Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

15.Vorlesung

26 Juni 2017

Beweis von Stickelberger.

Erinnerung (ÜB)**:** Sei L/K eine endliche separable Erweiterung, $\{\mu_1, \dots, \mu_n\}$ eine Basis, $n = [L : K]$, $\sigma_1, \dots, \sigma_n$ die verschiedene Einbettungen von L über K in Ω; dann gilt $\det(B_{L/K}(\mu_i, \mu_j)) = \underbrace{(\det(\sigma_i(\mu_j))^2}_{\neq 0} \in \mathbb{Z}$.

Sei nun $\{\mu_1, \dots, \mu_n\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$; es ist

$$\begin{aligned}
D(\mathcal{O}_L/\mathbb{Z}) &= [\sum_{\pi \in S_n} (\text{sign}(\pi)\sigma_{\pi(1)}(\mu_1) \dots \sigma_{\pi(n)}(\mu_n)]^2 \\
&= [(\sum_{\pi \in A_n} \text{sign}(\pi) \dots) + (\sum_{\pi \in S_n \setminus A_n} \text{sign}(\pi))]^2 \\
&= (G - U)^2 \in \mathbb{Z}
\end{aligned}$$

wobei $G := (\sum_{\pi \in A_n} \dots) \in \mathcal{O}_L \subseteq \Omega$ und $U := -(\sum_{\pi \in S_n \setminus A_n} \dots) \in \mathcal{O}_L \subseteq \Omega$.
Nun ist $L \subseteq \Omega$ galoissch. Für $\tau \in \text{Gal}(\Omega/\mathbb{Q})$:

Bemerkung
$\sigma_1, \dots, \sigma_n : L \hookrightarrow \Omega$, sei $i \in \{1, \dots, n\}$, $L \xrightarrow{\sigma_i} \Omega \xrightarrow{\tau} \Omega$, also $\exists j \in \{1, \dots, n\}$, so daß $\tau \circ \sigma_i = \sigma_j$, also ist die Abbildung $\rho : i \mapsto j \quad (\rho(i) = j \Leftrightarrow \tau \circ \sigma_i = \sigma_j)$ eine Permutation, d.h $\rho \in S_n$.

Wir berechnen:

$$\begin{aligned}
&\tau(\sigma_{\pi(1)}(\mu_1) \dots \sigma_{\pi(n)}(\mu_n)) = \\
&\tau \circ \sigma_{\pi(1)}(\mu_1) \dots \tau \circ \sigma_{\pi(n)}(\mu_n) = \\
&\sigma_{\rho\circ\pi(1)}(\mu_1) \dots \sigma_{\rho\circ\pi(n)}(\mu_n)
\end{aligned}$$

Daraus folgt: $\rho \in A_n \Rightarrow \tau(G) = G, \tau(U) = U$ und $\rho \in S_n \setminus A_n \Rightarrow \tau(G) = U, \tau(U) = G$ und somit ist $\tau(G + U) = G + U$ und $\tau(GU) = GU \quad \forall \tau \in \text{Gal}(\Omega/\mathbb{Q})$.
Nun $\Omega/\mathbb{Q}$ galoissch $\Rightarrow G + U, GU \in \text{Inv}(\Omega/\mathbb{Q}) \underset{FSGT}{=} \mathbb{Q}$
$G + U, GU \in \mathbb{Q}$ und $\mathbb{Z}$ ganz abgeschlossen$\Rightarrow G + U, GU \in \mathbb{Z}$. Also ist
$D(\mathcal{O}_L/\mathbb{Z}) = (G - U)^2 = \underbrace{(G + U)^2}_{\in \mathbb{Z}} - \underbrace{4GU}_{\in 4\mathbb{Z}} \Rightarrow (G - U)^2 \equiv (G + U)^2 \bmod 4$ in $\mathbb{Z}$. □

Definition 15.1
Sei $L/\mathbb{Q}$ ein Zahlkörper. Eine Einbettung von L in $\mathbb{C}$ ist <u>reell</u>, wenn ihr Bild in $\mathbb{R}$ liegt; sonst ist sie <u>komplex</u>.

