Üb. AZ 1 26.10.15 ①

P-adische Zahlen

$a_i \in \{0, \dots, p-1\}$, $p \in \mathbb{Z}$ feste Primzahl $\rightsquigarrow$ $\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i\}$ formale Reihen

Addition, Multipl. wie bei form. Reihen, aber man muß die Koeff. dann neu ersetzen. z.B. $p=3$, $(2\cdot 3)^2 = 4\,3^2 = (1\cdot 3+1)3^2 = 3^2+3^3$.

$\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}] = \{\sum_{i \geq -\infty} a_i p^i\}$. Dabei: algebr. Konstr. via

Inverser (projektiver) Limes.

$\mathcal{C}$ Kategorie (z.B. ab. Gruppen), $(X_i)_{i \in I}$ System von Obj in $\mathcal{C}$, $f_{ij}: X_i \to X_j$ für $i \geq j$ (allg.: ~~index~~ part. geord. Menge I).

$\varprojlim X_i$ erfüllt UAE:

$\varprojlim X_i$
$\downarrow p_i$
X_i

$$\begin{tikzcd} & & X_i \arrow[d, "f_{ij}"] \\ Y \arrow[r, dashed, "\exists!"] \arrow[urr, bend left] \arrow[drr, bend right] & \varprojlim X_i \arrow[ur, "p_i"] \arrow[r, "p_j"'] & X_j \end{tikzcd}$$

Bsp. $\mathcal{C} = \mathcal{S}et$, so ex. $\varprojlim X_i \subseteq \prod X_i$, $\varprojlim X_i = \{(x_1, x_2, \dots) \mid f_{ij}(x_i) = x_j\}$

i) z.B. X Menge, $\{X_i\} \subseteq \mathcal{P}(X)$ mit $X_{i+1} \underset{f_{i+1,i}}{\subseteq} X_i \subseteq X \Rightarrow \varprojlim X_i = \bigcap X_i$.

ii) $X_i = X$, $f_{ij} = id \rightsquigarrow \varprojlim X_i = X$

iii) $\mathbb{Z}/p^m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ nat. Proj. $\rightsquigarrow$ $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$ Hier leicht zu sehen, $\mathbb{Z}_p$ Ring!

$(x \bmod p^i) \leftrightarrow \sum a_i p^i = x$

iv) $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Satz 3 sagt uns: $F(x_1, \dots, x_n)$ hat Lsg in $\mathbb{Z}_p \Leftrightarrow F(x_1, \dots, x_n)$ hat Lsg in $\mathbb{Z}/p^n\mathbb{Z}$ $\forall n$

$\quad\ \ \in \mathbb{Z}[x_1, \dots, x_n]$

~~Für $\mathbb{Z}$ kl~~

Zeigen was ähnliches: $x, a \in \mathbb{Z}_p$: ~~(sonst $a = p^k a'$)~~, $p \nmid a'$ Lsg von $X^2 = a$ in $\mathbb{Z}_p$?

$\underline{p > 2}$: $\Leftrightarrow x^2 \equiv a'$ mod p, k gerade. Bew: $x = \sum_{i \geq 0} x_i p^i$, $x_0^2 \equiv a$ (p).

zuerst mit $a \not\equiv 0$ (p)

$(x_0 + x_1 p)^2 \equiv a \quad (p^2)$

$\equiv x_0^2 + 2x_0x_1p + \cancel{x_1^2p^2} \equiv a \Leftrightarrow x_1 p \equiv \frac{a - x_0^2}{2x_0} \quad (p^2)$,

aber $p \mid a - x_0^2 = p \cdot x_1' \rightsquigarrow \exists!\, x_1 \in \{0, \dots, p-1\}$: $x_1 p \equiv \frac{p x_1'}{2x_0}$

Allg. Ang. $x^2 \equiv a\ (p^n) \rightsquigarrow (x + x_n p^n)^2 \equiv x^2 + 2x x_n p^n + x_n p^{2n} \overset{!}{\equiv} a \quad (p^{n+1})$

$\Leftrightarrow x_n p^n \equiv \frac{a - x^2}{2x} \quad (p^{n+1})$

$\underline{p=2}$: $x, a \in \mathbb{Z}_2$, $2 \nmid a$, $a = \cancel{2^k}(1 + a_1 2 + a_2 2^2 + \dots)$, $x^2 \equiv a$ $(2) \Leftrightarrow$ (~~k gerade~~), $a_1 = a_2 = 0$.

Bew. $x^2 \equiv 1$ (2), $x = \sum x_i 2^i$, so $x^2 \equiv 1$ (8): $x^2 \equiv (x_0 + x_1 2 + x_2 2^2)^2 =$

$\equiv a$

$x_0^2 + x_0x_1 2 + x_0x_2 2^2 + \cancel{x_0 x_1 2} + x_1 2^2 + \cancel{x_1 x_2 2^3} + x_0 x_2 2^2 \equiv x_0^2 + \cancel{x_0 x_1} 2^2 + x_1 2^2 + \cancel{x_2 2^3}$

$x_0 = 1$. Falls $x_1 = 0 \rightsquigarrow x^2 \equiv 1$ (8), $x_1 = 1 \rightsquigarrow x^2 \equiv 1$ (8). $\rightsquigarrow a_1 = a_2 = 0$.

Analoge Konstr. wie oben liefert das Ziel: $x_0 = 1$, $x_1 = 0$. $\rightsquigarrow x' = x_0 + 2 \cdot x_1 \equiv a$ (8)

$(x' + x_2 \cdot 2^2)^2 = x' + x' x_2 2^3 + x_2 2^4 \equiv x' + x' x_2 2^3 \overset{!}{\equiv} a \ (2^4)$, $2^3 \mid a - x'$, $\Leftrightarrow x_2 2^3 \equiv \frac{a - x'}{x'} \ (2^4)$

$\rightsquigarrow x_2$ festgelegt. $\rightsquigarrow x^2 \equiv a$ hat Lsg. in $\mathbb{Z}_2$

Bewertungen. $\|\cdot\|: k \to \mathbb{R}_{\geq 0}$ Absolutbetrag: $\|x\| = 0 \iff x = 0$.

$\|xy\| = \|x\|\cdot\|y\|$, $\|x+y\| \leq \|x\| + \|y\|$. (ultrametrisch: $\|x+y\| \leq \max\{\|x\|, \|y\|\}$.)

Exp. Bew.: $v: k \to \mathbb{R}\cup\{\infty\}$ Expbew.: $v(x) = \infty \iff x = 0$,

$v(xy) = v(x) + v(y)$, $v(x+y) \geq \min\{v(x), v(y)\}$.

Bsp: $\mathbb{Q} = k$, $v = v_p$: $x \in \mathbb{Q}$, $x = p^k \cdot \frac{a}{b}$, $a,b \in \mathbb{Z}$, $k \in \mathbb{Z}$, $p \nmid a,b$ ⇝

$v_p(x) = k$. ist ultrametr. Expbew. ⇝ $\|x\| = \frac{1}{p^{v_p(x)}}$ nichtarch. Betrag.

(man kann $\alpha \in \mathbb{R}: 0<\alpha<1$ bel. wählen).

Werden diese Woche sehen: v_p setzt sich eindeutig auf $\mathbb{Q}_p$ fort!

$x = \sum_{k \geq -\infty} p^k x_k$, so $v_p(x) = -n$, falls $x = p^n \cdot x'$, $x' \in \mathbb{Z}_p^\times$.
$= \sum_{k\geq 0} a_k p^k$, $a_0 \neq 0$.

Damit. $p > 2$: $a \in \mathbb{Z}_p$, $a = p^k a'$, $x^2 = a \iff k$ gerade, $a' \equiv x'^2\ (p)$ für ein $x' \in \{0,\dots,p-1\}$.

„⇒“: $x^2 = p^k a'$, $x = p^n \cdot x'$, $v(x) = n$, da $v(x') = 0$ ($x \in \mathbb{Z}_p^\times \iff v(x) = 0$,

⇝ $p^{2n} x'^2 = p^k a'$, $k = 2n$ gerade $\overset{\cdot p^{-k}}{\Rightarrow}$ $x'^2 = a'$ siehe vorher. $v(x\cdot y) = v(1) = 0 = \underbrace{v(x)}_{\geq 0} + \underbrace{v(y)}_{\geq 0}$.)

„⇐“: von vorher.

$p = 2$: $a \in \mathbb{Z}_2$, $a = 2^k a'$, $a' \in \mathbb{Z}_2^\times$. $x^2 = a \iff k$ gerade, $a_1, a_2 = 0$.

Benutze dies, um $\mathbb{Q}_p \not\cong \mathbb{Q}_q$ z.z., $q \neq p$. (+ Chin. Restsatz).

Weitere Eigenschaften. • $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ unendlich-dim. (nachher: $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ ist Erw. vom Grad $\varphi(p^n)$) (*)

aber $\mathbb{C}/\mathbb{R}$ über $\mathbb{R}$ 2-dim ⇝ $\mathbb{R} \not\cong \mathbb{Q}_p$

• $\sigma: \mathbb{Q}_p \to \mathbb{Q}_p$ ~~stetig~~ Autom., so σ stetig (Bew. später (#)). Damit $\sigma = \mathrm{id}$

da $x \in \mathbb{Q}_p$, $x = \lim x_n$ ⇝ $\sigma(\lim x_n) = \lim \sigma(x_n) = \lim x_n = x$, da $\sigma|_{\mathbb{Q}} = \mathrm{id}$.

• $\sigma: \mathbb{R} \to \mathbb{R}$ Autom., so $\sigma = \mathrm{id}$. (Bew?) $x > 0$, so $x = y^2$, $\sigma(x) = \sigma(y)^2 > 0$,

analog $\sigma(x) < 0$ für $x < 0$. $x > y$ ⇝ $\sigma(x) - \sigma(y) = \sigma(x-y) > 0$ ⇝ $\sigma(x) > \sigma(y)$

$\sigma|_{\mathbb{Q}} = \mathrm{id}$, $x \in \mathbb{R}$, $u < x < v$, $u, v \in \mathbb{Q}$ ⇝ $u < \sigma(x) < v$, u,v bel.

⇝ $\sigma(x) = x$.

• $d(x,y) = \|x-y\|$ def. Metrik auf k ($d(x,y) = 0 \iff x = y$, $d(x,y) = d(y,x)$, Δ-Ugl.)

Topologie lässt sich am einfachsten durch Umgebungsbasen definieren. $k = \mathbb{Q}_p$, $\|\cdot\|$ durch v_p $= \|\cdot\|_p$.

offene Kugeln um 0: $d(x,0) < r \iff \|x\| < r$, so $\{x \in \mathbb{Q}_p \mid d(x,0) < r\} = p^n\mathbb{Z}_p$,

für $p^{-n} < r$ kleinstes n, da $\|\mathbb{Z}_p^\times\| = \{1\}$. Analog $\{x \mid d(x,y) < r\}$ ist Umgebung von

y, $\|x-y\| < r \iff x - y \in p^n\mathbb{Z}_p \iff x \in y + p^n\mathbb{Z}_p$.

(*) d: $\exists\, K/\mathbb{Q}_p$: $[K:\mathbb{Q}_p] = d$. $\mathbb{F}_{p^d}/\mathbb{F}_p$ ex. $\forall d$ (Erw. durch $X^{p^d} - X$) ⇝ $\mathbb{F}_{p^d} = \mathbb{F}_p(\alpha)$, $\bar f \in \mathbb{F}_p[X]$ Mipo ⇝ irred., $\partial f = d$

$f \in \mathbb{Z}_p[X]$ mit $f \equiv \bar f\ (p)$ ⇝ f irred in $\mathbb{Z}_p[X]$ ⇝ f irred in $\mathbb{Q}_p[X]$ (Gauß) ⇝ erhält Erw. vom Grad d.

Af 1 2. Übung 2.11.15

$(K, |\cdot|)$ bew. Kp $\leadsto$ $(\hat{K}, |\cdot|)$ Vervollst. ex. und ist bis auf eind. Isom. eind.: $\hat{K} = R/m$, R CF in K, m NF, $a \mapsto (a, a, \dots)$
$|(a_n)| = \lim |a_n|$ ex. $\quad i: K \to \hat{K}$,

Vollständigkeit von $\hat{K}$: Sei $(\xi_n) \subseteq \hat{K}$ CF. $\forall n \in \mathbb{N}: |\xi_n - i(x_n)| < \frac{1}{n}$, $x_n \in K$.
Sei $\varepsilon > 0 \leadsto N \gg 0$: $\frac{1}{p} < \varepsilon/3$, $\frac{1}{q} < \frac{\varepsilon}{3}$, $|\xi_p - \xi_q| < \varepsilon/3 \leadsto |x_p - x_q| \leq$
$|i(x_p) - \xi_p| + |\xi_p - \xi_q| + |\xi_q - i(x_q)| < \varepsilon$. $\leadsto \xi = (x_n)$ ist CF in K $\leadsto$
$\lim i(x_n) = \xi$ in $\hat{K}$. Also $|\xi_n - \xi| < |\xi_n - i(x_n)| + |i(x_n) - \xi| < \varepsilon$ für $n \gg 0$
$\leadsto \lim \xi_n = \xi$.

Meistens $|\,|$ jetzt nicht-archim. $\leadsto v = -\log|\,|$ Exp. bew. $v: K \to \mathbb{R} \cup \{\infty\}$.
$v(K^\times) \not\subseteq \mathbb{R}$ diskret, so v diskret: $M \subseteq \mathbb{R}$ heißt diskret $:\Leftrightarrow \{x\} \subset M$ ist offen. $\Leftrightarrow \forall x \in M\, \exists \varepsilon > 0: B_\varepsilon(x) \cap M = \{x\}$, $B_\varepsilon(x) = \{y \in M \mid |y - x| < \varepsilon\}$.:
„$\Rightarrow$" $\{x\} \subseteq M$ offen $\Leftrightarrow \{x\} = B_\varepsilon(x) \cap M$ f. ein ε nach Def der Unterraum-top.

Bsp $\frac{1}{m}\mathbb{Z} \subseteq \mathbb{R}$ diskret., $\mathbb{Q} \subseteq \mathbb{R}$ aber nicht.
Da $v: K^\times \to \mathbb{R}$ Gruppenhom. ist $v(K^\times)$ diskrete UG, falls v diskret,
Beh. $v(K^\times) = \alpha\mathbb{Z}$. Wähle $x \in v(K^\times)$ mit $v(x) \overset{=\alpha}{>} 0$ minimal (nicht-triv)
ex., da sonst Folge $v(x_n) \searrow 0 \leadsto \forall \varepsilon > 0$ $B_\varepsilon(0) \cap v(K^\times)$ trifft ein x_n.
$\leadsto \langle x \rangle \subseteq v(K^\times) \ni y$, falls $y \notin \langle x \rangle$ so ex. n, $0 \leq v(y \cdot x^n) = v(y) + n v(x) < v(x)$
Also $v(K^\times) = \alpha\mathbb{Z}$. $\quad$ ↯

Triviale Bew. $v: K^\times \to \mathbb{R}$, $x \mapsto 0$, $0 \mapsto \infty$ Beh. K hat diskrete Top.:
i) $B_\varepsilon(0) = \{y \in K \mid |y| < \varepsilon\} = \{0\}$ für $\varepsilon < 1$ erfüllt.
ii) $B_\varepsilon(x) = \{y \in K \mid \overset{v(y) > 0}{|y - x| < \varepsilon}\}$ $y - x \in B_\varepsilon(0) \Leftrightarrow y \in x + \overset{\{0\}}{B_\varepsilon(0)}$
$= \{x\}$ für $\varepsilon < 1$

$\leadsto$ Langweilig!

