Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Uhu
K. Halupczok

Z6: Norm, Spur, Diskriminante

Stichworte: Norm, Spur in Zahlkörpern, Einheitengruppe (insb. imag.qu. Zk), Schachtelungssatz, Diskriminante, Norm/Spur/disc ganzer Elemente ist ganz, Diskriminante normaler Zahlkörpererweiterungen, disc(x), disc einer EW, Satz von Kronecker-Weber

---

6.1. **Einleitung:** Anhand der Norm (bzw. Spur) von Elementen im Zahlkörper lassen sich viele Eigenschaften der Zahlringelemente untersuchen, z.B. ob eine Einheit des Zahlrings vorliegt: wir bestimmen damit die Einheitengruppen der imaginärquadratischen Zahlkörper. Weiter ist die Norm und Spur ganzer Ringelemente sind ganz. Die Diskriminante ist ferner eine wichtige Kenngröße eines Zahlkörpers.

6.2. **Def.:** Sei K Körper, $L|K$ Erweiterung vom Grad n (d.h. $K \subseteq L$ und $[L:K] = \dim_K L = n$). Für $x \in L$ betr. $\mu_x : L \to L$, $y \mapsto xy$. Die Abb. μ_x ist L-linear, also auch K-linear.

$T_K^L(x) := \operatorname{Spur} \mu_x$ heißt Spur von x (bzgl. $L|K$),

$N_K^L(x) := \det \mu_x$ heißt Norm von x (bzgl. $L|K$).

Aus LA: $\operatorname{Spur}(a_{ij})_{i,j} := \sum_{i=1}^{n} a_{ii}$, Spur eines Endos ist basisunabh.

6.3. **Bem.:** (1) Die Spurabb. $T_K^L : L \to K$ ist ein Homomorphismus der additiven Gruppen (von L und K). $T_K^L(x+y) = \operatorname{Spur} \mu_{x+y} = \operatorname{Spur}(\mu_x + \mu_y) = \operatorname{Spur}\mu_x + \operatorname{Spur}\mu_y = T_K^L(x) + T_K^L(y)$.

(2) Die Normabb. $N_K^L : L^\times \to K^\times$ ist ein Homomorphismus der multiplikativen Gruppen (von L und K). $N_K^L(x \cdot y) = \det \mu_{xy} = \det \mu_x \circ \mu_y = (\det \mu_x)(\det \mu_y) = N_K^L(x) \cdot N_K^L(y)$.

(3) Sei $x \in K$. Dann ist $T_K^L(x) = nx$, $N_K^L(x) = x^n$.

Berechnung von T_K^L und N_K^L:

6.4. **Speziell:** Sei $L = K(x)$, $f(T) = T^n + a_{n-1}T^{n-1} + \dots + a_0 \in K[T]$ sei Mipo von $x|K$. Dann ist $\mathcal{B} : 1, x, \dots, x^{n-1}$ K-Basis von L. Es folgt:

$$M := M_{\mathcal{B}}(\mu_x) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & 0 & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

die Begleitmatrix zum Mipo $f \in K[T]$.

Somit ist $T_K^L(x) = -a_{n-1}$, $N_K^L(x) = (-1)^n a_0$.

6.5. **Allgemein:** Sei $y_1, \dots, y_n$ eine Basis von $L|K(x)$. Dann ist

L / n / $K(x)$ / m / K

$B' : y_1, y_1x, \dots, y_1x^{m-1}, \; y_2, y_2x, \dots, y_2x^{m-1}, \; \dots, \; y_n, y_nx, \dots, y_nx^{m-1}$

eine K-Basis von L. Die Matrix von μ_x bzgl. B' ist dann

$$M_{B'}(\mu_x) = \begin{pmatrix} M & & 0 \\ & \ddots & \\ 0 & & M \end{pmatrix}$$ (n Blöcke). Es folgt: $T_K^L(x) = n\, T_K^{K(x)}(x)$,

$N_K^L(x) = \left(N_K^{K(x)}(x)\right)^n$.

6.6. **Kor.:** In Zahlkörpern ist die Norm und Spur ganzer Elemente ganz rational, d.h. $\in \mathbb{Z}$.
(Dies gilt auch für Zahlringerweiterungen.)

