B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

20.Vorlesung

29. Juni 2021

In diesem Skript werden wir weitere Berechnungen für Diskriminante führen und damit Kapitel 5 beenden. Wir werden dann Kapitel 6 über Gitter und die Geometrie der Zahlen anfangen, mit dem Ziel, die Endlichkeit der Klassenzahl für Zahlkörper zu beweisen.

Ansatz und Bezeichnung weiterhin wie im Skript 14, 15, 16, 17, 18, 19.

Proposition 20.1
Sei L/K eine endliche separable Körpererweiterung, $[L:K]=n$, α primitives Element, $f = \text{MinPol}_K(\alpha)$. Es ist

$$D(f) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$$

Beweis. Seien $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f, und $\sigma_1, \ldots, \sigma_n$ die Einbettungen von L über K in Ω. Schreibe $f(x) = \prod(x-\alpha_i)$ und berechne

$$(\dagger) \qquad f'(x) = \sum_{i=1}^{n} (\prod_{j\neq i} (x-\alpha_j)\,.$$

• Per Definition von $N_{L/K}$ und Satz 15.4 haben wir

$$(\ddagger) \qquad N_{L/K}(f'(\alpha)) = \prod_{k=1}^{n} \sigma_k(f'(\alpha)) = \prod_{k=1}^{n} (f'(\sigma_k(\alpha))) = \prod_{k=1}^{n} f'(\alpha_k)\,.$$

• Einsetzen von α_k in $(\dagger)$ und von $f'(\alpha_k)$ in $(\ddagger)$ ergibt:

$$f'(\alpha_k) = \prod_{j\neq k} (\alpha_k - \alpha_j)$$

und

$$(*) \quad N_{L/K}(f'(\alpha)) = \prod_{k=1}^{n} \prod_{j\neq k} (\alpha_k - \alpha_j)\,.$$

• Per Definition haben wir:

$$(**) \quad D(f) = \prod_{j<k} (\alpha_k - \alpha_j)^2\,.$$

• Wir vergleichen nun das Produkt im $(*)$ mit $(**)$:
In $N_{L/K}(f'(\alpha))$ wie in $(*)$ erscheint jede Differenz $(\alpha_k - \alpha_j)$ zweimal und zwar für (j,k) und (k,j), d.h. $(\alpha_j - \alpha_k)(\alpha_k - \alpha_j) = -(\alpha_j - \alpha_k)^2$ erscheint im $(*)$.
Dagegen erscheint für jedes $k = 1, \ldots, n$, mit $j < k$ der Faktor $(\alpha_j - \alpha_k)^2$ wie in $(**)$ in $D(f)$.

Zusammengefasst: $\forall k = 1, \ldots, n$ und $j < k$ wird ein Faktor (-1) beigetragen, insgesamt also $(n-1) + (n-2) + \cdots + 0$ Beiträge. Also weicht $(**)$ von $(*)$ mit dem Faktor $(-1)^{\frac{n(n-1)}{2}}$ ab. $\square$

Proposition/Beispiel
Sei $f(x) = x^n + ax + b \in \mathbb{Q}[x]$ irreduzibel, α eine Nullstelle, setze $L := \mathbb{Q}(\alpha)$, $n = [L : \mathbb{Q}]$.
Wir wollen Proposition 20.1 anwenden und $D(f)$ berechnen. Setze $\gamma := f'(\alpha) = n\alpha^{n-1} + a$. Wir müssen $N_{L/\mathbb{Q}}(\gamma)$ berechnen.
Dafür werden wir das minimal Polynom von γ berechnen und dann Lemma 14.2 4 (i) anwenden.

Nun erfüllt α die Gleichung $\alpha^n + a\alpha + b = 0$. 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 $n = [\mathbb{Q}(\gamma) : \mathbb{Q}]$.
Setze $y = \frac{-nb}{x + (n-1)a} \in \mathbb{Q}(x)$ und betrachte die rationale Funktion $f(y) = \frac{p(x)}{q(x)} \in \mathbb{Q}(x)$. Einsetzen von $x = \gamma$ in y ergibt:

$$0 = f(\alpha) = \frac{p(\gamma)}{q(\gamma)} = 0\,.$$

Somit muss $p(\gamma) = 0$. Wenn wir $f(y) = y^n + ay + b$ direkt berechnen und als Quotient umschreiben bekommen wir

$$p(x) = (x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$$

und der konstante Koeffizient a_0 von $p(x)$ ist

$$(n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1}$$

(ÜA).
Da $p(x) \in \mathbb{Q}[x]$ normiert ist, $\deg p = n$ und $p(\gamma) = 0$, folgt nun $p(x)$ ist das $\mathrm{MinPol}_{\mathbb{Q}}(\gamma)$.

Wir berechnen nun wegen Lemma 14.2 4 (i):

$$N_{L/\mathbb{Q}}(\gamma) = (-1)^n a_0 = (-1)^n (n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1}\,.$$

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 20.1
$f(x) = x^3 - x - 1$ 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 $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

Kapitel 6: Gitter in $\mathbb{R}^n$

Wir behalten die Bezeichnungen der LA I und LA II, zum Beispiel: $||x||$ ist die euklisdische Norm für $x \in \mathbb{R}^n$.

Definition 20.1 (i) Sei $\{e_1, \ldots, e_m\} \subseteq \mathbb{R}^n$ linear unabhängig über $\mathbb{R}$ (also $m \leq n$). Die von $\{e_1, \ldots, e_m\}$ erzeugte additive Gruppe Γ ist ein Gitter der Dimension m. Das heißt

$$\Gamma := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_m$$

ist eine freie abelsche Gruppe vom Rang m.

Wenn $m = n$ heißt Γ vollständiges Gitter

(ii) $X \subseteq \mathbb{R}^n$ ist beschränkt, wenn es ein $r \in \mathbb{R}_+$ gibt, so daß $X \subseteq B_r(0)$:=die Kugel mit Zentrum 0 und Radius r.

(iii) $X \subseteq \mathbb{R}^n$ ist diskret, wenn $|B_r(0) \cap X| < \infty$ für alle $r \in \mathbb{R}_+$.

Definition 20.2
Sei Γ ein Gitter mit erzeugender Menge $\{e_1, \ldots, e_n\}$.
$T := \{x \in \mathbb{R}^n \mid x = \sum a_i e_i, 0 \leq a_i < 1, a_i \in \mathbb{R}\}$ heißt fundamentaler Parallelotop von Γ.