Bemerkung
Setze $L = \mathbb{Q}(\alpha)$, $[L : \mathbb{Q}] = n$, $f :=$ MinPol$_{\mathbb{Q}}(\alpha)$, $f = \prod(x - \alpha_i) \in \mathbb{C}[X]$ mit r reellen Nullstellen und $2s$ komplexen Nullstellen, so daß $n = 2s + r$; dann hat L genau r relle Einbettungen in $\mathbb{C}$ und $2s$ komplexe Einbettungen in $\mathbb{C}$.

Satz (Satz von Brill)
(Ansatz wie oben) Es gilt $\mathrm{sign} D(\mathcal{O}_L/\mathbb{Z}) = (-1)^s$

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_L$ Basis für $L/\mathbb{Q}$ (es ist immer möglich, solch eine Basis zu finden, z.B. α primitives Element in $\mathcal{O}_L$ und $\alpha_i := \alpha^i$). Es ist
$D(\alpha_1, \ldots, \alpha_n) = (\det P)^2 D(\mathcal{O}_L/\mathbb{Z})$ ($P \in M_{n\times n}(\mathbb{Z})$ nicht unbedingt invertierbar). Insbesondere $\mathrm{sign} D(\alpha_1, \ldots, \alpha_n) = \mathrm{sign} D(\mathcal{O}_L/\mathbb{Z})$. Wir berechnen nun $\mathrm{sign} D(1, \alpha, \ldots, \alpha^{n-1})$, d.h wir berechnen $\mathrm{sign} D(f)$, wobei $f :=$ $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Seien $\beta_1, \ldots, \beta_r, z_1, \ldots, z_s, \bar{z}_1, \ldots, \bar{z}_s$ alle Nullstellen von f in $\mathbb{C}$.

$$f = \prod (x - \alpha_i) = \prod_r (x - \beta_j) \prod_s (x - z_k) \prod_s (x - \bar{z}_k)$$

$$\underset{\text{Def 14. Vor.}}{\Rightarrow} \quad D(f) = \prod_{i<j} (\beta_i - \beta_j)^2 \prod_{i,k} (\beta_i - z_k)^2 \prod_{i,k} (\beta_i - \bar{z}_k)^2 \prod_{k<l} (z_k - z_l)^2 \prod_{k,l} (z_k - \bar{z}_l)^2 \prod_{k<l} (\bar{z}_k - \bar{z}_l)^2$$

.
Bezeichnung: $\mathbb{R}_+ = \mathbb{R}^{>0}, \mathbb{R}_- := \mathbb{R}^{<0}$.
Nun ist $\prod_{i<j} (\beta_i - \beta_j)^2 \in \mathbb{R}^2 > 0$ $(\beta_i \neq \beta_j)$,
$\underbrace{\prod_{i,k} (\beta_i - z_k)^2}_{:=w} \underbrace{\prod_{i,k} (\beta_i - \bar{z}_k)^2}_{\bar{w}} = w\bar{w} \in \mathbb{R}_+$.
Analog für $\prod_{k<l} (z_k - z_l)^2 \prod_{k<l} (\bar{z}_k - \bar{z}_l)^2 \in \mathbb{R}_+$, also bleibt $\prod_{k,l} (z_k - \bar{z}_l)^2$ übrig zu behandeln: ist $k \neq l$, dann erscheinen die Faktoren $z_k - \bar{z}_l$ sowie $z_l - \bar{z}_k$ im Produkt, also
$(z_k - \bar{z}_l)(z_l - \bar{z}_k)^2 = [-\underbrace{(z_k - \bar{z}_l)(\bar{z}_k - z_l)}_{\in \mathbb{R}^+}]^2 \in \mathbb{R}_+$. Letztendlich ist also
$\mathrm{sign}(D(1, \alpha, \ldots, \alpha^{n-1})) = \mathrm{sign}(\prod_{k=1}^s (z_k - \bar{z}_k)^2)$,
aber $z_k - \bar{z}_k \in i\mathbb{R}$, also ist $(z_k - \bar{z}_k)^2 \in \mathbb{R}_-$, also ist $\prod_{k=1}^s (z_k - \bar{z}_k)^2$ Produkt von s negativen reellen Zahlen, und damit ist sein Zeichen $(-1)^s$. □