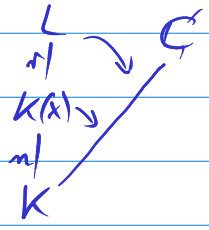
6.7. **Satz:** Seien $L|K$ Zahlkörper, $[L:K]=n$, und seien $\sigma_1, \dots, \sigma_n$ die Einbettungen von $L|K$ in $\mathbb{C}$ (d.h. inj. Körperhom, die K fix lassen: $\forall i \; \forall x \in K : \sigma_i(x) = x$.)
Dann gilt für $x \in L$: $T_K^L(x) = \sum_{i=1}^{n} \sigma_i x$ und $N_K^L(x) = \prod_{i=1}^{n} \sigma_i x$.

Bew.: • **Speziell:** Sei $L = K(x)$, $f = T^m + a_{m-1}T^{m-1} + \dots + a_0 \in K[T]$ das Mipo von $x|K$.
Es gilt: $f = \prod_{i=1}^{m} (T - \sigma_i x)$. Somit: $a_{m-1} = -\sum_{i=1}^{m} \sigma_i x$, $a_0 = (-1)^m \prod_{i=1}^{m} \sigma_i x$.

• **Allgemein:** Sei $[K(x):K] = m$, $[L:K(x)] = r$, und $n := m \cdot r$, seien $\tau_1, \dots, \tau_n$ die Einbettungen von $L|K$.
Für $1 \le i \le m$ ist dann $\#\{j;\ \tau_j|K(x) = \sigma_i\} = r$.
Somit ist

$$\sum_{j=1}^{n} \tau_j(x) = \sum_{i=1}^{m} \sum_{\substack{j \text{ mit} \\ \tau_j|K(x)=\sigma_i}} \tau_j(x) = \sum_{i=1}^{m} \sum_{\substack{j \text{ mit} \\ \tau_j|K(x)=\sigma_i}} \sigma_i(x) = \sum_{i=1}^{m} r\,\sigma_i(x)$$

$$= r \sum_{i=1}^{m} \sigma_i(x) = r\, T_K^{K(x)}(x) = T_K^L(x).$$



Analog beweist man die Beh. für die Norm. □

6.8. **Anwendung/Bem.:** Sei $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z} \setminus \{0,1\}$ quadfrei, ist ZFK (Zerfällungskörper) von $T^2 - m = (T - \sqrt{m})(T + \sqrt{m})$ über $\mathbb{Q}$, d.h. quadr. Körpererw. sind normal.
Sei $x = a + b\sqrt{m} \in K$, mit $a, b \in \mathbb{Q}$. Die Einbettungen von K in $\mathbb{C}$ sind σ_1, σ_2, wo $\sigma_1(\sqrt{m}) = \sqrt{m}$, $\sigma_2(\sqrt{m}) = -\sqrt{m}$. Dann ist

$$T_{\mathbb{Q}}^K(x) = \sigma_1 x + \sigma_2 x = a + b\sqrt{m} + a - b\sqrt{m} = 2a,$$

$$N_{\mathbb{Q}}^K(x) = (\sigma_1 x)(\sigma_2 x) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

Bsp.: $N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{5})}\left(\frac{1+\sqrt{5}}{2}\right) = \frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = \frac{1}{4}(1-5) = -1$.

6.9. **Notation:** Schreiben im folgenden T bzw. N für $T_{\mathbb{Q}}^K$ bzw. $N_{\mathbb{Q}}^K$.