K endl. Kp, so jede Bew. $v: K^\times \to \mathbb{R}$ ist trivial, $v(K^\times) \subseteq (\mathbb{R}, +)$ endl. UG
$\leadsto v(K^\times) = \{0\}$ (sonst $\alpha = v(x) \neq 0$ für ein $x \neq 0$, $\leadsto n\alpha \in v(K^\times)$, aber
$v(x^k) = v(1) = 0 \overset{!}{=} k \cdot \alpha (\neq 0$ ↯ $)$.

(K, v) bew. Kp. Dann: v diskret $\Leftrightarrow m = \{x \in K \mid v(x) > 0\} = (\pi) \Leftrightarrow$
$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ HIR $\Leftrightarrow \mathcal{O}_v$ noethersch

Einzige Richtung, die wir noch nicht gesehen haben: $\mathcal{O}$ noethersch $\Rightarrow$
$m = (\pi)$. Sei $m = (x_1, \dots, x_n)$ mit $v(x_1) \leq \dots \leq v(x_n) \leadsto m = (x_1)$.
da $v(x_i \cdot x_1^{-1}) = v(x_i) - v(x_1) \geq 0 \leadsto x_i = x_1 \cdot \alpha$, $\alpha \in \mathcal{O}$.

• Sei nun (K,v) alg. abg. ⇝ $K^\times$ divisibel: $\forall y \in K^\times, n \in \mathbb{N}\ \exists x \in K^\times$: $y = x^n$ ⇝ $v(K^\times) \subseteq \mathbb{R}$ divisibel. Ang. v ist nicht-trivial, $v(y) \neq 0$

~~Sei $G \leq (\mathbb{R},+)$ diskret~~ ⇝ $v(y) = v(x^n) = n\, v(x)$ ⇝ $\frac{1}{n} v(y) = v(x)$ ex.

$\forall n$. $\frac{1}{n} v(y) \to 0$ ⇝ $v(K^\times)$ nicht diskret.

• Bewertungsring. R Integritätsbereich mit $K = \mathrm{Quot}(R)$. Gilt $x \in R$ oder $x^{-1} \in R$ für $x \in K$, so heißt R Bewertungsring. Klar: Ist (K,v) nicht-archim. bew. Körper, so $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ Bew.ring. Umgekehrt: R Bewertungsring, so setze $\Gamma = K^\times/R^\times$, $v: K^\times \to \Gamma$ kan. Abb. und versehe Γ mit der totalgeordn. Struktur, s.d. $v(R \setminus \{0\}) \geq 0_\Gamma = \bar{1}$ ⇝ (K,v) Bew. Körper mit Bewertungsring $\mathcal{O}$. $\quad x,y \in K^\times \quad \bar{x} \geq \bar{y} :\Leftrightarrow x \cdot y^{-1} \in R$

Bewertungsring ist ganzabg.: $x \in K$ ganz über $\mathcal{O}$, d.h. $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, $a_i \in \mathcal{O}$, so, falls $x^{-1} \in \mathcal{O}$, $x \notin \mathcal{O}$ ⇝ $x = -a_{n-1} - \dots - a_0 (x^{-1})^{n-1} \in \mathcal{O}$ ↯

• Wissen: $\mathbb{Q} \subseteq \mathbb{Q}_p$ dicht. Algebraisch? Cantors Diagonalargument: bzgl. $|\cdot|_p$

Ang. $\mathbb{Z}_p$ abzählbar, also
$$s_1 = (a_{00}, a_{01}, \dots) \qquad a_{ij} \in \{0,\dots,p-1\}$$
$$s_2 = (a_{10}, a_{11}, \dots)$$

⇝ $x_n = (b_0, b_1, b_2, \dots) \in \mathbb{Z}_p$ mit $b_0 \neq a_{00}$, $b_1 \neq a_{11}$, $b_2 \neq a_{22}$, … ⇝ $x_n \neq s_n\ \forall n$ ⇝ $\mathbb{Z}_p$ nicht abzählbar ⇝ $\mathbb{Q}_p$ transzendent über $\mathbb{Q}$ (alg. Erw. sind abzählbar: zähle die Polynome ab).

• perfekte/vollkommene Körper der Char $p > 0$: k perfekt (d.h. jede endl. Erw. ist sep ⇔ jedes irred Polynom ist sep.) ⇔ Frobenius $x \mapsto x^p$ ist surjektiv/bijektiv.

„⇒": Sei $\alpha \in k$, $X^p - \alpha$, und α habe kein p-te Wurzel in k ⇝ $\beta^p = \alpha$ in $\bar{k}$, $(X-\beta)^p = X^p - \beta^p = X^p - \alpha \in k[X]$ ⇝ $\mathrm{MiPo}_k \alpha \in k[X]$ hat mehrfache Nst, ↯ zu separabel.

„⇐": Sei Frob. surj., $f \in k[X]$ irred. nicht sep. ⇒ $\exists g$ irred, sep. $r \in \mathbb{N}$: $f(X) = g(X^{p^r}) = g(X)^{p^r}$ da die Koeff p^r-te Wurzeln in k haben ⇝ f nicht irred, ↯.

Bsp. i) $k = \mathbb{F}_p(t)$ nicht perfekt, da $x \mapsto x^p$ nicht surjektiv (t wird nicht getroffen)

ii) $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$ und wir betrachten den Ring $\mathcal{O}_{\bar{\mathbb{Q}}_p}/p\mathcal{O}_{\bar{\mathbb{Q}}_p}$, wobei wir annehmen, dass $\bar{v}$ Fortsetzung von v auf $\bar{\mathbb{Q}}_p$ mit $\bar{v}|_{\mathbb{Q}_p} = v$. ⇝ $\bar{v}$ nicht diskret.

Sei $\underbrace{\sqrt{p}}_{x}, \underbrace{\sqrt[3]{p}}_{y} \in \bar{\mathbb{Q}}_p$ ⇝ $v(x) = \frac{1}{2} v(p) = \frac{1}{2}$, $v(y) = \frac{1}{3}$ ⇝ $x^p - y^p = (x-y)^p$ in $\mathcal{O}_{\bar{\mathbb{Q}}_p}/p\mathcal{O}_{\bar{\mathbb{Q}}_p}$, also $\bar{v}(x^p - y^p) = p\,\bar{v}(x-y) \geq p \cdot \frac{1}{3} \geq 1$ ⇝ $\bar{x}^p = \bar{y}^p$ in $\mathcal{O}_{\bar{\mathbb{Q}}_p}/p\mathcal{O}_{\bar{\mathbb{Q}}_p}$, aber $x \neq y$.
$(p > 3)$

Ak 1 9.11.15 ÜS

K top. K vollst. diskret bew. (mit nicht-triv. Bew. v oder $|\ |$) mit endl. Restklassenkp., so heißt K lokaler Kp. (später)

K endl. Erw. von $\mathbb{Q}_p$ oder $\mathbb{F}_p((t))$ mit p-adischer bzw. t-adischer Bew.

Bsp: $\mathbb{Q}_p$ $v: |\ | = |\ |_p$, vollst, nicht-triv, $\kappa = \mathbb{Z}/p\mathbb{Z}$.

ii) $\mathbb{Z}[i]$ Gaußsche ganze Zahlen, ist Euklidischer Ring via $N: \mathbb{Z}[i] \to \mathbb{Z}$, $x \mapsto N(x)$

$\leadsto$ HIR. Wissen: $p \in \mathbb{Z}$ prim ist prim in $\mathbb{Z}[i] \iff p \equiv 3\ (4)$.

Bew $\kappa = \mathbb{Z}[i]/(3) \cong \mathbb{F}_{3^2} = \mathbb{F}_9$, denn: $\kappa/\mathbb{F}_3$ wegen $\mathbb{Z}/(3) \hookrightarrow \mathbb{Z}[i]/(3)$

$\mathrm{rk}_{\mathbb{Z}}\, \mathbb{Z}[i] = 2$, d.h. $\mathrm{rk}_{\mathbb{Z}/3}\, \kappa \leq 2$; ist $1, i$ Basis in $\mathbb{Z}[i]$, so erzeugt $\bar{1}, \bar{i}$ den $\mathbb{Z}/3$-VR κ. Wäre $\dim_{\mathbb{Z}/3} \kappa = 1$, so

$0 \to (3) \to \mathbb{Z}[i] \to \kappa \to 0$. $y = a + ib$ und $\mathbb{Z}[i] = \{uy + v\cdot 3 \mid u, v \in \mathbb{Z}\}$. $y \mapsto \bar{y}$. Ist $b \neq 0$, so $1 \notin \mathbb{Z}[i]$ ↯.

Betrachte $\mathbb{Z}_9 = \varprojlim_{n \geq 1} \mathbb{Z}[i]/3^n$. $\mathbb{Z}[i] \overset{\iota}{\hookrightarrow} \mathbb{Z}_9$ via $x \mapsto (\bar{x}, \bar{x}, \dots)$, denn $\ker \iota = \bigcap_{n \geq 1} (3^n) \subseteq \mathbb{Z}[i]$, also $x \in \ker \iota$, $x \neq 0$, $x = \varepsilon \cdot \prod p_i^{r_i}$, $p_i \in \mathbb{Z}[i]$ prim ↯

$\leadsto x = 0$. Sei $S = \{a + ib,\ a, b \in \{0,1,2\}\}$ ist Vertretersystem von $\mathbb{Z}[i]/3$ $\leadsto$ $\mathbb{Z}_9 = \{\sum_{n \geq 0} a_n 3^n \mid a_n \in S\}$ wie bei $\mathbb{Z}_p$. $\leadsto$ $x \in \mathbb{Z}_9$, so

$x = 3^k \cdot x'$, $\bar{x}' \not\equiv 0\ (3)$. setze $v(x) = k$, $\mathbb{Q}_9 = \mathrm{Quot}(\mathbb{Z}_9) = \mathbb{Z}_9[\frac{1}{3}]$

$= \{\sum_{n \gg -\infty} a_n 3^n \mid a_n \in S\}$. und setze Bew. v auf $\mathbb{Q}_9$ fort $\leadsto$ $\mathbb{Q}_9$ diskret Bew. Kp. mit endl. Restklassenkp. $\mathbb{Z}[i]/3 = \mathbb{F}_9$, $\mathbb{Q}_9$ vollst:

(a_n) CF in $\mathbb{Q}_9$ $\leadsto$ $\forall m\ \exists N$: $v(a_k - a_l) > m$, d.h. $a_k - a_l = 3^{m+1} \cdot (a_0 + a_1 3 + \dots)$

$a = \sum 3^n b_n$ ex. in $\mathbb{Q}_9$. $\mathbb{Q}_9$ ist endl. Erw von $\mathbb{Q}_3$. $\mathbb{Z}_3 \subseteq \mathbb{Z}_9$

wg $\mathbb{Z}/3^n \hookrightarrow \mathbb{Z}[i]/3^n$ (ÜA: $M_n \hookrightarrow N_n$ inj. $\leadsto \varprojlim M_n \hookrightarrow \varprojlim N_n$)

$\leadsto \mathrm{Quot}(\mathbb{Z}_3) = \mathbb{Q}_3 \subseteq \mathbb{Q}_9$. Sogar quadr. Erw. von $\mathbb{Q}_3$: $X^2 + 1$ irred in $\mathbb{F}_3[X]$ $\leadsto$ irred in $\mathbb{Z}_3[X]$ $\leadsto$ irred in $\mathbb{Q}_3[X]$ nach Gauß-Lemma.

$\leadsto i \in \mathbb{Q}_9$, $\underset{\mathbb{Q}_3(i)}{\mathbb{Q}_3/(X^2+1)} \underset{\mathbb{Z}[i]}{\cup} \subseteq \mathbb{Q}_9$. Später $\mathbb{Q}_3(i)$ vollst, da endl. Erw. von $\mathbb{Q}_3$ $\leadsto$ $\widehat{\mathbb{Q}(i)} \subseteq \mathbb{Q}_3(i)$ bzgl 3-ad.

Betrag $\leadsto \mathbb{Q}_9 = \mathbb{Q}_3(i)$.

- K lokaler Kp $\leadsto$ K lokal kompakt: Rem: T top Raum, so T kompakt: $\forall$ U_i off. Ü ex. endl. Teilüberd. von T. T lokal kompakt $\iff$ $\forall x \in T$ $\exists$ $U_x \in \mathcal{U}(x)$ off. Umg. s.d. $\bar{U}_x$ kompakt.

Also K lok. Kp. $\leadsto$ $\mathcal{O}_K$ kompakt: $\mathcal{O}_K = \varprojlim \mathcal{O}_K/\mathfrak{p}^n = \varprojlim \mathcal{O}_K/\pi^n$, $\mathfrak{p} = (\pi)$

Ist $x \in \mathcal{O}_K$, so $x = \sum a_n \pi^n$, $\bar{a}_n \in \mathcal{O}_K/\mathfrak{p}$ endl. Vertretersystem

$\prod \mathcal{O}_K/\mathfrak{p}^n \supseteq \varprojlim \mathcal{O}_K/\mathfrak{p}^n$ ersteres kompakt nach Tychonoff

Rechts 2.2: $\varprojlim \mathcal{O}_K/\pi^n$ abg. in $\prod \mathcal{O}_K/\pi^n$, denn: T top Raum T kompakt, $X \subseteq T$ abg. $\rightsquigarrow$ X kompakt: U_i off Überd. von X, so $U_i = \tilde{U}_i \cap X$, $\tilde{U}_i \subseteq T$ offen $\rightarrow$ $\bigcup \tilde{U}_i \cup T \setminus X$ off Überdeckung von T $\rightsquigarrow$ ex. endl. Teilüb. $\tilde{U}_{i_1} \cup \dots \cup \tilde{U}_{i_n} \cup T\setminus X$ von T $\rightsquigarrow$ $\{U_{i_j}\}$ überdecken X.

Sei $C_n \subseteq \prod \mathcal{O}_K/\pi^n$, $C_n = \{(x_n) \mid \pi_n(x_n) = x_{n-1}\}$, $\pi_n: \mathcal{O}_K/\pi^n \to \mathcal{O}_K/\pi^{n-1}$

$\rightsquigarrow$ $\varprojlim \mathcal{O}_K/\pi^n = \bigcap C_n$, $C_n^c = \prod_{k \neq n, n+1} \mathcal{O}_K/\pi^k \times \underbrace{U_n \times U_{n-1}}_{(x_n, x_{n-1})}$. $\pi_n(x_n) \neq x_{n-1}$

offen nach Def. der Produkttop. $\rightsquigarrow$ C_n abg. $\rightsquigarrow$ $\bigcap C_n$ abg $\rightarrow$ Beh.

