'(t) = \begin{cases} 1, & -1 < t < 0 \\ \frac{1}{p^k - p^{k-1}}, & p^{k-1} - 1 < t < p^k - 1 \qquad 1 \leq k \leq n-1 \\ \frac{1}{p^n - p^{n-1}}, & p^{n-1} - 1 < t \end{cases}$$

$$\psi'(t) = \begin{cases} 1, & -1 < t < 0 \\ p^k - p^{k-1}, & k-1 < t < k \qquad 1 \leq k \leq n-1 \\ p^n - p^{n-1}, & n-1 < t \end{cases}$$

(Sprünge der Steigung von ψ an $\{0, \dots, n-1\}$)

Proposition 4.19. Gelte $N \trianglelefteq G$ und sei $E = L^N$. Dann:

$$\varphi_{L|K} = \varphi_{E|K} \circ \varphi_{L|E} \quad \text{und} \quad \psi_{L|K} = \psi_{E|K} \circ \psi_{L|E}$$

Lemma 4.20. Für $N \trianglelefteq G$ und $E = L^N$ gilt:

$$\forall \delta \in \mathrm{Gal}(E|K): \quad i_{E|K}(\delta) = \frac{1}{e(L|E)} \sum_{\substack{\sigma \in G \\ \sigma|_E = \delta}} i_{L|K}(\sigma)$$

$$G\left(\begin{array}{c} L \\ \big| \, N \\ E \\ \big| \, G/N \\ K \end{array}\right.$$

Beweis. (Tate)

- Falls $\delta = \mathrm{id}$: $\infty = \infty$.
- Falls $\delta \neq \mathrm{id}$: Wähle $x \in \mathcal{O}_L$, $y \in \mathcal{O}_E$ mit $\mathcal{O}_K[x] = \mathcal{O}_L$, $\mathcal{O}_K[y] = \mathcal{O}_E$.

Wähle $\tau \in G$ mit $\tau|_E = \delta \Rightarrow \{\sigma \in G \mid \sigma|_E = \delta\} = \tau \cdot N = N \cdot \tau$

Beobachte:

$$e(L|E) \cdot i_{E|K}(\delta) = v_L(\tau y - y)$$

$$i_{L|K}(\sigma) = v_L(\sigma x - x)$$

Behauptung: $a = \tau y - y$ und $b = \prod_{\sigma \in N} (\tau\sigma x - x)$ sind assoziiert in $\mathcal{O}_L$.

<u>$a \mid b$:</u> Sei $f \in E[X]$ das Minimalpolynom von x über E.

$$f(X) = \prod_{\sigma \in N} (X - \sigma x) = X^{\#N} + \sum_{i=0}^{\#N-1} b_i X^i \quad \text{mit } b_i \in \mathcal{O}_E \text{ da } x \text{ ganz über } \mathcal{O}_E.$$

$$\tau f - f = \sum_{i=0}^{\#N-1} \underbrace{(\tau b_i - b_i)}_{v_E(\cdot) \geq i_{E|K}(\delta)} X^i \qquad (\tau b_i = \delta b_i)$$

$$\xrightarrow[\text{Koeffizienten von } f]{a \text{ teilt}} \quad a \mid (\tau f - f)(x) = (\tau f)(x) = \prod_{\sigma \in N} (x - \tau\sigma x) = \pm b$$

<u>$b \mid a$:</u> Schreibe $y = g(x)$ für ein $g \in \mathcal{O}_K[X]$.

$\Rightarrow$ $g(X) - y \in \mathcal{O}_E(X)$ und das Polynom hat x als Nullstelle.

$$\Rightarrow g(X) - y = \underbrace{f(X)}_{\text{normiert}} \cdot h(X) \quad \text{für ein } h \in \mathcal{O}_E[X].$$

Wende τ an; anschließend x einsetzen. (beachte $\tau g = g$)

$$\Rightarrow a = y - \tau y = (\tau f)(x) \quad (\tau h)(x)$$
$$= \pm b \cdot (\tau h)(x)$$

also gilt $b \mid a$.