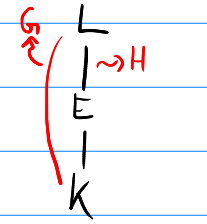
6.10. **Bem.:** Sei K ZK (Zahlkörper) mit ZR (Zahlring) A.
Sei $0 \neq x \in A$, $f = T^n + a_{n-1}T^{n-1} + \dots + a_0 \in \mathbb{Z}[T]$ das Mipo von $x/\mathbb{Q}$.
(1) Dann: $x \in A^\times \Leftrightarrow \hat{x} \in A \Leftrightarrow$ Mipo von $\hat{x}$ über $\mathbb{Q}$ liegt in $\mathbb{Z}[T] \Leftrightarrow a_0 = \pm 1$.
⌜Das Mipo von $\hat{x}$ über $\mathbb{Q}$ ist $\hat{a}_0(a_0T^n + \dots + 1)$, $\mathbb{Q}(\hat{x}) = \mathbb{Q}(x) \Rightarrow$ Mipo von $\hat{x}$ hat Grad n.
(haben: $x^n + a_{n-1}x^{n-1} + a_1x + a_0 = 0 \Leftrightarrow 1 + a_{n-1}(\hat{x}) + \dots + a_1(\hat{x})^{n-1} + a_0(\hat{x})^n = 0$)⌟
(2) Wegen $N(x) = \pm a_0^n$ folgt: $A^\times \overset{!}{=} \{x \in A;\ N(x) = \pm 1\}$.
⌜2. Bew.: Es ist $N(x) = \prod_{i=1}^{n} \sigma_i x = x \cdot \prod_{i=2}^{n} \sigma_i x$. ($\sigma_1 = \mathrm{id}$; $\prod_{i=2}^{n} \sigma_i x =: y \in A$). Dann: „$\supseteq$": $N(x) = \pm 1 \Rightarrow x \in A^\times$ mit $y = \pm\hat{x}$,
„$\subseteq$": $x \cdot \hat{x} = 1$, also $\frac{N}{x} = \prod_{i=2}^{n} \sigma_i x = y \in A$, $\Rightarrow N \in A^\times \cap \mathbb{Z} \Rightarrow N(x) = \pm 1$.⌟

6.11. **Def.:** $A^\times$ heißt auch Einheitengruppe von K. Die Elemente von $A^\times$ heißen auch Einheiten von K.

6.12. **Anwendungen / Bem.:** (1) Die Einheitengruppen der imaginärquadr. ZK sind alle endlich. ⌜vgl. 6.13⌟
(2) Sei $K = \mathbb{Q}(\sqrt{2})$, dann ist $A = \mathbb{Z}[\sqrt{2}]$ nach 4.4.
Sei $x = a + b\sqrt{2} \in A$ mit $a, b \in \mathbb{Z}$. Dann ist $N(x) = a^2 - 2b^2$,
also $1 < 1 + \sqrt{2} \in A^\times$, d.h. $\{(1+\sqrt{2})^n;\ n \in \mathbb{Z}\}$ ist unendliche zyklische UG der Einheitengruppe $A^\times$.

Der folgende Satz heißt **Schachtelsatz für Norm und Spur:**

6.14. **Satz:** Seien $K \subseteq E \subseteq L$ ZK. Dann gilt für alle $x \in L$:
$$T_K^L(x) = T_K^E(T_E^L(x)) \quad \text{und} \quad N_K^L(x) = N_K^E(N_E^L(x)).$$
Bew.: *1. Fall:* L/K normal, dann galois, setze $G := \mathrm{Gal}(L/K)$.
Die Elemente von $\mathrm{Gal}(E/K)$ entsprechen (eineindeutig) den Nebenklassen σH der Untergruppe $H = \mathrm{Gal}(L/E)$ von G (laut dem HS der Galoistheorie (Algebra A23.10(2)).
Ist $\mathcal{V} \subseteq G$ ein Vertretersystem der Nebenklassen σH in G, ⌜$\mathrm{Gal}(E/K) \cong G/H$⌟
so entsprechen die $\sigma \circ \tilde{\sigma}$ mit $\sigma \in \mathcal{V}$, $\tilde{\sigma} \in H$, genau den Elementen von $G = \mathrm{Gal}(L/K)$.
Da die $\sigma\tilde{\sigma} \in G$, werden damit genau die Elemente von G durchlaufen.
Aufgrund von Satz 6.7 ist also das Mipo von $x \in L$ über K gleich
$$\prod_{\sigma \in \mathcal{V}} \prod_{\tilde{\sigma} \in H} (T - \sigma\circ\tilde{\sigma}(x))$$