- Sei $\overline{\mathbb{Q}}_p = k$ nichtarch. top., wobei wir annehmen, daß Fortsetzung von v_p auf k ex. $\rightsquigarrow$ $v(k) \supseteq \mathbb{Q}$, da n-te Wurzeln von jedem Elt in k ex. müssen. $\rightsquigarrow$ v_K nicht diskret (in $\mathbb{R}$). insbes. $\mathcal{O}_K = \{x \in k \mid v_p(x) \geq 0\}$ nicht noethersch (sonst $m_K = (x)$). $m_K \subseteq \mathcal{O}_K$ ist abgeschlossen? allg. K nicht-arch. top. ~~$B(x,r)$~~, $x \in k$, $r > 0$ $\rightsquigarrow$ $B_r(x) = \{y \in k \mid |y-x| < r\}$ ist offen & abg. Offen klar, abg.: Sei $z \in \overline{B_r(x)}$, d.h. $\forall \varepsilon > 0$ $B_\varepsilon(z) \cap B_r(x) \neq \emptyset$. Sei $s \leq r$ $\rightsquigarrow$ $\exists y \in B_s(z) \cap B_r(x) \neq \emptyset$, $|y - z| \leq s \leq r$, $|y-x| < r$ $\rightsquigarrow$ $|z-x| = |z-y+y-x| \leq \max\{|z-y|, |y-x|\} < r$ $\rightarrow$ $z \in B_r(x)$.
$m_K \subseteq k$ abg. also $m_K = \mathcal{O}_K \cap m_K$. also m_K abg in $\mathcal{O}_K$. Zeige: m_K nicht kompakt $\Rightarrow$ $\mathcal{O}_K$ nicht kompakt. $m_K = \bigcup_{n \geq 1} \{x \in \mathcal{O}_K \mid v(x) > \frac{1}{n}\}$ offen aber keine endl. Teilüber ex., da sonst $m_K = \{x \mid v(x) > \frac{1}{m}\}$ aber $p^{1/m+1} \in m_K$, $\notin \{x \mid v(x) > \frac{1}{m}\}$.

- Einheiten in K, k lokaler top, π prim

$K^\times = (\pi) \times \mathbb{Z}/q-1 \times \underset{1+p}{U^{(1)}}$ via $k^\times = (\pi) \cup \mathcal{O}_K^\times$, $U^{(1)} \to \mathcal{O}_K^\times \xrightarrow{x \bmod p} k^\times \to 0$ und $k^\times$ zyklisch der Ordn. $q-1$.

$\rightsquigarrow$ $k^\times = \mathbb{Z} \oplus \mathbb{Z}/q-1 \oplus \mathbb{Z}/p^a \oplus \mathbb{Z}_p^d$ in char $k = 0$ $q = p^d$.
$k^\times = \mathbb{Z} \oplus \mathbb{Z}/q-1 \oplus \mathbb{Z}_p^{\mathbb{N}}$. in char $k = p > 0$

Bel. Ist K lokal von char $k = p > 0$, so ex. ein

U6 $\Delta \subseteq k^\times/k^{\times n}$ $\overset{1:1}{\longleftrightarrow}$ ab Erw. von Grad $\mid n$ $K(\Delta^{1/n})$
$\Delta = (k^\times \cap (L^\times)^n)/k^{\times n}$

AZ1 Üb. 16.11.15

K vollst. ultrametrischer Kp.

Hensel's Lemma. $f \in K[X]$, $|f| = \sup\{|a_k|\} \doteq 1$ (d.h. f primitiv) und gilt $f \equiv \bar{g} \cdot \bar{h} \mod \mathfrak{p}$ mit $\bar{g}, \bar{h} \in \mathcal{O}/\mathfrak{p}[X]$ tf., so besitzt f eine Zerlegung $f = gh$ in $\mathcal{O}[X]$, $\partial f = \partial \bar{f}$, $\partial g = \partial \bar{g}$.

Wichtig, weil wir oft an Erw. $K[X]/(f)$ interessiert sind und $(f) = (af)$, $a \in K^\times$, s.d. wir meist f primitiv annehmen können

Insbes.: Ist $\bar{\alpha} \in \kappa$ mit $f \equiv \bar{g} \cdot (X - \bar{\alpha}) \mod \mathfrak{p}$, d.h. $\bar{\alpha}$ Nst von $\bar{f}$ (und damit die einzige nötige Vor.), so ex. eine eind. Nst. α von f in $\mathcal{O}$. mit $\alpha \equiv \bar{\alpha}$ $(\mathfrak{p})$

Sonst: $f = f' (X - \alpha)(X - \alpha')$ mit $\alpha \equiv \alpha' \equiv \bar{\alpha}$ $(\mathfrak{p})$ ⇝ $\bar{f} = \underbrace{\bar{f}' (X - \bar{\alpha})}_{\bar{g}} \underbrace{(X - \bar{\alpha})}_{\bar{h}} =$ ↯.

Wie sieht es z.B. mit Polyn. aus, die mod $\mathfrak{p}$ nicht separabel?

Bsp. $f = X^p - 1$, $K = \mathbb{Q}_p$. ⇝ $f \equiv (X-1)^p \mod p$. Wenn diese Faktorisierung zu $\mathbb{Z}_p[X]$ liften würde, enthielte $\mathbb{Q}_p$ alle p-ten EW. ⇝ $f = \prod (X - \alpha_i) = (X-1)^p$ ⇝ $\alpha_i \equiv 1$ (p). d.h. $\alpha = \alpha_i = 1 + x$, $x \in \mathfrak{p}$ ⇝ $\log((1+x)^p) = p \cdot \log(1+x) = \log(1) = 0$
⇝ $\log(1+x) = 0$, also $\exp\log(1+x) = 1 + x = \exp(0) = 1$ ⇝ $x = 0$.

Weitere Anwendung. Autom. von $\mathbb{Q}_p$: $\sigma: \mathbb{Q}_p \to \mathbb{Q}_p$ Km. autom, so σ stetig. Dann folgt $\sigma(\lim x_n) = \lim \sigma(x_n)$, d.h. $\sigma = id$, da $\forall x \in \mathbb{Q}_p$ $\exists (x_n) \subseteq \mathbb{Q}$ CF mit $\lim x_n = x$. Warum stetig? Kriterium: $a \in \mathbb{Z}_p^\times \Leftrightarrow X^n = a^{p-1}$ hat Lsg für ∞-viele versch. n.

„⇒": $a^{p-1} \equiv 1$ (p) da $\# \mathbb{F}_p^\times = p - 1$. Sei $n \in \mathbb{N}$, $p \nmid n$ ⇝ $f = X^n - 1$, $f' = n X^{n-1} \not\equiv 0$ (p) hat nur 0 als Nst. d.h., da f 0 nicht als Nst hat, ist f separabel mod p (die mehrfachen Nst stimmen mit den gem. Nst von f, f' überein). ⇝ 1 ist Nst von f mod p und liftet mit Hensel zu einer eind. Nst. von $X^n - a^{p-1}$ in $\mathbb{Z}_p$.

„⇐", $x^n = a^{p-1}$ für ∞-viele n ⇝ $n \cdot v(x) = (p-1) v(a)$ ⇝ $n \mid (p-1) v(a)$ für ∞-viele n ⇝ $v(a) = 0$. ⇝ $a \in \mathbb{Z}_p^\times$.

Damit also: $x = \mathbb{Q}_p$, $x = p^n \cdot a$, $a \in \mathbb{Z}_p^\times$, $\sigma(x) = p^n \sigma(a) = p^n a'$, $a' \in \mathbb{Z}_p^\times$ d.h. $|x|_p = |\sigma(x)|_p$, insbes. $|\sigma(x) - \sigma(y)| = |x - y| \leq 1 \cdot |x - y|$ also lipschitz stetig

Verzw. index & Trägheitsgrad. Wissen: wenn L/K endlich, K wie oben, so ex. eind. Fortsetzung von v_K auf L durch $v_L(x) = \frac{1}{[L:K]} v_K(N_{L/K}(x))$.
Da $N_{L/K}(x) = x^{[L:K]}$ für $x \in K$ ist $v_L(K^\times) \subseteq v_K(K^\times)$ eine UG. (von endl. Index)
$e = e_{L/K} = (v_L(L^\times) : v_L(K^\times))$ Verzweigungsindex, klar: ist L/K, M/L endlich, so $e_{M/K} = e_{M/L} \cdot e_{L/K}$ (Gruppenindexformel)
$f = f_{L/K} = [\kappa_L : \kappa_K]$ heißt der Trägheitsgrad. Ebenfalls klar: $M/L/K$ wie oben, so $f_{M/K} = f_{M/L} \cdot f_{L/K}$ (Kp.indexformel)

Bsp. $\mathbb{Z}_9$ bzw. $\overset{L}{\mathbb{Q}_9}/\overset{K}{\mathbb{Q}_3}$ aus letzter Übung: $\mathbb{Z}_9 = \{\sum a_n 3^n \mid a_n \in S\}$, $S = \{a+ib,\ a,b \in \{0,1,2\}\}$.

$\mathbb{Z}_9/m_9 = \mathbb{F}_9$, d.h. $f_{\mathbb{Q}_9/\mathbb{Q}_3} = 2$ $(3^2 = 9)$

$v_{\mathbb{Q}_9}$ ges. durch $v_{\mathbb{Q}_9}(x) = \sqrt[{[\mathbb{Q}_9:\mathbb{Q}_3]}]{N_{L/K}(x)}$ ~~Bsp~~ Zunächst: $\mathbb{Q}_3(i) \subseteq \mathbb{Q}_9$, $\mathbb{Z}[i] \subseteq \mathbb{Q}_3(i)$

und $\mathbb{Q}_9 = \widehat{\mathbb{Q}(i)} \subseteq \mathbb{Q}_3(i)$ da endl. Erw. und damit vollst. (bzgl. 3-adischen Norm)

$\leadsto \mathbb{Q}_9 = \mathbb{Q}_3(i)$, d.h. $[\mathbb{Q}_9 : \mathbb{Q}_3] = 2$. $N_{L/K}(S) = \{0, 1, \sqrt{2}, 2, \sqrt{8} = 2\cdot\sqrt{2}, \sqrt{5}\}$.

Dabei $\sqrt{2}, \sqrt{5} \in \mathbb{Q}_3$, da X^2-2 bzw. X^2-5 mod 3 in LF zerfallen,

d.h. Lsg. in $\mathbb{Z}_3$ ex. $\leadsto x \in \mathbb{Z}_9$, $x = \sum a_n 3^n$, so $N(x) = \lim_{k\to\infty} N(\sum_{n=0}^{k} a_n 3^n)$

~~$= \lim \sum N(a_n)3^n$, also surjektiv, da~~ aber Norm nicht additiv!

Trotzdem folgendes Diagramm:

$$\begin{tikzcd} 0 \arrow[r] & U_9^{(1)} \arrow[r] \arrow[d, "N"] & \mathbb{Z}_9^\times \arrow[r] \arrow[d, "N"] & \mathbb{F}_9^\times \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & U_3^{(1)} \arrow[r] & \mathbb{Z}_3^\times \arrow[r] & \mathbb{F}_3^\times \arrow[r] & 0 \end{tikzcd}$$

$U_9^{(1)} = 1+3\cdot\mathbb{Z}_9$, $U_3^{(1)} = 1+3\mathbb{Z}_3$ und

$N(U_9^{(1)}) \subseteq U_3^{(1)}$: $1+x \in U_9^{(1)}$, $\sigma(1+x) = 1+\sigma(x)$ $\forall \sigma \in Gal(L/K)$, $\sigma(x) \in 3\mathbb{Z}_9$

$\underbrace{N(1+x)}_{\in \mathbb{Z}_3} = \prod_{\sigma\in Gal}(1+\sigma(x)) = \underbrace{1+\sum\sigma(x)}_{\in\mathbb{Z}_3} \mod 3^2\cdot\mathbb{Z}_9$ $\Rightarrow$ Rest $\in \mathbb{Z}_3$, also $N(1+x) \equiv 1$ (3)

Damit macht Diagramm Sinn. Z.z. also: $N : \mathbb{Z}_9^\times \to \mathbb{Z}_3^\times$ surjektiv. (Analog: (n) statt (1))

Wissen: $U^{(1)} = \varprojlim U^{(1)}/U^{(n)}$, $U^{(n)} = 1+p^n$. $\leadsto$

$$\begin{tikzcd} 0 \arrow[r] & U_9^{(n-1)}/U_9^{(n)} \arrow[r] \arrow[d] & U_9^{(1)}/U_9^{(n)} \arrow[r] \arrow[d] & U_9^{(1)}/U_9^{(n-1)} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & U_3^{(n-1)}/U_3^{(n)} \arrow[r] & U_3^{(1)}/U_3^{(n)} \arrow[r] & U_3^{(1)}/U_3^{(n-1)} \arrow[r] & 0 \end{tikzcd}$$

Äußeren zwei surj., also Mitte auch $\leadsto$

$\varprojlim U_9^{(1)}/U_9^{(n)} \to \varprojlim U_3^{(1)}/U_3^{(n)}$ surj! (ML-Bed.)

$\leadsto N : \mathbb{Z}_9^\times \twoheadrightarrow \mathbb{Z}_3^\times$ $\leadsto$ $e_{L/K} = 1$, da $v(N(x)) = 2\cdot\mathbb{Z}$, also $\frac{1}{[L:K]}\cdot 2\mathbb{Z} = \mathbb{Z}$

Unverzw. Erweiterungen (für Aufg. 1) Zunächst $K/\mathbb{Q}_p$ endlich mit $k_K = \mathbb{F}_q$, $q = p^f$

$\leadsto K$ enthält nach Hensel die (p^f-1)-ten EW da $X^{p^f-1}-1$ in $\mathbb{F}_q$ vollst. in LF zerfällt. (versch.) Gibt es umgekehrt zu jeder (eind.) $\mathbb{F}_q/\mathbb{F}_p$ eine Erw. $K/\mathbb{Q}_p$, die "minimal" mit dieser Eig. ist? Ja! D.h. $[K:\mathbb{Q}_p] = [\mathbb{F}_q : \mathbb{F}_p] = f$?

Zunächst: $[K:\mathbb{Q}_p] \geq f$ wie oben, da $\mathbb{F}_q = \mathbb{F}_p(\bar{\alpha})$ und $\bar{g} = \mathrm{Mipo}_{\mathbb{F}_p}\bar\alpha$, $\partial\bar{g} = f$

$\leadsto \exists\, g \in \mathbb{Z}_p[x]$: $\bar{g} \equiv g$, (p), $\partial g = f$, g irred. (sonst mod p red.) $\leadsto \bar{\alpha}$ liftet nach Hensel zu einer Nst α von g $\leadsto$ $\mathbb{Q}_p[x]/(g) \subseteq K$ d.h. $[K:\mathbb{Q}_p] \geq f$.

D.h. wenn wir eine Nst von g in $\overline{\mathbb{Q}}_p$ zu $\mathbb{Q}_p$ adjungieren, erhalten wir eine Erw K vom Grad f, d.h. $\mathcal{O}_K/m_K = \mathbb{F}_q$. Andererseits hat $X^{p^f-1}-1$ eine ~~eind.~~ Lsg. α in K da primitiv und mod m_K in $\mathbb{F}_q$ eine Lsg. ex., s.d. $\langle\bar{\alpha}\rangle = \mathbb{F}_q$. $\leadsto \alpha, \alpha^2, \dots, \alpha^{p^f-1}$ alle verschieden, da mod m_K verschieden

$\leadsto$ e prim. (p^f-1)-te EW., $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geq f$, aber auch

$K \supseteq \mathbb{Q}_p(\alpha)$ $\leadsto f = [K:\mathbb{Q}_p] \geq [\mathbb{Q}_p(\alpha):\mathbb{Q}_p] \geq f$ $\leadsto$ "=". Die eind. Erw. vom Grad f erhält man durch Adj. einer primit. (p^f-1)-ten EW.