$\blacksquare$

Korollar 4.21. (s. Serre, Local Fields) Sei $N = G_j$ für ein $j \geq 0$. Dann:

(a) $(G/N)_i = G_i/N$ für $i < j$ (b) $(G/N)_i = \{1\}$ für $i \geq j$

Beweis. Übung.

$\blacksquare$

Lemma 4.22. Für $t \geq -1$ gilt:

$$\phi_{L|K}(t) + 1 = \frac{1}{\# G_0} \sum_{\sigma \in G} \min(i_{L|K}(\sigma), t+1)$$

Beweis. Beide Seiten sind 1 an $t = 0$, $(i_{L|K}(\sigma) = 0$ für $\sigma \in G \setminus G_0$, ≥ 1 für $\sigma \in G_0)$

stückweise linear für $t \in [i, i+1]$ und stetig. Sei $t \in \mathbb{R}_{\geq -1} \setminus \mathbb{Z}$:

$$\phi'_{L|K}(t) = \frac{1}{[G_0 : G_{i+1}]} = \frac{\# G_{i+1}}{\# G_0}$$

$$\left(\begin{smallmatrix}\text{Rechte} \\ \text{Seite}\end{smallmatrix}\right)'(t) = \frac{1}{\# G_0} \sum_{\sigma \in G} \frac{d}{dt} \underbrace{\min\{i_{L|K}(\sigma), t+1\}}_{\text{Fkt. konstant nahe } t \iff i_{L|K}(\sigma) < t+1 \iff i_{L|K}(\sigma) \leq i+1}$$

$$= \frac{1}{\# G_0} \left(\sum_{\sigma \in G \setminus G_{i+1}} 0 + \sum_{\sigma \in G_{i+1}} 1 \right)$$

$\blacksquare$

Lemma 4.23. Für $N \trianglelefteq G$, $E = L^N$, $\delta \in \mathrm{Gal}(E|K)$ und $t \in \mathbb{R}_{\geq -1}$ gilt:

$$i_{E|K}(\delta) - 1 = \max\{\phi_{L|E}(i_{L|K}(\sigma) - 1) \mid \sigma \in G, \sigma|_E = \delta\}$$

Beweis. Wähle $\sigma \in \{\sigma' \in G \mid \sigma'|_E = \delta\}$ für welches $i_{L|K}(\sigma)$ maximal ist. Sei

$m = i_{L|K}(\sigma) - 1$. <u>Behauptung:</u> $\forall \tau \in N: \; i_{L|K}(\sigma\tau) = \min\{i_{L|K}(\tau), m+1\}$

<u>Fall $\tau \in N_m$:</u> d.h. $i_{L|K}(\tau) - 1 \geq m$. $\Rightarrow$ $i_{L|K}(\sigma\tau) \geq \min\{i_{L|K}(\sigma), i_{L|K}(\tau)\}$

$= m+1$ und $=$ nach Wahl von σ.

$= i_{L|K}(\sigma)$

<u>Fall $\tau \in N \setminus N_m$:</u> $i_{L|K}(\tau) \leq m \underset{4.5\,(ii)}{\Longrightarrow} i_{L|K}(\sigma\tau) \underset{\text{wie oben}}{=} i_{L|K}(\tau) \Rightarrow \boxed{} $ Behauptung.

$$4.20 \Rightarrow i_{E|K}(\delta) \underset{\text{Beh.}}{=} \frac{1}{e(L|E)} \sum_{\tau \in N} \min\{i_{L|K}(\tau), m+1\}$$

$\{\sigma' \in G \mid \sigma'|_E = \delta\} = \sigma N$

$$= \frac{1}{\# N_0} \sum_{\tau \in N} \min\{\underline{i_{L|E}(\tau)}, m+1\} \underset{\substack{4.22\\ \text{für } N}}{=} \phi_{L|E}(m) + 1$$

$(\mathcal{O}_K[x] = \mathcal{O}_L \Rightarrow \mathcal{O}_E[x] = \mathcal{O}_L)$

$$= \max\{\phi_{L|E}(i_{L|K}(\sigma) - 1) \mid \sigma \in G, \sigma|_E = \delta\} + 1$$

ϕ konvex $\Rightarrow$ "$\max(\phi) = \phi(\max)$"