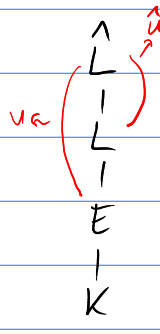


$$= T^n - \sum_{\sigma\in U} \sigma\Big(\sum_{\tilde\sigma\in H} \tilde\sigma(x)\Big) T^{n-1} + \dots + (-1)^n \prod_{\sigma\in U} \sigma\Big(\prod_{\tilde\sigma\in H} \tilde\sigma(x)\Big),$$

wobei $n := [L:K]$. Daran lässt sich ablesen, dass

$$T_K^L(x) = T_K^E\big(T_E^L(x)\big) \quad \text{und} \quad N_K^L(x) = N_K^E\big(N_E^L(x)\big).$$

2. Fall: L nicht normal. Betrachte dann eine normale Erweiterung $\hat L \mid L$ (ist galois), setze $\hat U = \mathrm{Gal}(\hat L \mid E)$, $\hat u = \mathrm{Gal}(\hat L \mid L)$. Ist U ein Vertretersystem der Nebenklassen $\sigma\hat U$ in $G = \mathrm{Gal}(\hat L \mid K)$, und $\hat U$ eines der Nebenklassen $\hat\sigma \hat U$ in $\hat U$, so bilden die $\tau = \sigma\circ\hat\sigma$ mit $\sigma\in U$, $\hat\sigma\in\hat U$, ein Vertretersystem der Nebenklassen $\tau\hat U$ in G.



Die Überlegung aus dem 1. Fall greift analog, wo $\tilde\sigma \in H$ durch $\hat\sigma\in\hat U$ ersetzt wird (denn Satz 6.7 gilt für die Einbettungen von $L\mid K$ in $\hat L$). □

6.13 Satz: Die Einheitengruppe eines imaginärquadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-m})$ mit $m\in\mathbb{N}$ quadratfrei ist endlich, nämlich

$$\begin{cases} \{\pm 1, \pm i\}, & \text{falls } m=1, \quad (\text{Gaußscher Zahlring } \mathbb{Z}[i]) \\ \{\pm 1, \pm\tfrac12 \pm \tfrac12\sqrt{-3}\}, & \text{falls } m=3, \quad (\text{Eisensteinring } \mathbb{Z}[\tfrac12+\tfrac12\sqrt{-3}]) \\ \{\pm 1\}, & \text{sonst.} \end{cases}$$

Bew.: Sei $m<0$ quadratfrei, und $K = \mathbb{Q}(\sqrt{m})$. Dann ist

$$A_K = \begin{cases} \mathbb{Z}[\sqrt{m}], & m\equiv 2,3\ (4), \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right], & m\equiv 1\ (4) \end{cases} \quad \text{nach 4.4.}$$

Nun gilt: $x\in A_K^\times \iff N_{\mathbb{Q}}^K(x) = \pm 1$ nach 6.10(2).

1. Fall: $m\equiv 2,3\ (4)$, sei $a+b\sqrt{m}\in\mathbb{Z}[\sqrt{m}]^\times$ mit $a,b\in\mathbb{Z}$, und $a^2 - b^2 m = \pm 1$.

- Falls $m=-1$, ist also $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
- Falls $m<-1$, muss $b=0$ sein, also ist $\mathbb{Z}[\sqrt{m}]^\times = \{\pm 1\}$.

2. Fall: $m\equiv 1\ (4)$, sei $\frac12(a+b\sqrt{m})\in\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]^\times$ mit $a,b\in\mathbb{Z}$ und $a\equiv b\ (2)$, vergleiche 4.5.

Also ist $\frac14(a^2 - mb^2) = \pm 1$.

- Falls $m=-3$, ist $(a^2=4 \ \&\ b^2=0)$ oder $(a^2=1 \ \&\ b^2=1)$, und somit $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \{\pm 1, \pm\tfrac12 \pm \tfrac12\sqrt{m}\}$.
- Falls $m\le -7$, muss $b=0$ sein, also ist $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]^\times = \{\pm 1\}$. □

Die Diskriminante

6.15. **Def.:** Sei $K \subseteq L$ ZK mit $[L:K]=n$, $\sigma_1,\dots,\sigma_n$ die Einbettungen von $L|K$ in $\mathbb{C}$. Für $x_1,\dots,x_n \in L$ heißt $\operatorname{disc}_K^L(x_1,\dots,x_n) := \left(\det(\sigma_i(x_j))_{1\le i,j\le n}\right)^2$ die Diskriminante von $x_1,\dots,x_n$ (bzgl. $L|K$).