Außerdem: $v_K(\alpha) = 0$, da Einheit. Ist $x \in K$, so also $x = a_0 + \alpha a_1 + \dots + \alpha^{f-1}a_{f-1}$

$a_i \in \mathbb{Q}_p$. Z.z.: $\alpha^i\cdot a_i = \sum_{n\geq 0} b_n p^n$, $b_n \in \mathbb{F}_q$ $\quad \alpha^i\cdot a_i \equiv b_0 \mod m_K$ $\leadsto$

$\alpha^i a_i - b_0 \equiv \sum_{n\geq 1}\alpha^i a_n p^n = p\cdot(\sum_{\geq 0}\alpha^i a_n p^n)$ $\leadsto$ $\alpha^i\frac{a_i - b_0}{p} \equiv b_1$ (m_K), $\quad \alpha^i a_i = b_0 + pb_1 + \dots + p^k b_k + r$, $r \in m_K^{k+1}$ $\Rightarrow$ Beh.

$\leadsto$ $e_{K/\mathbb{Q}_p} = 1$, $\pi_K = p$ Primelt.

Az 1 23.11.15 Üb.

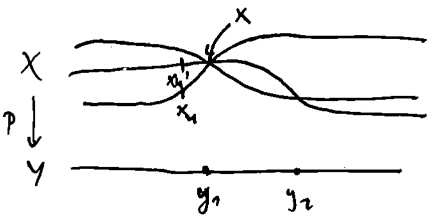
K vollst. bew. Kp mit na Bew., L/K endlich.

Verzweigungsindex. $e = (w(L^\times) : v(K^\times))$ endlich, weil ... ? $(K \subseteq L)$.

Trägheitsgrad. $f = [\lambda : k] = [\kappa_L : \kappa_K]$ endlich, weil ... ? $[L:K] \geq [\kappa_L : \kappa_K]$.

Fund. Gleichung für K lokal; L/K endlich: $[L:K] = e \cdot f$

L/K unverz. $:\Leftrightarrow$ $[L:K] = [\kappa_L : \kappa_K]$, κ_L / κ_K separabel. Warum diese Def?



Geom. Interpret. i) $X \to Y$ Abb. top. Räume. y_1, y_2 sind Verzw.-punkte ($\nexists$ Umg. $Y_1 \ni y_1$: $X_1 \subseteq Y_1$ offen, $p|_{X_1}$ inj.). Betrachte $\Delta : X \to X \times_Y X$ (m (x, x') : $p(x) = p(x')$), $\Delta(x) = (x, x)$. p vzw. bei $y = y_1$ $\Leftrightarrow$ $X \times_Y X \setminus \Delta(X)$ nicht abg. $\Leftrightarrow$ $\exists$ Folge $(x_n, x_n') \in X \times_Y X \setminus \Delta(X)$ deren Grenzwert in $\Delta(X)$ liegt. D.h. definiere $X \to Y$ unverz. $\Leftrightarrow$ $\Delta : X \to X \times_Y X$ off. Immersion.

ii) $p : X \to Y$ von (kompakten) Riemann'schen Flächen, mit Garben von meromorphen Fn. / holom.: $\mathcal{O}_X$: Fn auf Umg. von $x \in X$, die holom. bei x sind, analog $\mathcal{O}_Y$, m_x max. Ideal darin von Fn, die verschwinden bei x. Dann p unverz. bei y $\Leftrightarrow$ $m_y \mathcal{O}_X = m_x$, i.a. $= m_x^e$

$\mathcal{O}_Y \to \mathcal{O}_X$
$f \mapsto f \circ p$

iii) $p : X \to Y$ von Schemata (bei uns: $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$, L/K wie oben, ind. $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$)

Aber haben noch "versteckte" Verzw. beim Restkl.-Kp. (spezielle Fasern), die endl. sep. Erw. liefern gerade die "geom. Punkte". Insgesamt kann man zeigen: $\Delta : X \to X \times_Y X$ offene Imm. bei x $\Leftrightarrow$ $m_y \mathcal{O}_{X,x} = m_x$, $\kappa(x)/\kappa(y)$ separabel. (Milne 3.6)
(insbes. $\pi_L = \pi_K$)

Beschreibung unverz. Erw. L/K unverz. $\Leftrightarrow$ $L = K(x)$ für $x \in \mathcal{O}_K$ für $\bar{f} = \mathrm{Mipo}_K(x) \in \kappa_K[X]$ sep. Dann gilt $\mathcal{O}_L = \mathcal{O}_K[x]$

Bew: $\kappa_L = \kappa_K(\bar{x})$, $\cancel{f = \mathrm{Mipo}_{\kappa_K}(x)}$, $f \in \mathcal{O}_K[X]$ liegt irred. Mipo von $x \in \mathcal{O}_L$ Lift $\rightsquigarrow$ $\bar{f}$ irred, $[K(x) : K] = \deg f = [\kappa_L : \kappa_K]$ $\rightsquigarrow$ $K(x) = L$.

Umkehrung analog.

Falls $\mathcal{O}_L \neq \mathcal{O}_K[x]$, so ex. $y \in \mathcal{O}_L$: $\pi_K y \in \mathcal{O}_K[x]$, aber $y \notin \mathcal{O}_K[x]$.

$\pi y = \sum a_i x^i$, $1, \bar{x}, \dots, \bar{x}^{n-1}$ Basis von κ_L / κ_K, mod π muß $a_i \equiv 0$ gelten $\rightsquigarrow$ $a_i \in \pi \mathcal{O}_K$ $\rightsquigarrow$ $y \in \mathcal{O}_K[x]$ ↯.

Aufg 3 auf Zettel: L/K, M/K endl. sep. $\sigma : L \to M$ K-Algebrenhom. ergibt $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_M$: alles spielt sich in $L \cdot M$ über K ab. Fortsetzung der Bew. mit der Norm. $\rightsquigarrow$ σ induziert κ_K-Algebrenhom. $\kappa_L \to \kappa_M$, da auch $\sigma(m_L) \subseteq m_K$

$L \mapsto \kappa_L$, $\sigma : L \to M \mapsto \sigma : \kappa_L \to \kappa_M$ ist also Funktor

$\{L/K$ endl., sep.$\} \to \{$endl. sep. Erw. von $\kappa_K\}$.

Aufg 3 sagt also, falls L unverzw. ist, so $\mathrm{Hom}_{K\text{-Alg}}(L,M) \to \mathrm{Hom}_{\kappa_K\text{-Alg}}(\kappa_L,\kappa_M)$ bijektiv

Folgerung. k'/κ_K endl. sep., so ex. eind. Erw. L/K unverzw. mit $\kappa_L = k'$ (bis auf Iso)

$k' = \kappa_K(\bar{x}) \leadsto$ lifte Minipo zu $K[X]$ $\leadsto$ $L = K(x)$ hat richtigen Grad, also unverzw. M unverzw so ex. also ~~...~~ Iso zw. L, M.

Bsp i) Unverzw. Erw. von $\mathbb{F}_p((t))$ mit t-adischer Bew. sind gerade $\mathbb{F}_{p^n}((t))$, max. unverzw. Erw. ist also $\bigcup_{n \geq 1} \mathbb{F}_{p^n}((t)) \neq \overline{\mathbb{F}_p((t))}$.

ii) total verzw. Erw. von $\mathbb{F}_p((t'))$: $t^e = t'$, $\mathbb{F}_p((t))/\mathbb{F}_p((t'))$ ist total verzw. mit Verzw.index e. (entsteht durch $X^e - t^e$)

$[L:K] = [\kappa_L : \kappa_K]$

Bsp einer Erw. L/K mit: K vollst nicht-archim., κ_K nicht perfect von char. p. (z.B. $\kappa = \mathbb{F}_p((t))$): wähle etwa $C(\kappa) = \mathcal{O}_K$ Cohen-Ring zu κ, ist vollst diskreter Bew.ring (d.h. $\mathcal{O}_K = \varprojlim \mathcal{O}_K/p^n\mathcal{O}_K$, $\mathcal{O}_K/p\mathcal{O}_K = \kappa$). $K = \mathrm{Quot}(\mathcal{O}_K)$.

Sei $a \in \kappa$ nicht p-te Wurzel (e.g. $a = t$) $\leadsto$ $X^p - a \in \kappa[X]$ irred.

sei f lift von $X^p - a$ (d.h. mod p: $\bar{f} = X^p - a$) $\leadsto$ f irred in $K[X]$, ($L = K[X]/f$) Erw von K vom Grad p, separable, da char $= 0$. $\mathcal{O}_L = \mathcal{O}_K[X]/f$ ist ~~Bew.ring~~: Intbereich und $\mathcal{O}_L/p\mathcal{O}_L = (\mathcal{O}_K[X]/p)/(f)/(pf) \cong \kappa[X]/(X^p - a)$ Körper. $\leadsto$ $p\mathcal{O}_L$ max. Ideal von $\mathcal{O}_L$. Ist m' weiteres max. Ideal von $\mathcal{O}_L$ so $m' \cap \mathcal{O}_K = (p)$ ist maximal, d.h. $p\mathcal{O}_L \subseteq m'$ $\leadsto$ $m' = p\mathcal{O}_L$.

Also $\mathcal{O}_L$ diskr. Bew.ring, da ~~...~~ lokal mit max. Ideal HI. ! $x \in \mathcal{O}_L \setminus \mathcal{O}_L^\times$ (d.h. $x \in p\mathcal{O}_L$) so $x \in (p)$, also $x = p^n v = p^m v'$ mit $v, v' \in \mathcal{O}_L^\times$ $\leadsto$ $p^n v = p^m v' \overset{m>n}{\Leftrightarrow} p^n(v - p^{m-n}v') = 0 \Leftrightarrow vv'^{-1} = p^{m-n} \notin \mathcal{O}_L^\times$ ↯.

$\leadsto$ $\mathcal{O}_L$ diskr Bew.ring, $L = \mathrm{Quot}(\mathcal{O}_L)$, $\mathcal{O}_L$ ist der ganze Abschluß von $\mathcal{O}_K$ in L, also der Bewring von L. $\leadsto$ $\kappa_L = \kappa[X]/(X^p - a)$ von Grad p, rein insep. aber L/K sep, $e_{L/K} = 1$, $f_{L/K} = [L:K] = [\kappa_L : \kappa_K]$, aber L/K nicht unverzw. ($\mathrm{Gal}(L/K) = \mathbb{Z}/p\mathbb{Z}$, falls K p-te EW enthält, aber ~~...~~ $\mathrm{Gal}(\kappa_L/\kappa_K) = 1$)

$x \in p^k v \ \forall k$, so $x \in \bigcap p^k = 0$,

da $\mathcal{O}_L = \varprojlim \mathcal{O}_L/p^n\mathcal{O}_L = \ldots$

bzw $p^n\mathcal{O}_L = p^n\mathcal{O}_K[X]/(p^n f)$

$$\begin{tikzcd}
& 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & (f) \arrow[r] \arrow[d, "p"] & \mathcal{O}_K[X] \arrow[r] \arrow[d, "p"] & \mathcal{O}_L \arrow[r] \arrow[d, "p"] & 0 \\
& (f) \arrow[r] \arrow[d] & \mathcal{O}_K[X] \arrow[r] \arrow[d] & \mathcal{O}_L \arrow[r] \arrow[d] & 0 \\
& (f)/(pf) \arrow[r] & \mathcal{O}_K[X]/p \arrow[r] & (\mathcal{O}_K[X]/f)/p \arrow[r] & 0
\end{tikzcd}$$

Serre, LF V. §2. Lemma 2.
(oder Bourbaki)

AZ 1 ÜS 30.11.15

k vollst. nicht-arch. bew. Kp ($\rightsquigarrow$ Hensels Lemma gilt).

L/K Erw. endl.

- unverzweigt $\Leftrightarrow$ κ_L/κ_K sep, $[L:K]=[\kappa_L:\kappa_K]$ (entsteht durch Polynome $X^{p^f-1}-1$)
- zahm verzweigt $\Leftrightarrow$ κ_L/κ_K sep, $p\nmid[L:T]$, $K\subseteq T\subseteq L$ max. unverz. Teilerw.

Insbes.: unverzweigt $\Rightarrow$ zahm verzweigt.

- ~~vollst. verzweigt~~ $\Leftrightarrow$ $T=K$.

VL: L/K zahm verzweigt $\Leftrightarrow$ $L=T(\sqrt[m_1]{a_1},\dots,\sqrt[m_r]{a_r})$ mit $p\nmid m_i$.

Beweisidee: (wie finde ich die $\sqrt[m_i]{a_i}$?) wähle Repräsentantensystem von $w(L^\times)/v(K^\times)$ mit Ordnungen m_i sowie Elt in $L^\times$, die gerade diese Ordnung haben.

Speziellere Situation. K diskret bewertet. Dann $\underset{T}{w}(L^\times)/v(K^\times)=\mathbb{Z}/e\mathbb{Z}$.
so ex. π_T' Unif.: $L=k(\sqrt[e]{\pi_T'})$

Wähle $m_1=e$, $a_1=\pi_T$ Uniformisierende (Sei ex.), d.h. $w(\pi_T)=1$, $w(\underset{\gamma}{\sqrt[e]{\pi_T}})=\frac{1}{e}$.

Wie haben wir $\sqrt[e]{\pi_T}$ dabei gefunden? $\gamma\in L$, $w(\gamma)=\frac{1}{e}$, $\rightsquigarrow$ $w(\gamma^e)=w(\pi_T)$

$\rightsquigarrow$ $\gamma^e=\underset{\in L}{\varepsilon}\cdot\pi_T$, $\kappa_L=\kappa_T$: $\varepsilon=b\cdot u$, $b\in T$, $u\in\mathcal{U}_L^1$; $b\in\mathcal{O}_T^\times$ ($\Leftrightarrow u\equiv 1 \bmod p_L$)

$$0\to \underset{1+p_L}{\mathcal{U}_L^1}\to\mathcal{O}_L^\times\to\kappa_L^\times=\kappa_K^\times\to 0,\quad \mathcal{O}_K^\times\subseteq\mathcal{O}_L^\times$$

X^e-u nach Hensel Lsg β in L,

$\alpha=\gamma\cdot\beta^{-1}$ $\rightsquigarrow$ $w(\alpha)=e$, $\alpha^e=a:=\pi_T\cdot b\in K$. $[L:k]\le e$, aber $[L:k]\geq e\cdot f=e$

also „=" $\rightsquigarrow$ $L=\mathbb{T}(\sqrt[e]{\pi_T\cdot b})$

Achtung: i.a. kann man zu vorgeg. π_T nicht einfach die e-te Wurzel ziehen, um die zahm verz. Erw. zu erhalten!

Bsp. $k=\mathbb{Q}_5$, $f(X)=X^4-50$. $50=25\cdot 2=5^2\cdot 2\rightsquigarrow\sqrt{50}=5\cdot\sqrt{2}$.

X^4-50 ist irred. in $\mathbb{Q}_5[X]$.: (können nicht einfach in $\mathbb{Z}_5$ argumentieren)

Falls $f=(X^2-a)(X^2+a)$, so $a=\sqrt{50}=5\cdot\sqrt{2}$, also $\sqrt{2}\overset{!}{\in}\mathbb{Q}_5$, d.h. X^2-2 muss Lsg haben, aber mod 5: $1^2-2\equiv-1$, $2^2-2\equiv 2$, $3^2-2=7\equiv 2$, $4^2-2\equiv 14\equiv 4$ keine Lsg. (muß in $\mathbb{Z}_5$ sein, da $y^2=2$, $v_5(2)=0$).