$\blacksquare$

Korollar 4.24. (Herbrand's Theorem)

Sei $v = \phi_{L|E}(u)$. Dann: $G_u N/N = \underbrace{(G/N)}_{\cong \mathrm{Gal}(E|K)}{}_v$

Beweis. (Notation wie in 4.23)

$\delta \in G_u N/N \iff \max\{i_{L|K}(\sigma) - 1 \mid \sigma \in G, \sigma|_E = \delta\} \geq u$

$\underset{\substack{4.23,\\ \phi_{L|E} \text{ mon. wachs.}}}{\iff} i_{E|K}(\delta) - 1 \geq \phi_{L|E}(u) = v$

$\iff \delta \in (G/N)_v$

$\blacksquare$

Beweis von 4.19. (Transitivität

(nur für ϕ, da $\psi = \phi^{-1}$ ..) Sei $u \in \mathbb{R}_{\geq -1} \setminus \mathbb{Z}$.

$$\frac{d}{dt}\left(\phi_{E|K} \circ \phi_{L|E}\right)(u) = \phi'_{E|K}(v) \cdot \phi'_{L|E}(u) \qquad v := \phi_{L|E}(u) \notin \mathbb{Z} \ (4.16\ v)$$

$$= \frac{\#\left(\mathrm{Gal}(E|K)_v\right)}{e(E|K)} \cdot \frac{\#\left(\mathrm{Gal}(L|E)_u\right)}{e(L|E)} \underset{4.24}{=} \frac{\# \, G_uN/N \cdot \# \mathrm{Gal}(L|E)_u}{e(L|K)}$$

$$\left(G_uN/N \cong G_u/N \cap G_u \cong G_u/N_u \right) \Rightarrow \quad = \frac{\# \, G_u/\# N_u \cdot \# N_u}{e(L|K)}$$

$$= \phi'_{L|K}(u)$$

∎

Beweis von 4.18. Sei $v \in \mathbb{R}_{\geq -1}$, $x = \psi_{E|K}(v)$, $w = \psi_{L|E}(x) = \psi_{L|K}(v)$

$$(G/N)^v \underset{\text{Def.}}{=} (G/N)_{\psi_{E|K}(v)} = (G/N)_x \underset{\substack{4.24 \\ \phi_{L|E}(w) = x}}{=} G_wN/N = G_{\psi_{L|K}(v)}N/N$$

$$\underset{\text{Def.}}{=} G^vN/N.$$

∎

Satz. (Hasse-Arf, o. Beweis, s. Serre)

Ist $\underset{\mathrm{Gal}(L|K)}{\overset{\|}{G}}$ abelsch, $v \in \mathbb{Q}$ ein Sprung der oberen Verzweigungs Filtrierung, so gilt: $v \in \mathbb{Z}$.

05. Abgeleitete Funktoren (von Modulkategorien)

Sei R ein (nicht-notw. kommutativer) Ring mit 1.

${}_R\underline{\mathrm{Mod}} := R\text{-}\underline{\mathrm{Mod}}$: Kategorie der (Links-) R-Moduln.

Def. 5.1. $Ch^\circ(R)$: Kategorie der (kohomologischen) Komplexe über ${}_R\underline{\mathrm{Mod}}$.

Objekte: $C^\circ = (C^k, d^k)_{k\in\mathbb{Z}}$ so dass $\forall k\in\mathbb{Z}$: $d^k : C^k \to C^{k+1}$ ein Morphismus in ${}_R\underline{\mathrm{Mod}}$ ist und $\forall k\in\mathbb{Z}$: $d^{k+1}\circ d^k = 0$.

Morphismen: $f^\circ = (f^k)_{k\in\mathbb{Z}} : C^\circ = (C^k, d^k)_{k\in\mathbb{Z}} \longrightarrow \overline{C}^\circ = (\overline{C}^k, \overline{d}^k)_{k\in\mathbb{Z}}$ sind $\forall k\in\mathbb{Z}$: Morphismen $f^k : C^k \to \overline{C}^k$ so dass $\overline{d}^i \circ f^i = f^{i+1}\circ d^i$.