6.16. **Bem.:** (1) disc_K^L hängt nicht von der Reihenfolge der σ_i und der x_j ab.

(2) Es ist $T: L \to K$ (Spurabbildung von $L|K$) K-linear, $(T = T_K^L)$

sei $\Phi_T: L\times L \to L \xrightarrow{T} K$

$(x,y) \mapsto x\cdot y \mapsto T(xy)$. Dann ist Φ_T nichtausgeartete symmetrische K-Bilinearform auf L, d.h. $\forall x\neq 0\ \exists y: \Phi_T(x,y)\neq 0$.

⌜Sei $x\neq 0$. Dann ist $\Phi_T(x,\frac{1}{x}) = T(x\cdot\frac{1}{x}) = T(1) = n \neq 0$.⌟

6.17. **Lemma:** Es ist $\operatorname{disc}_K^L(x_1,\dots,x_n) = \det\left(T(x_i x_j)_{1\le i,j\le n}\right)$.

Bew.: Es ist $\operatorname{disc}_K^L(x_1,\dots,x_n) = \left(\det(\sigma_j(x_i))_{1\le i,j\le n}\right)^2 = \det(\sigma_i(x_j))\cdot\det(\sigma_i(x_j))$

$= \det((\sigma_i x_j)^T)\det(\sigma_i x_j) = \det\left((\sigma_i x_j)^T\cdot(\sigma_i x_j)\right) = \det\left(\sum_\ell (\sigma_\ell x_i)(\sigma_\ell x_j)\right)$

$= \det\left(\sum_\ell \sigma_\ell(x_i x_j)\right) = \det T(x_i x_j)$. □

6.18. **Kor.:** Sei $d := \operatorname{disc}_K^L(x_1,\dots,x_n)$. Dann ist $d\in K$, und ist $L|K$ normal, so ist d ein Quadrat in L. Die Diskriminante ganzer (d.h. ganz algebraischer) Elemente ist ganz.

Bew.: $d\in K$ klar nach Def. von disc / Lemma 6.17. Ist $L|K$ normal, so sind alle $\sigma_i \in \mathrm{Aut}(L|K) = \mathrm{Gal}(L|K)$, also liegen alle $\sigma_i x_j$ in L, dann ist d Quadrat in L nach Def. von disc. Sind $x_1,\dots,x_n$ ganz, so ist auch d ganz, vgl. 6.4, 6.6, 6.17. □

6.19. **Kor.:** $\operatorname{disc}(x_1,\dots,x_n)\neq 0 \iff x_1,\dots,x_n$ sind K-Basis von L.

Bew.: $0 = \operatorname{disc}(x_1,\dots,x_n) \overset{6.17}{(=)} \det((\sigma_i x_j)_{i,j}) = 0 \iff$ Spalten $\begin{pmatrix}\sigma_1 x_1\\ \vdots\\ \sigma_n x_1\end{pmatrix},\dots,\begin{pmatrix}\sigma_1 x_n\\ \vdots\\ \sigma_n x_n\end{pmatrix}$ lin. abh.

$\iff \exists \lambda_i\in K$, nicht alle $=0$: $\sum_{i=1}^n \lambda_i \begin{pmatrix}\sigma_1 x_i\\ \vdots\\ \sigma_n x_i\end{pmatrix} = 0$ bzw. $\forall \ell\le n$: $0 = \sum_{i=1}^n \lambda_i \sigma_\ell x_i = \sigma_\ell\left(\sum_{i=1}^n \lambda_i x_i\right)$ bzw. $\sum_{i=1}^n \lambda_i x_i = 0$

$\iff x_1,\dots,x_n$ sind K-lin. abhängig. □

6.20. **Lemma:** Sei $K = \mathbb{Q}(x)$ vom Grad n über $\mathbb{Q}$, $f(T) = \prod_{i=1}^{n} (T - x_i)$ das Mipo von x über K, die $x_i \in \mathbb{C}$. Dann: $\operatorname{disc}_{\mathbb{Q}}^{K}(1, x, \dots, x^{n-1}) = \prod_{1 \le i < j \le n} (x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} N(f'(x))$.