Falls α Nst von f in k, so, da $p-1=4$, also die 4-ten EW $\zeta^i\in k$, schon komplett in Lf zerfällt. Insbes. muß $\sqrt{2}\in\mathbb{Q}_5$ sein, ↯.

Also f irred in $\mathbb{Q}_5[X]$. $\rightsquigarrow$ $\mathbb{Q}_5[X]/(f)=L$ Erw. von Grad 4 von $\mathbb{Q}_5$.

e, f? Max. unverz. Erw.: Sei $\alpha\in L$: $\alpha^4=50$. $\rightsquigarrow$ $1,\alpha,\alpha^2,\alpha^3$ $\mathbb{Q}_5$-Basis von L. $L/\mathbb{Q}_5$ galoissch, da $\mu_4\subseteq\mathbb{Q}_5$. $\mathrm{Gal}(L/\mathbb{Q}_5)\cong\mathbb{Z}/4\mathbb{Z}=\langle\sigma\rangle$,

$\sigma:\alpha\mapsto\zeta\alpha$, wenn ζ prim. 4-te EW.

Wäre $L/\mathbb{Q}_5$ unverz., so müßte $X^4-50=f$ mod 5 irred sein (ist es aber nicht), da L ja aus Lift von irred. Polynom von Grad 4 in $\mathbb{Z}_5$ entsteht. ($\bar\beta\in\kappa_L$: $\kappa_L/\mathbb{F}_5$ von Grad 4, $\beta\in\mathcal{O}_L$ Lift, $f=\mathrm{Mipo}_{\mathbb{Q}_5}\beta$ $\rightsquigarrow$ $\bar f=\mathrm{Mipo}_{\mathbb{F}_5}\bar\beta$, $L=\mathbb{Q}_5(\beta)=\mathbb{Q}_5[X]/\mathrm{Mipo}\,\beta$, d.h. $\mathrm{Mipo}\,\beta=X^4-50$), Bsp. $T = \mathbb{Q}_5(\alpha^2)$ ist die max. unverzw. Teilerw. (auch der einzige), echte Erw., da $\alpha^2 = 5\cdot\sqrt{2} \notin \mathbb{Q}_5$. T ist gerade der Fixkörper von $\mathbb{Z}/2\mathbb{Z}$ ($\alpha^2 \mapsto \zeta^4\alpha^2 = \alpha^2$). $\mathbb{Q}_5(\alpha^2) = \mathbb{Q}_5(\sqrt{2})$ und vorher schon gesehen daß X^2-2 irred. in $\mathbb{Z}_5[X]$ bzw. $\mathbb{F}_5[X]$.

D.h. $L = T(\sqrt{5\cdot\sqrt{2}})$, $5\cdot\sqrt{2} = \pi_T \notin \mathbb{O}_5$ Primelement, da $\sqrt{2} \in \mathcal{O}_T^\times$.
Aber ex. kein $\pi_T' \in \mathbb{Q}_5$ prim, s.d. $L = T(\sqrt{\pi_T'})$: $\pi_T' = 5\cdot u$, $u \in \mathbb{Z}_5^\times$ und es muß $\pi_T'^2 = 50$ gelten, da L ja gerade aus Adj. der Nst von $X^4 - 50$ entst.
Also $25u^2 = 50$, also $u^2 = 2$ ↯ da X^2-2 irred. in $\mathbb{Z}_5$.

Wissen aus VL. L/K zahm ⇝ L'/K' zahm (insbes.: Komp. von zahm verzw. ist wieder zahm).
Wissen aus Üb: Komp. zweier total verzw. nicht notw. total verzw.

$$\begin{tikzcd} & L' = L\cdot K' \arrow[dl, dash] \arrow[d, dash] \\ L \arrow[d, dash] & K' \\ K \arrow[ur, dash] & \end{tikzcd}$$

Bsp. $p \neq 2$. $K = \mathbb{Q}_p$ ⇝ $\mathbb{Q}_p^\times = \mathbb{Z} \oplus \underbrace{\mathbb{Z}/(p-1)}_{\mu_{p-1}} \oplus \underbrace{\mathbb{Z}_p}_{U^1_{\mathbb{Q}_p}}$
⇝ $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, Vertreter sind $1, p, u, up$, wobei $u \in \mathbb{Z}_p^\times$:
u quadr. Nichtrest in $\mathbb{F}_p^\times$ (d.h. $\nexists\, v \in \mathbb{F}_p^\times: v^2 = u$) ⇝ gibt 3 nicht-isom. quadr. Erw. von $\mathbb{Q}_p$, die zu u ist unverzw. (Lsg von $X^2 - \bar{u}$ in $\mathbb{F}_p$), die zu p, up sind total verzweigt. Setze also
$L = \mathbb{Q}_p(\sqrt{p})$, $K' = \mathbb{Q}_p(\sqrt{up})$ ⇝ $L' = \mathbb{Q}_p(L \cup K') = \mathbb{Q}_p(\sqrt{p}, \sqrt{u})$.
$k_{L'}$ enthält also die Wurzel von $u \in \mathbb{F}_p$ ⇝ $[k_{L'} : \mathbb{F}_p] = f_{L'/\mathbb{Q}_p} \geq 2$. $(2 \mid f)$
Andererseits $e_{L/\mathbb{Q}_p} \overset{e_{K'/\mathbb{Q}_p}}{=} 2$, und $e_{L'/\mathbb{Q}_p} = e_{L'/L}\cdot e_{L/\mathbb{Q}_p}$, also $2 \mid e_{L'/\mathbb{Q}_p}$
$4 = e\cdot f = 2\cdot 2\cdot a\cdot b$ ⇝ $e = 2$, $f = 2$. Also $f_{L'/L} = f_{L'/K'} = 2$, da $[L':L] = [L':K'] = 2$ und ⇝ L'/L, L'/K' unverzw. kein Widerspr., da unverzw. auch zahm verzw.

$\sqrt{5\cdot\sqrt[4]{2}} \notin \mathbb{Q}_5(\sqrt{2}, \sqrt{5u})$, $u \in \mathbb{Z}_5^\times$

AZ 1 Übung 7.12.15

(K,v) vollständig bew. kp. L/K endlich, K_v Vervollst. von K bzgl. v,

$\tau: L \to \overline{K_v}$ K-Einbettung (ex., da L/K alg.).

$\omega = \bar{v} \circ \tau$ Bew. auf L, L_ω Vervollst. von L bzgl. ω.

$\leadsto L_\omega = LK_v$, da $L \cdot K_v \subseteq L_\omega$ vollständig, enthält L,

also gleich L.

$$\begin{array}{ccc} & & L_\omega \\ L & \nearrow & | \\ | & & K_v \\ K & \nearrow & \end{array}$$

Umkehrung? D.h. L_ω/K_v geg., ex. L/K, s.d. $L \subset L_\omega \to \overline{K_v}$,

L/K endl. und L_ω gerade Vervollst. von L? Ja, zumindest, wenn

L_ω/K_v separabel: $L_\omega = K_v[X]/(f_v)$, $f_v \in K_v[X]$ sep, irred., d.h. $L_v = K_v(\alpha)$,

$f_v(\alpha) = 0 \leadsto f_v'(\alpha) \neq 0$. Sei $f \in K[X]$, s.d. die Koeff nahe bei f_v.

Dann f irred für nahe genug, sonst würde Folge ex. g_n, h_n mit $f_n = g_n h_n \to g \cdot h = f_v$

d.h. f_v red. Sei $L = K[X]/f$. [analog: f separabel $(ggT(f,f') = 1)$]

Wähle Einbettung $\tau: L \to \overline{K_v}$ und L'_ω Vervollst. davon, gleicher Grad wie

L_ω/K_v. Betrachte f_v über L'_ω. Es ex. $x' \in L'_\omega$ mit $|f_v(x')| < |f_v'(x')^2|$

nämlich x' so, daß $L = K(x') = K[X]/f$, da $f(x') = 0$, $f'(x') \neq 0$. $\leadsto$

ex. eind. Nst. $\alpha' \in L'_\omega$: $f_v(\alpha') = 0$. nach Hensel $\leadsto K_v[X]/f_v \hookrightarrow L'_\omega$,

aber aus Gradgründen schon Iso.

Bsp. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $p = 5 \hookrightarrow v_5 = v$. $X^2 + 2 = \bar{f}_v$ in $\mathbb{F}_5[X]$ irred $\leadsto \mathbb{F}_{5^2} = \mathbb{F}_5[X]/\bar{f}_v$

$\leadsto f_v = X^2 + [2]$, $[2] = \lim 2^{5^n} = 2 \cdot 5^0 + 1 \cdot 5^1 + 1 \cdot 5^2 + \ldots \in \mathbb{Q}_5 \setminus \mathbb{Q}$.

und $\mathbb{Q}_5[X]/f_v$ ist die unverz. Erw. vom Grad 2. $f = X^2 + 2$ liefert

$\widehat{\mathbb{Q}(\sqrt{2})} = \#$.

Kummertheorie. Aufgabe 4: K lokal, L/K zahm $\leadsto L = T(\sqrt[e]{\pi})$, $\pi \in T$ prim.

und $I = Gal(L/T)$ ist eine sog. Kummererw. $\cong Hom(\omega(L^\times)/v(K^\times), \mu_{K_L})$

Dazu: K bel. kp., alle n-ten EW in K. Dann klassifiziert Kummerth.

die abelschen Erw. von K vom Exponenten n.

Wir wiederholen das mit Galoiskohomologie: Sei dazu L/K endlich,

galoissch mit Gruppe G. Dann operiert $G \circlearrowright L^\times$. Allg.: ist G endl.

Gruppe, M G-Modul und $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ ex. Sequenz

von G-Moduln (d.h. ex. von ab. Gruppen mit $\iota(\sigma x) = \sigma\iota(x)$

und π ebenso $\leadsto 0 \to M'^G \to M^G \xrightarrow{\pi} M''^G$ ex., aber i.a.

π nicht surjektiv $\quad \{x \in M' \mid \sigma x = x\}$.

Dann ex. nat. Weise, wie man diese Sequenz fortsetzen kann:

$0 \to M'^G \to M^G \to M''^G \xrightarrow{\delta} H^1(G, M') \to H^1(G,M) \to H^1(G,M'') \xrightarrow{\delta} H^2(G,M') \to \ldots$

d.h. $\exists$ ab. Gruppen $H^i(G, M^{(i)})$ die das ex. machen

Schreiben auch $H^0(G,M) = M^G$.

In unserer Sit. betrachten wir $L^\times \xrightarrow{n} L^{\times n} \to 0$, hat Kern gerade $\mu_n = \{x \in L^\times \mid x^n = 1\}$. ⇝ Gal Koh. sequenz

$$0 \to \mu_n^G \to (L^\times)^G \to ((L^\times)^n)^G \to H^1(G, \mu_n) \to H^1(G, L^\times) \to H^1(G, (L^\times)^n) \to \dots$$

Tatsachen. • $\mu_n \le K^\times$, d.h. $\mu_n^G = \{x \in K^\times \mid x^n = 1, \sigma \in Gal(L/k), \sigma(x) = x\} = \mu_n$

Offensichtlich $(L^\times)^G = K^\times$, $(L^\times)^{n\,G} = (K^\times) \cap (L^\times)^n$. Hilbert Satz 90 sagt: $H^1(G, L^\times) = 0$. ⇝

⇝ $0 \to \mu_n \to K^\times \xrightarrow{n} K^\times \cap (L^\times)^n \to H^1(G, \mu_n) \to 0$ exakt.

Da wieder G trivial operiert, kann man zeigen: $H^1(G, \mu_n) = Hom_{Gp}(G, \mu_n)$

$\Rightarrow K^\times \cap (L^\times)^n / K^{\times n} \cong Hom(G, \mu_n)$.

~~Damit~~ . "Ersetze" nun L durch $\bar{k} = \bigcup_{L/k} L$ endlich., $G = Gal(\bar{k}/k)$.

⇝ $(\bar{k}^\times)^n = \bar{k}^\times$ ⇝ $K^\times / K^{\times n} \cong Hom(Gal(\bar{k}/k), \mu_n)$.

Erhalten Entsprechung: zyklische (bzw. ab.) UG von $K^\times/(K^\times)^n$ und zykl. (bzw. ab.) Erw. ~~von~~ L/k vom Exp. n. (Ist $C \le Hom(G, \mu_n)$ zyklisch, so endlich, d.h. $\exists\, \varphi: G \to \mu_n$, mit $C = \langle \varphi \rangle$, $\ker \varphi$ fast alles, d.h. $G/\ker\varphi \cong Im\,\varphi \le \mu_n$ endl. entspricht L_φ/k endlich mit Gal. gruppe zyklisch vom Exp n. $\varphi \mapsto \varphi \circ p$

Umgekehrt: L/k zyklisch vom Exp. n. $\longleftrightarrow G/H$, $H = Gal(\bar{K}/L)$ via $Hom(G/H, \mu_n) \to Hom(G, \mu_n)$

liefert zykl. UG.

Allg. G Abelsch, so $G = \mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_r$, $n_i \mid n$ ⇝ $Hom(G, \mu_n) = \prod Hom(\mathbb{Z}/n_i, \mu_n)$

In unserer Sit.: $Gal(L/T) = \mathbb{Z}/e\mathbb{Z} = \omega(L^\times)/\nu(K^\times)$ und $(e, p) = 1$, d.h. wenn L/T galoissch, so liegen die e-ten EW in T (macht Sinn, da diese Erw. unverz. sind). bzw. entsprechen EW vom Restklassenkörper von L, nämlich $\kappa_L = d$.

Elt. aus H^1 repr. durch $\partial f: G \to M$, $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$

$0 \to M'^G \to M^G \to M''^G \xrightarrow{\delta} H^1(G, M')$

$\underset{\in M}{a} \mapsto \bar{a} \mapsto \delta(\bar{a}) = [G \to M', \sigma \mapsto \underbrace{\sigma(a) - a}]$

modulo Ränder... $\sigma(\bar{a}) - \bar{a} = \bar{a} - \bar{a} = 0$. ⇝ $\in M'$.

Az.1 Üb. 14.12.15

(K,v) vollst. diskret bew. Kp., L/K endlich gal., κ_L/κ_K sep. v_L normiert (auf $\mathbb{Z}$).

$G = Gal(L/K)$. $\quad G \supseteq I \supseteq R$
$$\overset{\shortparallel}{G_{-1}} \supseteq \overset{\shortparallel}{G_0} \supseteq \overset{\shortparallel}{G_1} \supseteq G_2 \supseteq \dots \supseteq 1.$$ höhere Verzw.gruppen.

