Vorlesung Zahlentheorie I (Algebraische ZT) WiSe '22/'23, hhu
K. Halupczok

Z2: Kummersches Lemma

Stichworte: Beweis des Kummerschen Lemmas

2.1. **Einleitung:** Das Kummersche Lemma 1.14 ist wesentlicher Baustein zum Beweis von Satz 1.16, dem Fermatschen Satz für Exponenten $3 < p \leq 19$, $p \nmid xyz$. Nach diesem Lemma ist $\frac{u}{\bar u}$ eine Potenz von $\omega = e^{2\pi i/p}$, wenn $u \in \mathbb{Z}[\omega]^\times$ ist.

Beweis des Kummerschen Lemmas 1.14: Für jede Einheit $u \in \mathbb{Z}[\omega]^\times$, $\omega = e^{2\pi i/p}$, ist $\frac{u}{\bar u}$ eine Potenz von ω. ($p \geq 3$ prim)

⌈Mit 2.2 (i) und 2.3 (ii).⌋

2.2. (i) **Beh.:** Es gibt ein $k \in \mathbb{Z}$ mit $\frac{u}{\bar u} = \pm \omega^k$:

Bew.: Es gilt: $u \in \mathbb{Z}[\omega] \Rightarrow \bar u \in \mathbb{Z}[\omega]$. Sei $u = \sum_{k=0}^{p-2} a_k \omega^k$.

Somit: $u \in \mathbb{Z}[\omega]^\times \overset{!}{\Rightarrow} \bar u \in \mathbb{Z}[\omega]^\times$. ⌈$\frac{1}{u} \in \mathbb{Z}[\omega] \Rightarrow \frac{1}{\bar u} \in \mathbb{Z}[\omega]$⌋

Nun ist $\left|\frac{u}{\bar u}\right| = 1$. Sei $\sigma \in \mathrm{Aut}(\mathbb{Q}(\omega))$. Dann folgt

$$\sigma\left(\frac{u}{\bar u}\right) = \frac{\sigma(u)}{\sigma(\bar u)} \overset{!}{=} \frac{\sigma(u)}{\overline{\sigma(u)}}, \text{ also auch } \left|\sigma\left(\frac{u}{\bar u}\right)\right| = 1.$$

← σ bildet p-te EW auf p-te EW ab

⌈Sei $\sigma(\omega) \overset{!}{=} \omega^l$, dann ist $\sigma(\bar u) = \sum_{k=0}^{p-2} a_k \sigma(\omega)^{p-k} = \sum_{k=0}^{p-2} a_k \omega^{(p-k)l}$

$$= \sum_{k=0}^{p-2} a_k \omega^{-kl} = \sum_{k=0}^{p-2} a_k \overline{\omega^{kl}} = \overline{\sum_{k=0}^{p-2} a_k \sigma(\omega)^k} = \overline{\sigma(u)}.$$ ⌋

Nach Zusatz 2.4 ist dann $\frac{u}{\bar u}$ eine Einheitswurzel.

Wegen Kor. 5.5 gibt es dann ein $k \in \mathbb{N}$ mit $\frac{u}{\bar u} = (\omega^{\frac12})^k \overset{!}{=} -(\omega^{\frac12})^{k+p}$, $\omega^{\frac12} = e^{\frac{\pi i}{p}}$.

⌈D.h. die EW in $\mathbb{Q}(e^{2\pi i/m})$ sind die m-ten, falls $2 \mid m$, und die $2m$-ten, falls $2 \nmid m$.⌋ Kor. 5.5

⌈Es ist $(\omega^{\frac12})^p = (e^{\frac{\pi i}{p}})^p \underset{\text{deM.}}{=} e^{\frac{\pi i}{p}\cdot p} = e^{\pi i} = -1$

sowie $-(\omega^{\frac12})^k = (\omega^{\frac12})^p \cdot (\omega^{\frac12})^k = (\omega^{\frac12})^{p+k}$ ✓. [deMoivre: $(e^z)^k = e^{z\cdot k}$ für $z \in \mathbb{C}$, $k \in \mathbb{N}_0$]

Dabei ist dann $\frac{k}{2} \in \mathbb{Z}$ oder $\frac{k+p}{2} \in \mathbb{Z}$. Es folgt (i).

2.3 (ii) **Beh.:** Es ist $\frac{\mu}{\bar\mu} = +\omega^k$:

Bew: Sonst ist $\frac{\mu}{\bar\mu} = -\omega^k$, und $\left(\frac{\mu}{\bar\mu}\right)^p = -\omega^{kp} = -1$, also $\mu^p = -\bar\mu^p$.