Notation: Komplexe

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & C^{i-1} & \xrightarrow{d^{i-1}} & C^i & \xrightarrow{d^i} & C^{i+1} & \longrightarrow \cdots \\
& \downarrow f^{i-1} & \circlearrowleft & \downarrow f^i & \circlearrowleft & \downarrow f^{i+1} & \\
\cdots \longrightarrow & \overline{C}^{i-1} & \xrightarrow{\overline{d}^{i-1}} & \overline{C}^i & \xrightarrow{\overline{d}^i} & \overline{C}^{i+1} & \longrightarrow \cdots
\end{array}$$

Proposition 5.2. $Ch^\circ(R)$ ist eine abelsche Kategorie.

Struktur geg. durch:

Addition auf $\mathrm{Hom}_{Ch^\circ(R)}(-,-)$: $(f^\circ + g^\circ)^i := f^i + g^i$

Null: Nullkomplex $\ldots \to 0 \to 0 \to \ldots \to 0 \to 0 \to \ldots$

Kern: zu $f^\circ : C^\circ \to \overline{C}^\circ$ definiere Komplex $\ker f^\circ := (\ker f^i, d^i|_{\ker f^i})_{i\in\mathbb{Z}}$ als Kern zu f° mit Inklusion nach C.

Cokern: dual.

Bemerkung: Wg. Prop. 5.2. können von Exaktheit von Diagrammen $\overline{C}^\circ \to C^\circ \to \overline{\overline{C}}^\circ$ von Komplexen reden. und von kurzen exakten Sequenzen $0 \to \overline{C}^\circ \to C^\circ \to \overline{\overline{C}}^\circ \to 0$ in $Ch^\circ(R)$.

Def. 5.3. Sei $C^\circ = (C^i, d^i)_{i\in\mathbb{Z}} \in Ch^*(R)$. Definiere

$Z^i := Z^i(C^\circ) := \ker d^i$ (i-Kozykeln) $\quad (B^i \subseteq Z^i$ wg. $d^i\circ d^{i-1} = 0)$

$B^i := B^i(C^\circ) := \mathrm{im}\, d^{i-1}$ (i-Koränder)

$H^i := H^i(C^\circ) := Z^i(C^\circ)/B^i(C^\circ)$ (i-te Kohomologie)

$C^\bullet$ heißt exakt oder azyklisch $:\Longleftrightarrow \forall i \in \mathbb{Z}: \; H^i(C^\bullet) = 0$.

Für $f^\bullet: C^\bullet \to \bar{C}^\bullet$ ein Morphismus in $Ch^\bullet(R)$ gelten:

$$f^i(Z^i(C^\bullet)) \subseteq Z^i(\bar{C}^\bullet), \quad f^i(B^i(C^\bullet)) \subseteq B^i(\bar{C}^\bullet)$$

$\rightsquigarrow$ induzierte Abbildungen $\quad H^i(f^\bullet): H^i(C^\bullet) \longrightarrow H^i(\bar{C}^\bullet)$

Proposition 5.4. $\forall i \in \mathbb{Z}: \; H^i(-): Ch^\bullet(R) \to {}_R\underline{\mathrm{Mod}}$ ist ein Funktor.

Bemerkung: Homologische Komplexe: $Ch_\bullet(R)$

Objekte: $\quad \cdots \; C_1 \xrightarrow{d_1} C_0 \xrightarrow{d_0} C_{-1} \to \cdots$

Z_i, B_i, H_i analog wie oben (z.B. $Z_i = \ker d_i$)

$$Ch^\bullet(R) \xrightarrow{\sim} Ch_\bullet(R): \; (C^i, d^i) \longmapsto (C_i, d_i) \text{ mit } C_i := C^{-i}, \; d_i := d^{-i}$$

Homologie $\qquad Ch_{\leq 0}(R)$

Kohomologie verwendet üblicherweise $Ch^{\geq 0}(R) \subseteq Ch^\bullet(R)$, die Unterkategorie der Komplexe mit $(C^\bullet)^i = 0 \;\; \forall i < 0$.
$(C_\bullet)_i = 0 \;\; \forall i > 0$