$I = \{\sigma \in G \mid \sigma x \equiv x \mod m_L \ \forall x \in \mathcal{O}_L\}$. Trägheitsgruppe

$R = \{\sigma \in I \mid \frac{\sigma x}{x} \equiv 1 \mod p_L \ \forall x \in L^\times\}$. Verzweigungsgruppe. $= \{\sigma \in G \mid \dots\}$ wg. $\frac{\sigma(x)}{x} \in \mathcal{O}_L$

(#) (†) Allg.: $G_i = \{\sigma \in G \mid v_L(\sigma(x) - x) \geq i+1 \ \forall x \in \mathcal{O}_L\}$. $\leadsto G_{-1} = G$ ✓

$G_0 = I$ ✓ $\quad G_1 \underset{ii)}{=} R \overset{!}{\underset{ii)}{=}} \{\sigma \in G \mid \frac{\sigma \pi_L}{\pi_L} \equiv 1 \mod p_L\}$, denn i) „$\subseteq$" ✓

„$\supseteq$": $x \in L^\times$, $x = \pi^k o$, $o \in \mathcal{O}_L^\times$ $\leadsto \frac{\sigma(x)}{x} = \frac{\sigma(\pi)^k}{\pi^k}\frac{\sigma(o)}{o} \equiv \frac{\sigma(o)}{o} \mod p_L$, d.h.

wg. $R \subseteq I$: $\sigma(o) \equiv o \ (p_L)$, also $\frac{\sigma(x)}{x} \equiv 1 \mod p_L \ \forall x \in L^\times$.

ii) Sei o.E. L/K total verzw., $\sigma \in G_0$. (ersetze G durch G_0, K durch L^{G_0})

z.z.: $\sigma \in G_1 \iff \frac{\sigma \pi_L}{\pi_L} \equiv 1 \mod p_L$. $\quad \mathcal{O}_L = \mathcal{O}_K[\pi_L]$ $\quad G_1(L/L^{G_0}) = \underset{G_0}{\underset{\shortparallel}{G(L/L^{G_0})}} \cap G_1(L/K) \underset{(L/K)}{= G_1}$

D.h. $v_L(\underset{\geq 2}{\sigma(\pi_L) - \pi_L}) = 1 + v_L(\underset{\geq 1}{\sigma(\pi_L)/\pi_L - 1})$, da $v_L(\pi_L) = 1$

Funktioniert analog für G_i: $G_i = \{\sigma \in G_0 \mid \frac{\sigma(\pi_L)}{\pi_L} \equiv 1 \ (p_L^i)\}$.

Bsp i) $K = \mathbb{Q}_5$, $f = X^4 - 50$, $L = \mathbb{Q}_5[X]/f$ vom Grad 4 / K. $Gal(L/K) = \mathbb{Z}/4\mathbb{Z}$
$= \mathbb{Q}_5(\underbrace{\sqrt[4]{50}}_{\alpha})$ Kummer-Erw.

$T = \mathbb{Q}_5(\alpha^2)$ max. unverzw. Teilerw., L/T zahm verzw., da $L = T(\sqrt{5 \cdot \sqrt{2}})$

und $(2,5) = 1$. $\leadsto$ $\underset{L/K}{\underset{\updownarrow}{G_{-1} = \mathbb{Z}/4\mathbb{Z}}} \supseteq \underset{L/T}{\underset{\updownarrow}{G_0 = \mathbb{Z}/2\mathbb{Z}}} \supseteq \underset{L/L}{\underset{\updownarrow}{1}}$, da $G_1 = 0 \iff L/K$ zahm verzweigt.
prim zu T

ii) $\underset{L}{\shortparallel}\mathbb{Q}_3(\zeta_3, \sqrt[3]{2}) / \mathbb{Q}_3$ galoissch, da Zfkp von $X^3 - 2$.

D.h. $\#Gal(L/K) \mid 3! = 6$. Nun ist $[\mathbb{Q}_3(\zeta_3) : \mathbb{Q}_3] = 2$,

$[\mathbb{Q}_3(\sqrt[3]{2}) : \mathbb{Q}_3] \overset{(*)}{=} 3$, d.h. $[L:K] = 6$. Wg. $G \hookrightarrow S_3$ und

gleicher Ordnung $\leadsto G = S_3 = \langle \tau, \sigma \rangle$, $\tau = (12)$, $\sigma = (123)$

$$\begin{array}{ccc} & L & \\ \mathbb{Z}/3\mathbb{Z} & | & S_3 \\ & \mathbb{Q}_3(\zeta_3) & \quad \mathbb{Q}_3(\sqrt[3]{2}) \\ \mathbb{Z}/2\mathbb{Z} & \mathbb{Q}_3 & \nwarrow \text{nicht gal.} \end{array}$$

Einziger NT (echter) von G ist $\mathbb{Z}/3 = \langle \sigma \rangle$. Max. unverzw? $L/\mathbb{Q}_3$ nicht

unverzw da $\mathbb{Q}_3(\zeta_3)$ ja schon verzweigt, d.h. ebenso $L^{\langle \sigma \rangle} = \mathbb{Q}_3(\zeta_3)$ nicht

unverzw, $\leadsto T = \mathbb{Q}_3$. $L/\mathbb{Q}_3$ auch nicht zahm verzweigt, da $[L : \mathbb{Q}_3(\zeta_3)] = 3 = p$.

$\leadsto G_1 = R \neq 1$, $G_0 = G_{-1} = G$. und $V = L^{G_1} = \mathbb{Q}_3(\zeta_3)$ max. zahm verzw.

Zwischenerw. vom Grad 2, $p \nmid 2$. G_2? Brauchen Uniformisierendes

Elt. von L/K, wobei $v_3 = v$ auf K so normiert, daß $v(3) = 6$ (wg.

$[L:K] = 6 = e_{L/K}$).

da $\mathbb{Q}_3(\sqrt[3]{2})$ nicht zahm verzw. sein kann (sonst L/K zahm)

und die andere Erw. vom Grad 2 wild verzw. (wieder mit Argument über den Grad).

ζ_3 hat Mipo $f(X)=X^2+X+1$ über $\mathbb{Q}_5$, d.h. ζ_3-1 hat Mipo
$f(X+1)=(1+X)^2+1+X+1 = X^2+3X+3$

$\sqrt[3]{2}$ hat Mipo $g(X)=X^3-2$ ~~(mod 3 keine Lsg: $1^2=-1$, $2^3=2$)~~ Quatsch,

da $g(X+1)=(X+1)(X^2+2X+1)-2 = X^3+2X^2+X-X^2+2X-1-2 = X^3-3X^2+3X-3$
irred. nach Eisenstein. (d.h. $\sqrt[3]{2}$ liefert überhaupt erstmal Erw. vom Grad 3...)
d.h. $\underbrace{\sqrt[3]{2}+1}_{u}$ hat Mipo X^3-3X^2+3X-3. $\Rightarrow$

i) $(\zeta_3-1)^2 = -3(\underbrace{\zeta_3-1}_{=\zeta_3}+1)$, d.h. $2v_L(\zeta_3-1)=v_L(3)=6$, also $v_L(\zeta_3-1)=3$.

ii) $u^3 = 3(u^2-u+1)$. d.h. $3v_L(u) = 6+v_L(u^2-u+1)$. Falls $v_L(u)=0$, so $\lightning$,
also $v_L(u)\neq 0$ und $v_L(u^2-u-1) = \min(v_L(u^2-u), v(1)) = 0$. $\rightarrow$ $V_L(u)=2$.
$\rightsquigarrow v(u^2-u)=v(u(u-1))\neq 0$

$\Rightarrow \pi_L := \frac{\zeta_3-1}{\sqrt[3]{2}+1}$ erfüllt $v_L(\pi_L)=1$. also Uniformisierende $\rightsquigarrow$

$G_{-1}=G=S_3 \supsetneq G_0 \supsetneq G_1 = \mathbb{Z}/3\mathbb{Z} \overset{\langle\sigma\rangle}{=} \supseteq G_2$ und $\sigma: \sqrt[3]{2}\mapsto \zeta_3\sqrt[3]{2}$, $\zeta_3\mapsto\zeta_3$. $\Rightarrow$

$\sigma(\pi_L)-\pi_L = \frac{\zeta_3-1}{\zeta_3\sqrt[3]{2}+1} - \frac{\zeta_3-1}{\sqrt[3]{2}+1} = \frac{(\zeta_3-1)(\sqrt[3]{2}+1)-(\zeta_3\sqrt[3]{2}+1)(\zeta_3-1)}{(\zeta_3\sqrt[3]{2}+1)(\sqrt[3]{2}+1)} = \frac{(\zeta_3-1)(\sqrt[3]{2}-\zeta_3\sqrt[3]{2})}{\dots} =$
$= \frac{(-\sqrt[3]{2})(\zeta_3-1)^2}{(\zeta_3\sqrt[3]{2}+1)(\sqrt[3]{2}+1)}$, d.h. $v_L(\sigma(\pi_L)-\pi_L) = 2v_L(\zeta_3-1) - v(\sqrt[3]{2}+1)\cdot 2 = 2\cdot 3 - 2\cdot 2 = 2$

D.h. $\sigma\in G_1\setminus G_2 = \{\sigma\in G_1 : v_L(\sigma(\pi_L)-\pi_L)\geq 3\}$.

(f) Bsp. K vollst diskret bew. Kp, $\operatorname{char} k = 0$, L/K endlich galoisch $\Rightarrow$
$R = G_1(L/K) = 1$, $I = G_0(L/K)$ zyklisch, denn: jede Erw. mit Restklassenkp-char $=0$ ist zahm verzweigt $\Rightarrow R=1$. Waterhin: $L=T[\sqrt[e]{\pi_T}]$ gal. impliziert, daß e-te EW in T liegen $\rightsquigarrow$ $\operatorname{Gal}(L/T)=G_0\cong\mathbb{Z}/e$ zyklisch

Bsp. • $K=\mathbb{Q}((t))$ mit diskr. Bew: $v(t)=1$. $\rightsquigarrow$ bel. Erw. v. der Form $E((t^{1/e}))$.
• $K=\mathbb{C}((t))$ $\rightsquigarrow$ Erw. v.d. Form $\mathbb{C}((t^{1/e}))$ $\rightsquigarrow$ alg. Abschluß $\overline{K}=\bigcup_{n\in\mathbb{N}}\mathbb{C}((t^{1/n}))$, d.h.
$\operatorname{Gal}(\overline{K}/K)=\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n$

(#) Wissen: • L/K unverzweigt $\Leftrightarrow$ $I_0=1$, d.h. $L^{I}=L$, da $0\to I\to G\to \operatorname{Gal}(k_L/k_K)\to 0$ ex.
• L/K zahm verzweigt $\Leftrightarrow R=1$, da R einzige p-Sylowgr. $0\to R\to G \to G/R\to 0$
d.h. $p\nmid [L:K]=\# G$

AZ 1 Üb. 21.12.15

A ganz abg. Intbereich, $K = \mathrm{Quot}\,A$, L/K sep., $B = \bar{A}^L$ ganzer Abschluß.
Ist $\omega = (\omega_1, \dots, \omega_n)$ K-Basis von L, so
$d(\omega) = \det((\sigma_i \omega_j))^2$, $\sigma_i : L \to \bar{K}$ die n versch. $\bar{K}$-Einb. von L.
Quadrat, damit $d(\omega) \in K$: denn ist $\sigma = \sigma_k$, so $\sigma\, d(\omega) = \det((\sigma \sigma_i \omega_j))^2$
$= (-1)^2 \det((\sigma_i \omega_j))^2$, da dies Spalten permutiert, d.h. $d(\omega)$ fest unter allen
$\sigma_i \leadsto d(\omega) \in K$.

Ist $A = \mathbb{Z}$, $L/\mathbb{Q}$ endlich, $B = \mathcal{O}_K$ wie oben, so $d_L = d(\mathcal{O}_L)$ Diskriminante von L
wobei hier zu beachten:

- d_L unabhängig von der Basiswahl, da eine andere $\mathbb{Z}$-Basis von $\mathcal{O}_K = B$, eine Übergangsmatrix T in $\mathbb{Z}$ hat $\leadsto$ $\det T = \pm 1$, d.h. $d(\omega') = (\det T)^2 d(\omega)$.
- ω ex. überhaupt erstmal für $\mathcal{O}_L$, da jeder e.e. B-UM ein freier A-Modul vom Rang $[L:\mathbb{Q}]$ ist, insbes. gilt das für $B = M$ selbst, d.h. wir können K-Basis von L in $\mathcal{O}_L$ wählen (auch direkt über Lokalisierung klar).
- $d_L \in \mathbb{Z}$: denn die Elt. (ω_j), die Basis bilden, sind in $\mathcal{O}_L$, also ganz über $\mathbb{Z}$ $\leadsto$ $\sigma_i \omega_j \in B'$ ganz über $\mathbb{Z}^{(*)}$ $\leadsto$ $\det((\sigma_i \omega_j))^2$ als Summe von Produkten ganzer Elt. wieder ganz, und in K $\leadsto$ $d_L \in \mathbb{Z}$.

Wie vergleicht sich diese Diskriminante mit der, die wir aus der Algebra kennen? D.h. die, die von einem Polynom kommt?

Erinnerung. $f \in K[X]$ normiert, $x_1, \dots, x_n$ die Nst. von f in $\bar{K}$ (können erstmal auch gleich sein.) $\leadsto$ $\mathrm{Disk}\, f := \prod_{i<j} (x_i - x_j)^2$ Diskriminante von f.

Ist nun etwa $f \in \mathbb{Z}[X]$ normiert, irred., so $L = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/f$ endlich$/\mathbb{Q}$ und α Nst von f. $\mathrm{Disk}(f) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$, wobei $\sigma_i : L \to \bar{\mathbb{Q}}$ die verschiedenen $\mathbb{Q}$-Einbettungen von L in $\bar{\mathbb{Q}}$. Andererseits ist $(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) =: \omega$ eine $\mathbb{Q}$-Basis von L ($n = [L:\mathbb{Q}] = \partial f$). $d(\omega) = \prod (\sigma_i(\alpha) - \sigma_j(\alpha))^2$ nach VL (Bsp 2 IV.1) mittels Vandermondscher Matrix, d.h. $d(\omega) = \mathrm{Disk}(f)$. Dies können wir auch als $\mathfrak{n} = \mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ schreiben (denn α ganz über $\mathbb{Z}$), d.h.
$d(\omega) = \mathrm{Disk}\, f = d(\mathfrak{n})$. I.a. gilt aber nicht $\mathbb{Z}[\alpha] = \mathcal{O}_L$ sodaß wg.
Satz 1: $\mathfrak{n} \subseteq \mathfrak{n}' \subseteq \mathcal{O}_L \subseteq L$: $d(\mathfrak{n}) = (\mathfrak{n}' : \mathfrak{n})^2 d(\mathfrak{n}')$ folgt

$$d_L \cdot [\mathcal{O}_L : \mathbb{Z}[\alpha]]^2 = d(\mathbb{Z}[\alpha]) = \mathrm{Disk}\, f.$$

Bsp. $D \in \mathbb{Z}$, $D \neq 0, 1$, quadratfrei, $L = \mathbb{Q}(\sqrt{D})$, und falls $D \equiv 1$ (4)
so $(1, \frac{1+\sqrt{D}}{2})$ Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$, d.h. $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_L$, aber $\neq$, da $\frac{1}{2} \notin \mathbb{Z}[\sqrt{D}]$. Falls $D \equiv 2, 3$ (4), so $(1, \sqrt{D})$ Ganzheitsbasis von $\mathcal{O}_L$, d.h.
(vgl. Algebra 2, Aufg. 2)

(*) wobei wir zu einer normalen Hülle $L'/L/\mathbb{Q}$ übergehen $\leadsto$ sei B' ganzer Abschluß von $\mathbb{Z}$ in L', d.h. $B \subseteq B'$.