Proposition 15.1
Sei L/K endlich separabel, $\sigma_1, \ldots, \sigma_n$ die Einbettungen von L über K in Ω, α primitives Element, $f :=$ $\mathrm{MinPol}_K(\alpha)$, $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f.
Es ist $D(f) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$

Beweis. $f = \prod (x - \alpha_i) \Rightarrow$

$$f' = \sum_{i=1}^n (\prod_{j\neq i} (x - \alpha_j) \tag{‡}$$

Andererseits (per Definition der $N_{L/K}$) haben wir
$N_{L/K}(f'(\alpha)) = \prod_{k=1}^n \sigma_k(f'(\alpha)) = \prod_{k=1}^n (f'(\sigma_k(\alpha))) = \prod_{k=1}^n f'(\alpha_k)$.
Einsetzen von α_k in (‡) ergibt
$f'(\alpha_k) = \prod_{j\neq k} (\alpha_k - \alpha_j)$, also ist
$N_{L/K}(f'(\alpha)) = \prod_{k=1}^n \prod_{j\neq k} (\alpha_k - \alpha_j)$. Wir vergleichen nun dieses Produkt mit
$D(f) = \prod_{j<k} (\alpha_k - \alpha_j)^2$. In $N_{L/K}(f'(\alpha))$ erscheint jede Differenz $(\alpha_k - \alpha_j)$ zweimal und zwar für (j, k) und (k, j). Wir berechnen nun: für jedes $k = 1, \ldots, n$, $j < k \Rightarrow (\alpha_j - \alpha_k)^2$ erscheint in $D(f)$. Dagegen erscheint
$(\alpha_j - \alpha_k)(\alpha_k - \alpha_j) = -(\alpha_j - \alpha_k)^2$ im Produk, d.h $\forall k = 1, \ldots, n$ und $j < k$ wird ein Faktor (-1) beigetragen, insgesamt also $(n-1) + (n-2) + \cdots + 0$ Beiträge. □

Proposition/Beispiel
Sei $f(x) = x^n + ax + b$ irreduzibel, α eine Nullstelle,
$L := \mathbb{Q}(\alpha)$, $n = [L : \mathbb{Q}]$. Setze $\gamma := f'(\alpha) = n\alpha^{n-1} + a$. Wir berechnen $N_{L/\mathbb{Q}}(\gamma)$ (damit wir eine Formel für $D(f)$ bekommen). Nun erfüllt α: $\alpha^n + a\alpha + b = 0$. Multiplizieren mit α^{-1} ergibt $\alpha^{n-1} + a + b\alpha^{-1} = 0$, also ist $\gamma = -n(a + b\alpha^{-1}) + a = -(n-1)a - (nb\alpha^{-1})$, d.h $\alpha = \frac{-nb}{\gamma+(n-1)a}$ und somit ist $L = \mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$ und $n = [\mathbb{Q}(\gamma) : \mathbb{Q}]$.
Andererseits ist $f(\frac{-nb}{x+(n-1)a}) = \frac{p(x)}{q(x)} \in \mathbb{Q}(x)$,
also $f(\alpha) = \frac{p(\gamma)}{q(\gamma)} = 0$ und somit ist $p(\gamma) = 0$. Nun ist aber
$p(x) = (x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$. Also ist $p(x)$ normiert, $\deg p = n$ und $p(\gamma) = 0$, d.h $p(x)$ ist das $\mathrm{MinPol}_{\mathbb{Q}}(\gamma)$. Wir berechnen nun (Lemma 11.2)
$N_{L/\mathbb{Q}}(\gamma) = (-1)^n(n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1}$
Also $N_{L/\mathbb{Q}}(\gamma) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n$
und $D(f) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)$

Beispiel
$f(x) = x^3 - x - 1$ ist irreduzibel in $\mathbb{Q}[x]$. Sei $\alpha \in \mathbb{C}$ eine Nullstelle, berechne $D(1, \alpha, \alpha^2) = D(f) \overset{\text{Prop}}{=} -23$ ist quadratfrei, und $\alpha \in \mathcal{O}_L$ (weil $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = f(x) \in \mathbb{Z}[x]$), also ist $\{1, \alpha, \alpha^2\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$ und $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

16