<u>Lange exakte Sequenzen.</u> Sei $\mathcal{E}: 0 \to \bar{C}^\bullet \to C^\bullet \to \bar{\bar{C}}^\bullet \to 0$ exakt in $Ch^\bullet(R)$

$$\rightsquigarrow \quad \begin{tikzcd} 0 \arrow[r] & \bar{C}^i \arrow[r] \arrow[d, "\bar{d}^i"] \arrow[dr, phantom, "="] & C^i \arrow[r] \arrow[d, "d^i"] \arrow[dr, phantom, "="] & \bar{\bar{C}}^i \arrow[r] \arrow[d, "\bar{\bar{d}}^i"] & 0 \\ 0 \arrow[r] & \bar{C}^{i+1} \arrow[r] & C^{i+1} \arrow[r] & \bar{\bar{C}}^{i+1} \arrow[r] & 0 \end{tikzcd} \quad \xrightarrow[\text{lemma}]{\text{Schlangen-}} \quad \begin{tikzcd} 0 \arrow[r] & \bar{Z}^i \arrow[r] & Z^i \arrow[r] & \bar{\bar{Z}}^i & \\ & \bar{C}^{i+1}/\bar{B}^{i+1} \arrow[r] & C^{i+1}/B^{i+1} \arrow[r] & \bar{\bar{C}}^{i+1}/\bar{\bar{B}}^{i+1} \arrow[r] & 0 \end{tikzcd}$$

$$\rightsquigarrow \quad \begin{tikzcd} \bar{C}^i/\bar{B}^i \arrow[r] \arrow[d, "\bar{d}^i"] \arrow[dr, phantom, "="] & C^i/B^i \arrow[r] \arrow[d, "d^i"] \arrow[dr, phantom, "="] & \bar{\bar{C}}^i/\bar{\bar{B}}^i \arrow[r] \arrow[d, "\bar{\bar{d}}^i"] & 0 \\ 0 \arrow[r] \; \bar{Z}^{i+1} \arrow[r] & Z^{i+1} \arrow[r] & \bar{\bar{Z}}^{i+1} & \end{tikzcd} \quad \xrightarrow[\text{lemma}]{\text{Schlangen-}} \quad \begin{tikzcd} H^i(\bar{C}^\bullet) \arrow[r] & H^i(C^\bullet) \arrow[r] & H^i(\bar{\bar{C}}^\bullet) \arrow[dll, "\delta^i"'] \\ H^{i+1}(\bar{C}^\bullet) \arrow[r] & H^{i+1}(C^\bullet) \arrow[r] & H^{i+1}(\bar{\bar{C}}^\bullet) \end{tikzcd}$$

Satz 5.5. (a) Erhalten Randabbildungen $\delta^i = \delta^i_{\mathcal{E}}$ zu $\mathcal{E}$ und lange exakte Kohomologiesequenz; hierbei sind $H^i(\bar{C}^\bullet) \to H^i(C^\bullet)$ bzw. $H^i(C^\bullet) \to H^i(\bar{\bar{C}}^\bullet)$ die Abb.'en die durch die Funktoren aus 5.4. gegeben sind.

(b) Morphismen von kurzen exakten Sequenzen

$$\begin{tikzcd} \mathcal{E} \arrow[d] & 0 \arrow[r] & C'^{\bullet} \arrow[r] \arrow[d, "h'^{\bullet}"] & C^{\bullet} \arrow[r] \arrow[d, "h^{\bullet}"] & C''^{\bullet} \arrow[r] \arrow[d, "h''^{\bullet}"] & 0 \\ \mathcal{E}' & 0 \arrow[r] & D'^{\bullet} \arrow[r] & D^{\bullet} \arrow[r] & D''^{\bullet} \arrow[r] & 0 \end{tikzcd}$$

(in $Ch^{\bullet}(R)$) induzieren Morphismen zwischen den sich ergebenden langen ex. Sequenzen.