$\mathbb{Z}[\sqrt{D}] = \mathcal{O}_L$. Insbes. können wir hier d_L über disk f berechnen:
Im ersten Fall gilt Disk $f = (\sqrt{D}+\sqrt{D})^2 = 4D$ und wenn
$\omega = (\omega_1, \omega_2) = (1, \frac{1+\sqrt{D}}{2})$, so $1 = 1\cdot\omega_1$, $\sqrt{D} = 2\cdot\omega_2 - 1\cdot\omega_1 \rightsquigarrow \omega' = (1,\sqrt{D})^t = \underbrace{\begin{pmatrix} 1 & -1 \\ & 2 \end{pmatrix}}_{=T} \omega^t$
und $(\mathcal{O}_L : \mathbb{Z}[\sqrt{D}])^2 = |\det T|^2 = 4$, d.h. $d_L = D$.
Im zweiten Fall: $\mathcal{O}_L = \mathbb{Z}[\sqrt{D}]$, d.h. $d_L = 4D$.

Dedekindringe. ~~A~~ A ganzabg., noeth. Intbereich der Dim 1
$\Leftrightarrow$ A noeth, integer, $\mathfrak{p} \neq 0$ prim: $A_\mathfrak{p}$ DBR (nach Algebra 2)
Wichtigste Quelle von Dedekindringen: A Dedekind (z.B. $A = \mathbb{Z}$ oder allg. ~~A~~ HIR)
so B auch wieder (B wie vorher).
"Anderer Zugang" von geometrischer Seite mit folgendem (eigtl. genau das gleiche)
Bsp $A = \mathbb{C}[X]$, $B = \mathbb{C}[X,Y]/(\underbrace{X^2+Y^2-1}_{f})$, $f = X^2 + (Y-1)(Y+1) \in \mathbb{C}[Y][X]$ irred.
nach Eisenstein, aber B als ganzen Abschluß von A in $\mathbb{C}(Y)[X]/f = L$
zu erkennen? Schwierig! Geom. Methoden helfen.
B auf jeden Fall noethersch, integer ~~[illegible]~~ (f irred; $\mathbb{C}[X,Y]$ faktoriell) (über die Parametrisierung
des Einheitskreises zu sehen). $B_\mathfrak{p}$ DBR? Dazu auch geom. Krit.:
(R,m) lokaler noeth. Ring heißt regulär $\Leftrightarrow$ $\dim R = n$ mit $m = (b_1, \dots, b_n)$ minimal, $b_i \in R$.
$\Leftrightarrow$ $\dim_{R/m} m/m^2 = n$

D.h. R DBR $\Leftrightarrow$ R regulär lokal von Dim 1: „$\Rightarrow$" R DBR, so $m = (x) = \dim R = 1$. ✓
„$\Leftarrow$": $\dim R = 1 \overset{!}{=} (x) = m$, d.h. m Hauptideal. $0 \neq y \in R$, so $y \in (x^n) \setminus (x^{n+1})$
(irgendein n ex. auf jeden Fall), sonst $y \in \bigcap (x^n)$, d.h. $(y) \subseteq (yx^{-1}) \subsetneq (yx^{-2}) \dots$
echt aufst. ↯ zu noethersch. $\rightsquigarrow y = a\cdot x^n$, $a \in R^\times$ (sonst $a \in (x)$ ↯),
$v(y) = n$ ist diskrete Bew.
(V dim 1) ~~[illegible]~~
Die Regularitätsbed. ist an "Glattheit" von B gekoppelt: $\mathfrak{p} \subseteq B$ ~~[illegible]~~ (–) prim & $\mathfrak{p} \neq 0$
$(x,y) \in \mathbb{C}^2$: $f(x,y) = 0$, da diese gerade den abg. Pkten in der irred. Varietät V zu B
entsprechen. Unter dieser Entsprechung: $B_\mathfrak{p}$ reg. lokal von Dim 1 $\Leftrightarrow$
V glatt an der Stelle (x,y) :$\Leftrightarrow$ $(\partial f/\partial x, \partial f/\partial y)$ hat vollen Rang an (x,y):
$$\overset{\shortparallel}{(2x, 2y)} \quad \text{nur bei } (x,y) = (0,0) \text{ nicht}$$
vollen Rang, aber $(0,0) \notin V$, da $0 \neq 1$.
Erklärungen: R noeth $\rightsquigarrow \dim R[X_1,\dots,X_n] = \dim R + n \rightsquigarrow \dim \mathbb{C}[X,Y] = 2$, d.h.
$\dim B = 1$, da ≤ 1 (Ketten entsprechen Ketten, die (f) umfassen) und
$(X-1, Y) \supseteq (f)$ maximal
z.B. $\mathbb{Z}[X,Y]/(f)$ hat Dim 2, also kein Dedekindring $(X-1,Y,p) \supseteq (X-1,Y) \supseteq (f)$,
p irgendeine Primzahl.

Az 7 üb. 11.1.16.

A Dedekindring (ganz abg. noeth. Intbereich der Dim 1), $k = \operatorname{Quot} A$, L/k sep., $B = \bar{A}^L$ = ganzer Abschluß von A in L. Da B/A ganz: $\mathfrak{P} \subseteq B$ max, so $\mathfrak{p} = A \cap \mathfrak{P} \subseteq A$ maximal, $\mathfrak{P} | \mathfrak{p}$

$f_\mathfrak{P} = [B/\mathfrak{P} : A/\mathfrak{p}]$ Trägheitsgrad von $\mathfrak{P}$. wissen: $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$ eind. Primfaktorzerlegung $e_\mathfrak{P} = v_\mathfrak{P}(\mathfrak{p}B)$ Verzweigungsindex von $\mathfrak{P}$

<u>Fund. Gleichung</u> $n = [L:k]$, $n = \sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}$.

<u>Bsp.</u> A ~~...~~ Ded. ring, $\mathfrak{p} \in \operatorname{Spec}^1 A$, $\rightsquigarrow A_\mathfrak{p}$ DBR, also ebenfalls Dedekindring, $\mathfrak{P}|\mathfrak{p}$ in B und $B_\mathfrak{P}$ DBR, endliche Ringerw. von $A_\mathfrak{p}$ (da $\operatorname{Quot} B_\mathfrak{P} = \operatorname{Quot} B = L$ endl. über $k = \operatorname{Quot} A_\mathfrak{p} = \operatorname{Quot} A$) ~~...~~: $\varprojlim B_\mathfrak{P}/\mathfrak{P}^i B_\mathfrak{P} = \hat{B}_\mathfrak{P}$ ist dann vollst. DBR mit max. Ideal $\mathfrak{P}\hat{B}_\mathfrak{P}$, ebenso $\hat{A}_\mathfrak{p} = \varprojlim A_\mathfrak{p}/\mathfrak{p}^i A_\mathfrak{p}$ und Restklassenkp. $\hat{B}_\mathfrak{P}/\mathfrak{P}\hat{B}_\mathfrak{P} = B_\mathfrak{P}/\mathfrak{P}B_\mathfrak{P} = B/\mathfrak{P}$, ebenso $\hat{A}_\mathfrak{p}/\mathfrak{p}\hat{A}_\mathfrak{p} = A/\mathfrak{p}$ (z.B.: $A = \mathbb{Z}$, $\mathfrak{p} = (p)$ $\rightsquigarrow \hat{A}_\mathfrak{p} = \mathbb{Z}_p$, $A_\mathfrak{p} = \mathbb{Z}_{(p)}$). D.h. bezeichnen wir mit w die disk. Bew. auf $\hat{B}_\mathfrak{P}$ geg. durch $\mathfrak{P}$, mit v die disk. Bew. auf $\hat{A}_\mathfrak{p}$ geg. durch $\mathfrak{p}$, so gilt einerseits nach obigem: $\mathfrak{p}\hat{B}_\mathfrak{P} = (\mathfrak{P}\hat{B}_\mathfrak{P})^{e_\mathfrak{P}}$ (da nur ein max. Ideal in $\hat{B}_\mathfrak{P}$), andererseits $e = e(w/v) = e_{L_w/k_v} = (w(L_w^\times) : v(k_v^\times))$, d.h. mit $v(\pi) = \mathfrak{p}$, $\mathfrak{P} = \Pi$, s.d. $\pi = \varepsilon \cdot \Pi^{e(w|v)} \iff \mathfrak{p}\hat{B}_\mathfrak{P} = (\mathfrak{P}\hat{B}_\mathfrak{P})^{e(w|v)}$ d.h. $e(w|v) = e_\mathfrak{P}$, und analog $f = f(w|v) = f_\mathfrak{P} = [B/\mathfrak{P} : A/\mathfrak{p}]$. $\rightsquigarrow$ $n = [L_w : k_v] = e \cdot f$

Vgl. damit auch die Begriffe: unverzweigt, voll verzweigt.

<u>Wichtiges Problem</u>: Wollen obige Zerlegung für $\mathfrak{p}\mathcal{O}$ berechnen, z.B. über folg. Satz: $\alpha \in L$ primitives Elt, aber auch ganz (gilt, da $\alpha = \frac{b}{a}$, $b \in \mathcal{O}_L$, $a \in \mathcal{O}_k$) über $\mathcal{O}_k$. Es gelte $\mathcal{O}_L = \mathcal{O}_k[\alpha]$, $p = \operatorname{Mipo}_k \alpha$. Sei $\mathfrak{p} \in \operatorname{Spec}^1 \mathcal{O}_k$. Sei $\bar{p}(X) = \bar{p}_1(X)^{e_1} \cdots \bar{p}_r(X)^{e_r}$ Zerlegung von $p(X)$ mod $\mathfrak{p}$ mit $p_i(X) \in \mathcal{O}_k[X]$ normiert $\rightsquigarrow$ $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + p_i(\alpha)\mathcal{O}_L$ die verschiedenen Primideale über $\mathfrak{p}$ in $\mathcal{O}_L$, $f_i = \partial \bar{p}_i(X)$, $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$

<u>Bew.idee</u>. $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \xleftarrow{\sim} \mathcal{O}_k/\mathfrak{p}[X]/(\bar{p})$, $\alpha \mapsfrom X$, da $\mathcal{O}_L = \mathcal{O}_k[\alpha] = \mathcal{O}_k[X]/p$

$\cong \prod_i \mathcal{O}_k/\mathfrak{p}[X]/(\bar{p}_i(X))^{e_i}$

D.h. die Primideale über $\mathfrak{p}$ in $\mathcal{O}_L$ sind v.d. Form $\mathfrak{p}\mathcal{O}_L + p_i(\alpha) \cdot \mathcal{O}_L$

Eine Frage ist also: wann ist $\mathcal{O}_L = \mathcal{O}_K[\alpha]$? (Wenn das nicht gilt, kann man obigen Satz immer noch modifizieren und Zerlegungen für Primideale, die teilerfremd zum Führer sind, durchführen, vgl. Bem. 29).

Bsp i) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, In VL schon bek.: $\mathcal{O}_L \overset{\text{"}\supseteq\text{"}}{=} \mathbb{Z}[\sqrt[3]{2}] =: \mathfrak{a}$. Offensichtlich "$\supseteq$" ✓, da $\sqrt[3]{2}$ ganz. $d(\mathfrak{a})$: $\mathfrak{a}$ hat Basis $\omega = (1, \sqrt[3]{2}, \sqrt[3]{4})$, $d(\mathfrak{a}) = d(\omega)$

$$= \det(\mathrm{Spur}_{L/K}(\omega_i\omega_j)) = \begin{vmatrix} \mathrm{Tr}\,1 & \mathrm{Tr}\sqrt[3]{2} & \mathrm{Tr}\sqrt[3]{2^2} \\ \mathrm{Tr}\sqrt[3]{2} & \mathrm{Tr}\sqrt[3]{2^2} & \mathrm{Tr}\,2 \\ \mathrm{Tr}\sqrt[3]{2^2} & \mathrm{Tr}\,2 & 2\cdot\mathrm{Tr}\sqrt[3]{2} \end{vmatrix} = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3\cdot 2 \\ 0 & 3\cdot 2 & 0 \end{vmatrix} = -27\cdot 2^2 = -3^3\cdot 2^2$$

Damit: $d(\mathfrak{a}) = -3^3\cdot 2^2 = d(\mathcal{O}_L)\cdot \underbrace{(\mathcal{O}_L : \mathfrak{a})^2}_{\in\mathbb{Z}}$. Wenn $\mathfrak{a} \neq \mathcal{O}_L$, so $2 \mid (\mathcal{O}_L : \mathfrak{a})$ oder $3 \mid$

i) $2 \mid (\mathcal{O}_L : \mathfrak{a})$: $\leadsto \exists\, a \in \mathcal{O}_L \setminus \mathfrak{a}$: $2a \in \mathfrak{a}$. $2 = \sqrt[3]{2}^3$. $2 \mid x \in \mathbb{Z} \iff \sqrt[3]{2} \mid x$ in $\mathcal{O}_L$. Sei $2a = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$, mod $\sqrt[3]{2}$ $\Rightarrow$ $a_0 \equiv 0$ $(\sqrt[3]{2})$ $\leadsto$ $2 \mid a_0$. $2a - 2a_0' \equiv 0 \equiv a_1\sqrt[3]{2} \bmod \sqrt[3]{4}$ $\Leftarrow$, $a_1\sqrt[3]{2} = c\cdot(\sqrt[3]{2})^2$ $\Rightarrow$ $\sqrt[3]{2} \mid a_1 \Rightarrow 2 \mid a_1$ $\leadsto$ $2a \equiv 0 \equiv a_2\sqrt[3]{4} \bmod 2$ $\leadsto$ $2 \mid a_2$ $\leadsto$ $2a \in 2\mathbb{Z}[\sqrt[3]{2}]$ $\leadsto$ $a \in \mathfrak{a}$ ↯.

ii) $3 \mid (\mathcal{O}_L : \mathfrak{a})$: Beh: $3 = (1+\sqrt[3]{2})^3\cdot u$, $u \in \mathcal{O}_L^\times$. $(1+\sqrt[3]{2})^3 = 1 + 3\sqrt[3]{2} + 3\sqrt[3]{4} + 2 = 3(1+\sqrt[3]{2}+\sqrt[3]{4})$. $N(1+\sqrt[3]{2}) = 3$ $\leadsto$ $N((1+\sqrt[3]{2})^3) = 3^3 = N(3)$ $\leadsto$ $(1+\sqrt[3]{2}+\sqrt[3]{4}) = u \in \mathcal{O}_L^\times$ $\Rightarrow$ $a \in \mathbb{Z}$, $3 \mid a \iff (1+\sqrt[3]{2}) \mid a$ in $\mathcal{O}_L$. Sei also $a \in \mathcal{O}_L \setminus \mathfrak{a}$ mit $3a \in \mathfrak{a}$. $3a = a_0 + a_1(1+\sqrt[3]{2}) + a_2(1+\sqrt[3]{2})$ (da $\mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z}[1+\sqrt[3]{2}]$). Analog: modulo $(1+\sqrt[3]{2})^i$ liefert $a \in \mathfrak{a}$ ↯.

b) ζ_p prim. p-te EW, so $\mathcal{O}_L = \mathbb{Z}[\zeta_p]$ für $L = \mathbb{Q}(\zeta_p)/\mathbb{Q}$. Bew später!