Man betrachte dies in $\mathbb{F}_p(\omega)$.

Anwenden des Frobeniusmorphismus $x \mapsto x^p$ auf $\mu = \sum a_k \omega^k \in \mathbb{F}_p(\omega)$ liefert $\mu^p = (\sum a_k \omega^k)^p \equiv \sum a_k^p \omega^{kp} \equiv \sum a_k \ (p)$, da $x^p = x$ in $\mathbb{F}_p$,

und ebenso $\bar\mu^p \equiv \sum a_k \ (p)$.

Somit ist $\bar\mu^p \equiv \mu^p \ (p)$ und $\bar\mu^p \equiv -\mu^p \ (p)$,

beides ergibt $\mu^p \equiv 0 \ (p)$, d.h. $p \mid \mu^p$ in $\mathbb{Z}[\omega]$.

Da aber $\mu \in \mathbb{Z}[\omega]^\times$, ist dies ein ↯. □

2.4 **Zusatz:** Sei x ganzalgebraisch (s. Z3.15) und so, dass alle Konjugierten von x den Absolutbetrag 1 haben. Dann ist x eine Einheitswurzel.

Bew.: (i) **Beh.:** Hat x Grad n, so ist der i-te Koeff. des Mipos von $x|\mathbb{Q}$ absolut $\leq \binom{n}{i}$:

Bew.: Sei $f(T) = T^n + a_{n-1}T^{n-1} + \dots + a_0$ das Mipo von $x|\mathbb{Q}$, mit $a_i \in \mathbb{Z}$, vgl. Lemma Z3.20. Ferner ist $f(T) = \prod_{i=1}^{n} (T - x_i)$, $x_1 := x$, mit den Konjugierten $x_1, \dots, x_n$ von x. Es folgt: $a_{n-i} = \pm \sum_{\nu_1 < \dots < \nu_i} x_{\nu_1} \cdots x_{\nu_i}$ für $1 \leq i \leq n$, und somit ist auch $|a_{n-i}| \leq \sum_{\nu_1 < \dots < \nu_i} \underbrace{|x_{\nu_1}| \cdots |x_{\nu_i}|}_{=1}$

$$= \#\{(\nu_1, \dots, \nu_i);\ \nu_1, \dots, \nu_i \in \{1, \dots, n\} \text{ p.w.v.},\ \nu_1 < \dots < \nu_i\} = \binom{n}{i} = \binom{n}{n-i}.$$

■

(ii) **Beh.:** Es gibt nur endl. viele solche x vom Grad $\leq n$.

Bew.: Ist x ein solches, etwa mit $\deg(x) = m \leq n$, dann hat das Mipo von x die Koeff. $a_i \in \mathbb{Z}$, mit $|a_i| \leq \binom{m}{i}$ nach Teil (i),

das sind $2\binom{m}{i} + 1$ Möglichkeiten für ein a_i.

Vom Grad m gibt es also maximal $\prod_{i=0}^{m} \left(2 \cdot \binom{m}{i} + 1\right) < \infty$ viele solcher x, und vom Grad $\leq n$ insgesamt also maximal $\sum_{m=0}^{n} \prod_{i=0}^{m} \left(2 \cdot \binom{m}{i} + 1\right) < \infty$ viele. ■

(iii) **Beh.:** $\{x^m;\ m \in \mathbb{N}\}$ ist endlich.

Bew.: Es ist x^m ganzalgebraisch, sei y Konjugierte von x^m.
Dann $\exists$ Auto $\sigma: \mathbb{Q}(x^m) \to \mathbb{Q}(y)$ mit $x^m \mapsto y$. Dieser lässt sich zu einem Auto $\sigma: \mathbb{C} \to \mathbb{C}$ mit $x^m \mapsto y$ erweitern, und einschränken zu einem Auto $\sigma: \mathbb{Q}(x) \to \mathbb{Q}(\sigma x)$. Es folgt: $|y| = |\sigma(x^m)| = |\sigma x|^m = 1$.
Weiter sind alle x^m vom Grad $\le n$, falls x Grad n hat, da $x^m \in \mathbb{Q}(x)$.
Nach Teil (ii) ist daher $\{x^m;\ m \in \mathbb{N}\}$ endlich. ∎

(iv) Aus (iii) folgt: $\exists\, m, n \in \mathbb{N}$ mit $x^{m+n} = x^m$, also ist $x^n = 1$, und x eine n-te Einheitswurzel. □