(genauer:
$$\begin{tikzcd} H^i(C''^{\bullet}) \arrow[r, "\delta^i_{\mathcal{E}}"] \arrow[d] \arrow[dr, phantom, "="] & H^{i+1}(C'^{\bullet}) \arrow[d] \\ H^i(D''^{\bullet}) \arrow[r, "\delta^i_{\mathcal{E}'}"] & H^{i+1}(D'^{\bullet}) \end{tikzcd}$$
)

Homotopie :

Def. 5.6. (a) $f^{\bullet}: C^{\bullet} \to D^{\bullet}$ in $Ch^{\bullet}(R)$ heißt 0-homotop $:\iff$

$\exists$ (0-Homotopie) $(s^i : C^i \to D^{i-1})_{i\in\mathbb{Z}}$ mit s^i Morphismus in ${}_R\underline{Mod}$.

so dass $\forall i \in \mathbb{Z}$: $f^i - 0 = s^{i+1} \circ d^i_{C^{\bullet}} + d^{i-1}_{D^{\bullet}} \circ s^i$

$$\begin{tikzcd} \cdots \arrow[r] & C^i \arrow[r, "d^i_C"] \arrow[dl, "s^i"'] \arrow[d, "f^i"] & C^{i+1} \arrow[r] \arrow[dl, "s^{i+1}"] & \cdots \\ \cdots \arrow[r] D^{i-1} \arrow[r] & D^i \arrow[r] & \cdots \end{tikzcd}$$

(b) $f^{\bullet}, g^{\bullet}: C^{\bullet} \to D^{\bullet}$ in $Ch^{\bullet}(R)$ heißen homotop $\underset{(f\sim g)}{:\iff}$ $f-g$ ist 0-homotop

Satz 5.7. (a) $\sim$ ist eine Äquivalenzrelation auf $\mathrm{Hom}_{Ch^{\bullet}(R)}(-,-)$

(b) $f^{\bullet} \sim g^{\bullet} \Rightarrow H^i(f^{\bullet}) = H^i(g^{\bullet}) \quad \forall i \in \mathbb{Z}$

(c) $id_{C^{\bullet}} \sim 0 \Rightarrow C^{\bullet}$ ist azyklisch.

Bemerkung. "Man" definiert $K^{\bullet}(R)$ als $Ch^{\bullet}(R)/_{\sim}$ (Objekte dieselben, auf den Morphismen bildet man Äquivalenzklassen)

$K^{\bullet}(R)$ ist selten eine abelsche Kategorie (aber immer eine triangulierte Kategorie)

(abelsche Kategorie $\underset{??}{\iff}$ alle Objekte in ${}_R\underline{Mod}$ sind injektiv)

Auflösungen: Wdh. I injektiv $:\Longleftrightarrow$ $\mathrm{Hom}_R(-, I)$ exakter Funktor

P projektiv $:\Longleftrightarrow$ $\mathrm{Hom}_R(P, -)$ exakter Funktor

Sei R eine A-Algebra (A kommutativ!)

$F \in {}_R\mathrm{Mod}$ ist A-flach $:\Longleftrightarrow$ $F \otimes_A -$ ist exakter Funktor

Proposition. (a) ${}_R\mathrm{Mod}$ besitzt genügend injektive und genügend projektive

(b) Ist R A-flach, so besitzt ${}_R\mathrm{Mod}$ genügend viele A-flache

(alle proj. R-Moduln sind A-flach)

Bemerkung: Grothendieck-Kategorien besitzen genügend viele Injektive.

Def. 5.8. (a) Ein Komplex $I^\bullet \in Ch^{\geq 0}(R)$ zusammen mit einer Abbildung $\varepsilon : M \longrightarrow I^0$ ($M \in {}_R\mathrm{Mod}$) heißt injektive Auflösung von M $:\Longleftrightarrow$ alle I^i sind injektiv und $\underset{-1}{0} \to \underset{}{M} \xrightarrow{\varepsilon} \underset{0}{I^0} \xrightarrow{d^0} \underset{1}{I^1} \to \dots$ ist exakt.