Bsp i) $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$, $p = 3$ $\leadsto$ ~~da~~ Dann: $X^3 - 2 \equiv (X+1)^3 \bmod 3$ $\leadsto$ $3\mathbb{Z}[\sqrt[3]{2}] = \mathfrak{P}^3$ total verzweigt.

ii) $L = \mathbb{Q}(\zeta_5)$, $K = \mathbb{Q}$, $p = 11$. $\mathbb{Z}/11$ enthält alle 10-ten EW d.h. alle 5-ten ebenso, d.h. $\mathrm{Mipo}_{\mathbb{Q}}\zeta_5$ zerfällt in $\mathbb{Z}/11$ in LF. $\leadsto$ $11\mathcal{O}_L = \mathfrak{P}_1\cdots\mathfrak{P}_4$. total zerlegt.

iii) $A = \mathbb{Q}[X]$, $B = A[Y]/f$, $f = Y^3 + X^2 + 1$ irred. definiert glatte Kurve, d.h. B ganzabg. (vgl. letzte Üb.)

$B/XB = \mathbb{Q}[Y]/\underbrace{Y^3+1}_{=(Y+1)(Y^2-Y+1)} = K_1 \times K_2$ zwei Kp. $\leadsto$ $XB = \mathfrak{P}_1\cdot\mathfrak{P}_2$

$B/(X-1)B = \mathbb{Q}[Y]/Y^3$ $\leadsto$ $(X-1)B = \mathfrak{P}^3$

$B/(X^2+5) = \mathbb{Q}[Y]/\underset{\nwarrow\,\text{irred.}}{Y^3-4}$ $\leadsto$ $(X^2-5)B = \mathfrak{P}^1$ "träge"

$(\partial f/\partial x, \partial f/\partial y) = (2X, 3Y)$
nur bei $(0,0)$ nicht vollen Rang, aber $f(0,0) \neq 0$.

AZ1 Üb. 18.1.16. (1)

$K/\mathbb{Q}$ endlich $\rightsquigarrow$ O_K Dedekindring. Haben eind. Zerlegung für gebrochene Ideale $\mathfrak{a} \in I(O_K)$ (d.h. $\exists\, d \in K$: $d\mathfrak{a} \subseteq O_K$) in Primideale.
Die gebrochenen Ideale $P(O_K) = \{(x) \mid x \in K^\times\}$ sind UG von $I(O_K)$,
$Cl(O_K) = I(O_K)/P(O_K)$ Idealklassengruppe, abelsch! Operation ist Idealmultipl.

Mit Hilfe der Gittertheorie werden wir sehen:
i) $Cl(O_K)$ ist endlich
ii) Sind $n = [K:\mathbb{Q}]$ und r_2 die Anzahl der Paare der komplex konj. Einbettungen $\sigma, \bar{\sigma}: K \hookrightarrow \mathbb{C}$, so gilt mit $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|} =: \mu$ (d_K Diskriminante von K)
und zu jeder Klasse X von $Cl(O_K)$ ex. ein ganzes Ideal $\mathfrak{b} \subseteq O_K$ mit $\bar{\mathfrak{b}} = X$ und $\underset{\substack{\| \\ d(\mathfrak{b})}}{N(\mathfrak{b})} \leq \mu$.

Bsp. 1) $K = \mathbb{Q}(\sqrt{-61})$, $-61 \equiv 3\ (4)$ $\rightsquigarrow$ $O_K = \mathbb{Z}[\sqrt{-61}]$. Sei $\mathfrak{a} = (2, 3+\sqrt{-61}) \subseteq O_K$.
Beh: $\mathfrak{a}^2 = (2)$, d.h. ord $\mathfrak{a} \mid 2$ (Gilt $O_K/\mathfrak{a} = 1$?) Zeige dafür:
$(3+\sqrt{-61})^2 = 9 + 2\cdot 3 \cdot \sqrt{-61} + 61 = -52 + 2\cdot 3\sqrt{-61} = 2\cdot x$ $\Rightarrow$ Beh.

2) $K = \mathbb{Q}(\sqrt{-14})$. $n = 2$, $r_2 = 1$ (da $\sqrt{-14} \in \mathbb{C}\setminus\mathbb{R}$) $\rightsquigarrow$ $\mu = \frac{2}{\pi}\sqrt{|d_K|}$ $\quad -14 \equiv 2\ (4)$
d.h. $d_K = 4\cdot(-14) = -56$, also $\mu \approx 4.7$ $\Rightarrow$ $Cl(O_K)$ erzeugt von Primidealen $\mathfrak{p}$ mit $d(\mathfrak{p}) = 2, 3$. D.h. wir suchen die Primideale in O_K über 2 und 3:

2: $X^2 + 14 \equiv X^2\ (2)$, also $(2) = P_2^2$
3: $X^2 + 14 \equiv X^2 + 2\ (3) \equiv (X-1)(X+1)$, also $(3) = P_3 \cdot P_3'$
$\Bigg\} \Rightarrow$ $P_2 \sim P_2^{-1}$, $P_3' \sim P_3^{-1}$, also $Cl(O_K) = \langle P_2, P_3 \rangle$.

Wären P_2, P_3 Hauptideale, so $P_2 = (\underset{\substack{\| \\ a+b\sqrt{-14}}}{x_2})$, $P_3 = (\underset{\substack{\| \\ a'+b'\sqrt{-14}}}{x_3})$, also $d(P_2) \overset{\text{Satz 20}}{=} |N(x_2)| = a^2 + 14b^2 \overset{!}{=} 2$
$d(P_3) = |N(x_3)| = a'^2 + 14b'^2 \overset{!}{=} 3$
mit $a, b, \ldots \in \mathbb{Z}$. Diese Gleichungen haben aber keine Lsg in $\mathbb{Z}^2$. (da $b = b' = 0$ $\rightsquigarrow$ ↯)
Also Elt. $\neq 1$ in $Cl(O_K)$. Betrachte $\mathfrak{a} = (2+\sqrt{-14})$. $d(\mathfrak{a}) = |N(2+\sqrt{-14})|$
$= 18 = 2\cdot 3^2$ $\overset{\text{entw.}}{\Rightarrow}$ $P_3 \mid \mathfrak{a}$ oder $P_3' \mid \mathfrak{a}$. Sonst $\underset{\substack{\| \\ (3)}}{P_3 P_3'} \mid \mathfrak{a}$, d.h. $2 + \sqrt{-14} = 3\cdot x$
$x \in O_K$, geht aber nicht. Sei P_3 das Primid. über 3, das $\mathfrak{a}$ teilt. $\Rightarrow$ $\mathfrak{a} = P_2 P_3^2$, also $P_2 P_3^2 \sim 1$ also $P_3^2 \sim P_2^{-1} \sim P_2$
also $Cl(O_K) = \langle P_3 \rangle$ also zyklisch der Ordnung 4, da $P_2 \not\sim 1$, $P_2^2 \sim 1$
und $P_3^2 \sim P_2$.

3) $K = \mathbb{Q}(\sqrt{-23})$, $-23 \equiv 1 \ (4)$, also $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{-23}}{2}$. Statt X^2+23 betrachten wir also $f(X) = X^2 - X + \frac{1}{4}(1-d)$, $d = -23$, d.h. $|d_K| = 23$

$X^2 - X + 6$. $\mu = \frac{2}{\pi}\sqrt{|d_K|} \leq 4$ (≈ 3.05). D.h. $Cl(\mathcal{O}_K)$ erzeugt von Primidealen $\mathfrak{P}$ mit $d(\mathfrak{P}) = 2, 3$. $f \equiv X(X-1) \ (2, 3)$ d.h. $(2) = \mathfrak{P}_2\mathfrak{P}_2'$

$(3) = \mathfrak{P}_3\mathfrak{P}_3'$ konkret z.B. $\mathfrak{P}_2 = (2, \cancel{\ } \frac{1+\sqrt{-23}}{2})$, $\mathfrak{P}_2' = (2, \frac{\sqrt{-23}}{2} - \frac{1}{2})$, analog für $\mathfrak{P}_3, \mathfrak{P}_3'$. Es gilt: $N(\frac{1+\sqrt{-23}}{2}) = (\frac{1+\sqrt{-23}}{2})(\frac{1-\sqrt{-23}}{2}) = 6 = 2 \cdot 3$, d.h.

o.E. $(\frac{1+\sqrt{-23}}{2}) = \mathfrak{P}_2\mathfrak{P}_3$, also $\mathfrak{P}_3 \sim \mathfrak{P}_2^{-1}$. Weiterhin $N(1 + \frac{1+\sqrt{-23}}{2}) = 8 = 2^3$

Da $Gal(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle$ und ~~σ~~ transitiv auf Idealen über p operiert, gilt $\sigma(\mathfrak{P}_2) = \mathfrak{P}_2'$. Nun ist $(\underbrace{1+\frac{1+\sqrt{-23}}{2}}_{x})(\underbrace{1+\frac{1+\sqrt{-23}}{2}}_{\sigma(x)}) = (2^3) = \mathfrak{P}_2^3\mathfrak{P}_2'^3$

Wäre $\mathfrak{P}_2 \sim 1$, so $\mathfrak{P}_2 = (y) = (a+b\alpha)$, d.h. $d(\mathfrak{P}_2) = |N(y)| = 2 = (a+b\alpha)(a+b\sigma(\alpha))$

$= (a + b\frac{1+\sqrt{-23}}{2})(a + b\frac{1-\sqrt{-23}}{2}) = a^2 + ab + 6b^2$. Kann zeigen: hat keine Lsg in $\mathbb{Z}^2$. Daher kann (x) nicht gleich $\mathfrak{P}_2\mathfrak{P}_2'^2$ oder $\mathfrak{P}_2^2\mathfrak{P}_2'$ sein, da diese Elt ~ 1 in $Cl(\mathcal{O}_K)$ $\Rightarrow$ o.E. $(x) = \mathfrak{P}_2^3$. Wg. $\mathfrak{P}_2 \not\sim 1$ gilt also $Cl(\mathcal{O}_K) = \langle\mathfrak{P}_2\rangle = \mathbb{Z}/3\mathbb{Z}$, da $\mathfrak{P}_3 \sim \mathfrak{P}_2^{-1}$.

Haben Zerlegungsgruppe $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ bzw. Trägheitsgruppe $I_{\mathfrak{P}} = \ker(G_{\mathfrak{P}} \to Aut_{B/p}(B/\mathfrak{P}))$ kennen gelernt: z.B. $A = \mathbb{Z}$, $B = \mathcal{O}_K$, $K/\mathbb{Q}$ endlich, $\mathfrak{P} \mid (p)$, $p \in \mathbb{Z}$ prim. Wie aus letzter Üb, (p) bzw. $\mathfrak{P}$ induzieren nicht-arch. diskrete Bew. v auf bzw. w auf $\mathbb{Q}$ bzw. K via z.B. $B \hookrightarrow B_{\mathfrak{P}} \hookrightarrow DBR$. Sei $K_w/\mathbb{Q}_v$ die zug. Vervollständigung $\rightsquigarrow$ Erw. lokaler Kp. VL sagt dann,

$G_{\mathfrak{P}} = G_{\mathfrak{P}}(K/\mathbb{Q}) = G(K_w/\mathbb{Q}_p)$, $I_{\mathfrak{P}}(K/\mathbb{Q}) = I(K_w/\mathbb{Q}_p)$.

---

4) Lsg. von $Y^2 = X^3 - 51$

AZ 1 Üb. 18.1.16. ①

$k = \mathbb{Q}(\sqrt{-51})$

Lsg von $Y^2 = X^3 - 51$ in $\mathbb{Z}^2$: • X ungerade, sonst

$Y^2 \equiv -51 \equiv 5 \ (8)$ kein Quadrat, ↯. • $ggT(y, 51) = 1$, sonst $p=3 \mid y, p=17 \mid y$

$\leadsto p \mid x^3 = y^2 + 51 \leadsto p^2 \mid x^3, y^2$ ↯ zu $p^2 \nmid 51$.

$\alpha = \frac{1+\sqrt{-51}}{2}$, $f(X) = X^2 - X + 13$ Mipo von α über $\mathbb{Q}$. $\leadsto$

$x^3 = y^2 + 51 = (y - \sqrt{-51})(y + \sqrt{-51}) = (y - (2\alpha - 1))(y + (2\alpha - 1))$ in $\mathcal{O}_K = \mathbb{Z}[\alpha]$,

Beh. $\underbrace{(y + \sqrt{-51})}_{\mathfrak{a}} + \underbrace{(y - \sqrt{-51})}_{\mathfrak{b}} = \mathcal{O}_K$. Sonst $\exists\, \mathfrak{p} \mid \mathfrak{a}, \mathfrak{b} \leadsto y \pm \sqrt{-51} \in \mathfrak{p} \leadsto$

$2\sqrt{-51} \in \mathfrak{p}$, d.h. $\mathfrak{p} \mid (2)(\sqrt{-51})$, also $\mathfrak{p} \mid (2)$ oder $\mathfrak{p} \mid (\sqrt{-51})$.

$\mathcal{O}_K = \mathbb{Z}[X]/(X^2 + X + 13)$ in $(2) \subseteq \mathcal{O}_K$ prim, da $\mathcal{O}_K/(2) = \mathbb{F}_2[X]/(X^2 - X + 1)$

und $X^2 - X + 1$ irred. in $\mathbb{F}_2[X]$ $\Rightarrow$ falls $\mathfrak{p} \mid (2)$, so $\mathfrak{p} = (2)$, aber auch

$x^3 = (y + \sqrt{-51})(y - \sqrt{-51}) \in \mathfrak{p} \cap \mathbb{Z}$ ungerade $\leadsto ggT(x^3, 2) = 1 \in \mathfrak{p}$ ↯.

Falls $\mathfrak{p} \mid (\sqrt{-51}) \leadsto \sqrt{-51} \in \mathfrak{p}$, also $51 \in \mathfrak{p}$, aber $y + \sqrt{-51} \in \mathfrak{p} \leadsto y \in \mathfrak{p}$

und $ggT(y, 51) = 1 \in \mathfrak{p}$, ↯.

Da $\mathfrak{a} \cdot \mathfrak{b} = (x^3)$ und $\mathfrak{a}, \mathfrak{b}$ relat. prim $\Rightarrow$ alle Primideale in $\mathfrak{a}, \mathfrak{b}$

kommen mit Vielfachheit vor, die durch 3 teilbar ist $\Rightarrow$

$\mathfrak{a} = \mathfrak{a}'^3$, $\mathfrak{b} = \mathfrak{b}'^3$, $\mathfrak{a}', \mathfrak{b}' \subseteq \mathcal{O}_K$ Ideale. Kann zeigen: $Cl(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$

$\leadsto \mathfrak{a}' \sim 1$, $\mathfrak{b}' \sim 1$, also $\mathfrak{a}' = (a)$, $\mathfrak{b}' = (b)$, d.h. $y + \sqrt{-51} = u a^3$, $y - \sqrt{-51} = v b^3$,

$u, v \in \mathcal{O}_K^\times$. Kann weiter zeigen: $\mathcal{O}_K^\times = \{\pm 1\}$ (vgl. Berechn. in $\mathbb{Z}[i]$).

$\leadsto y + \sqrt{-51}$ ist dritte Wurzel in $\mathcal{O}_K$. $\leadsto y + \sqrt{-51} = (y-1) + 2\alpha =$

$(r + s\alpha)^3 = r^3 + 39 rs^2 - 13 s^3) + \underbrace{3s(r^2 + rs - 4s^2)}_{\text{hat auf jeden Fall } 3 \mid \ldots}\alpha$ (da $\alpha^2 - \alpha + 13 = 0$)

, aber links steht 2α, ↯.