(b) Sei $M \in {}_R\mathrm{Mod}$. Ein Komplex $P^\bullet \in Ch^{\leq 0}(R)$ zusammen mit einer Abbildung $\varepsilon : P^0 \longrightarrow M$ heißt projektive Auflösung $:\Longleftrightarrow$ alle P^i sind projektiv und

$$\dots \longrightarrow P^{-1} \xrightarrow{d^{-1}} P^0 \longrightarrow M \longrightarrow 0 \quad \text{ist exakt.}$$

Notation: $P^\bullet \xrightarrow{\varepsilon} M$, $\quad M \xrightarrow{\varepsilon} I^\bullet$

Satz 5.9. (a) Jedes Objekt in ${}_R\mathrm{Mod}$ besitzt eine injektive Auflösung.

(b) zu $M \xrightarrow{\varphi} M'$ ein Morphismus in ${}_R\mathrm{Mod}$ $\exists$ inj. Auflösungen $M \to I^\bullet$, $M' \to I'^\bullet$ und eine Abbildung von Komplexen $\psi : I^\bullet \to I'^\bullet$ so dass

$$\begin{array}{ccc} M & \longrightarrow & I^0 \\ \downarrow \varphi & /\!/ & \downarrow \psi^0 \\ M' & \longrightarrow & I'^0 \end{array}$$

(c) Die Abbildung $\psi : I^\bullet \to I'^\bullet$ (zu jeg. $\varphi : M \to M'$, zu jeg. $I^\bullet, I'^\bullet$) ist eindeutig bis auf Homotopie.

(d) Es gelten analoge (duale) Aussagen für projektive Auflösungen

Derivierte Funktoren.

Sei $F : {}_R\underline{Mod} \longrightarrow \underline{Ab}$ ein additiver Funktor, (d.h. die Abbildungen

$$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_{\underline{Ab}}(FM, FN) \quad \text{sind } \mathbb{Z}\text{-linear} \quad \forall M,N \in {}_R\underline{Mod})$$
$$\varphi \longmapsto F\varphi$$

- F induziert additiver Funktor $Ch^{\cdot}(R) \longrightarrow Ch^{\cdot}(\mathbb{Z})$

$$(C^i, d^i)_{i\in\mathbb{Z}} \longmapsto (FC^i, Fd^i)_{i\in\mathbb{Z}}$$

Def. 5.10. (a) Sei $P^{\cdot} \xrightarrow{\varepsilon} M$ eine projektive Auflösung und für $\varphi : M \to M'$ in ${}_R\underline{Mod}$ sei $\psi : P^{\cdot} \longrightarrow P^{\cdot\prime}$ Abbildung projektiver Auflösungen wie in 5.9.

Dann definiere $(L_iF)(M) := H^{-i}(FP^{\cdot}) \quad \forall i \geq 0$

$$(L_iF)(\varphi) : (L_iF)(M) \longrightarrow (L_iF)(N) = H^{-i}(FP^{\cdot} \xrightarrow{F\psi^{\cdot}} FP^{\cdot\prime})$$

(b) Sei $M \xrightarrow{\varepsilon} I^{\cdot}$ eine injektive Auflösung, und zu $M \xrightarrow{\varphi} M'$ sei $I^{\cdot} \xrightarrow{\psi} I^{\cdot\prime}$ Abb. von Auflösungen. Definiere

$$(R^iF)(M) := H^i(FI^{\cdot}) \quad \text{und} \quad (R^iF)(\varphi) := H^i(FI^{\cdot} \xrightarrow{F\psi^{\cdot}} FI^{\cdot\prime})$$

Proposition 5.11. $\forall i \geq 0$ erhält man Funktoren $R^iF, L_iF : {}_R\underline{Mod} \longrightarrow \underline{Ab}$

Idee: (a) wähle $\forall M \in {}_R\underline{Mod}$ projektive Auflösung $P_M^{\cdot} \xrightarrow{\varepsilon_M} M$

und $\forall \varphi$ Morphismen von Moduln

$$\begin{tikzcd} P_M^{\cdot} \arrow[r] \arrow[d] \arrow[dd, bend right] & M \arrow[d] \\ P_{M'}^{\cdot} \arrow[r] \arrow[d] & M' \arrow[d] \\ P_{M''}^{\cdot} \arrow[r] & M'' \end{tikzcd}$$

Wissen: $\downarrow\downarrow$ und (sind homotop

$\underset{5.9}{\Longrightarrow}$ induz. Abb'en $(L_iF)(M) \longrightarrow (L_iF)(M')$ sind dieselben.

=

Horseshoe Lemma. Ist $0 \to M' \to M \to M'' \to 0$ exakte Sequenz in ${}_R\underline{Mod}$, so existiert eine kurze exakte Sequenz von proj. Auflösungen

$$\begin{tikzcd} 0 \arrow[r] & P^{\cdot\prime} \arrow[r] \arrow[d, "\varepsilon'"] \arrow[dr, phantom, "\equiv"] & P^{\cdot} \arrow[r] \arrow[d, "\varepsilon"] \arrow[dr, phantom, "\equiv"] & P^{\cdot\prime\prime} \arrow[r] \arrow[d, "\varepsilon''"] & 0 \\ 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0 \end{tikzcd}$$

und von injektiven Auflösungen

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d, "\varepsilon'"] \arrow[dr, phantom, "\equiv"] & M \arrow[r] \arrow[d, "\varepsilon"] \arrow[dr, phantom, "\equiv"] & M'' \arrow[r] \arrow[d, "\varepsilon''"] & 0 \\ 0 \arrow[r] & I^{\cdot\prime} \arrow[r] & I^{\cdot} \arrow[r] & I^{\cdot\prime\prime} \arrow[r] & 0 \end{tikzcd}$$

Bemerkung. Beweis ist ein Induktionsargument. In jedem Schritt (z.B. projektiv)

$$\begin{tikzcd}
0 \arrow[r] & P^{\circ\prime} \arrow[r] \arrow[d, "\alpha'"', "\text{surj.}"] & P^{\circ} \arrow[r] \arrow[d, dashed, "\alpha'\oplus\hat{\alpha}"'] & P^{\circ\prime\prime} \arrow[r] \arrow[d, "\alpha''", "\text{surj.}"'] \arrow[dl, dashed, "\exists\hat{\alpha}"] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

Hufeisen

Bemerkung. $\forall i$: $0 \to P^{-i\prime} \to P^{-i} \to P^{-i\prime\prime} \to 0$ spaltet

$\Rightarrow F(\quad \text{—} \;\text{"}\; \text{—} \quad)$ spaltet, ist also exakt!

$\Rightarrow \quad 0 \to FP^{-i\prime} \to FP^{-i} \to FP^{-i\prime\prime} \to 0$ exakt!!

Satz 5.12. Erhalten lange exakte Kohomologiesequenzen

z.B. $0 \to R^0FM' \to R^0FM \to R^0FM'' \to R^1FM' \to R^1FM \to \dots$

(lange exakte Kohomologiesequenz zu $0 \to FI^{\circ\prime} \to FI^{\circ} \to FI^{\circ\prime\prime} \to 0$)

F heißt rechtsexakt (kovariant) $:\Leftrightarrow$ $\forall$ rechts ex. Sequenzen $M' \to M \to M'' \to 0$ ist $FM' \to FM \to FM'' \to 0$ rechtsexakt.

(analog linksexakt)

Lemma 5.13. (a) F rechtsexakt $\Rightarrow$ $L_0F(M) = M$ (kanonisch)

und $(L_iF)(P) = 0 \quad \forall i > 0$ falls P projektiv

(b) die duale Aussage für F linksexakt; $R^0F(M)$ und für Injektive.

Beweis. (a) Proj. Auflösung $\quad \dots \to P^{-1} \to P^0 \xrightarrow{\varepsilon} M \to 0$ (rechtsexakt)

$\xrightarrow[F \text{ rechtsexakt}]{} \quad \dots \to FP^{-1} \to FP^0 \to FM \to 0$

$$\Rightarrow H^0(FP) = \frac{FP^0}{Fd^{-1}(FP^{-1})} \underset{\text{via } \varepsilon}{\overset{\text{kanonisch}}{=}} FM.$$

(i) Ist P projektiv, so ist $\underset{-3}{0} \to \underset{-2}{0} \to \underset{-1}{0} \to \underset{0}{P} \xrightarrow{\mathrm{id}} \underset{1}{P}$ projektive Auflösung.

☐