Bew.: Seien $\sigma_1, \dots, \sigma_n$ die Einbettungen von $\mathbb{Q}(x)$ in $\mathbb{C}$, $\sigma_i x = x_i$.
Dann ist $\operatorname{disc}_{\mathbb{Q}}^{K}(1, x, \dots, x^{n-1}) = (\det(\sigma_i x^j))^2 = (\det(x_i^j))^2$
$\overset{\text{Vander-monde}}{=} \prod_{1 \le i < j \le n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{\substack{1 \le i, j \le n \\ i \ne j}} (x_i - x_j) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{j \ne i} (x_i - x_j)$
$\overset{!}{=} (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(x_i) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \sigma_i(f'(x)) = (-1)^{n(n-1)/2} N(f'(x))$.
Zu „$\overset{!}{=}$": Es ist $f' = \sum_{\ell=1}^{n} \prod_{j \ne \ell} (T - x_j)$, also $f'(x_i) = \prod_{j \ne i} (x_i - x_j)$. □

6.21. **Def.:** Sei $x \in \mathbb{C}$ vom Grad n über $\mathbb{Q}$, $K = \mathbb{Q}(x)$. Dann: $\operatorname{disc}(x) := \operatorname{disc}_{\mathbb{Q}}^{K}(1, x, \dots, x^{n-1})$.

6.22. **Bem.:** (1) p sei ungerade Pz, $\omega = e^{2\pi i/p}$. Haben $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p) = p - 1$,
d.h. $n = p - 1$. Nun ist $T^{p-1} - 1 = (T - 1)(\underbrace{T^{p-1} + \dots + T + 1}_{=: f(T) \text{ irred., Mipo von } x \text{ (d.h. } p\text{-tes Kreisteilungspolynom)}})$, (*)
mit $f(T) = \prod_{i=1}^{p-1} (T - \omega^i)$. Dann ist $\operatorname{disc}(\omega) = (-1)^{p(p-1)/2} N(f'(\omega))$ nach 6.20.

Ableiten von (*) liefert $pT^{p-1} = f(T) + (T - 1) f'(T)$,
also $p\omega^{p-1} = (\omega - 1) f'(\omega)$, d.h. $f'(\omega) = \frac{p}{(\omega - 1)\omega}$.
Nun ist $N(p) = p^{p-1}$, $N(\omega) = 1$ [= konst. Koeff. des Mipos]
und $N(\omega - 1) = \prod_{i=1}^{p-1} (\omega^i - 1) = (-1)^{p-1} \prod_{i=1}^{p-1} (1 - \omega^i) = (-1)^{p-1} f(1)$

$= (-1)^{p-1} p = p$, da p ungerade.

Eingesetzt:
$$\operatorname{disc}(\omega) = \frac{N(p)\,(-1)^{(p-1)p/2}}{N(\omega)\,N(\omega - 1)} = \frac{p^{p-1}}{p} \cdot (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

(2) Sei $m>2$, $\omega = e^{2\pi i/m}$. Dann: $\operatorname{disc}(\omega) \mid m^{\varphi(m)}$.

[Es ist $T^m - 1 = f \cdot g$, mit f Mipo von ω. Dann ist $g \in \mathbb{Z}[T]$, da $f \in \mathbb{Z}[T]$ nach 3.20. Wegen $m\omega^{m-1} = f'(\omega)\, g(\omega)$ [Ableiten] folgt $m = \omega f'(\omega) g(\omega)$, also $m^{\varphi(m)} = N(m) = \underbrace{N(\omega g(\omega))}_{\in \mathbb{Z}} \underbrace{N(f'(\omega))}_{\pm \operatorname{disc}(\omega)}$.]

6.23. **Kor.:** (i) Sei p ungerade PZ, $\omega = e^{2\pi i/p}$. Dann gilt:
$\mathbb{Q}(\omega)$ enthält $\sqrt{p}$, falls $p \equiv 1 \ (4)$,
bzw. $\sqrt{-p}$, falls $p \equiv 3 \ (4)$.
(ii) Jeder quadratische ZK ist in einem Kreisteilungskörper enthalten.

Bew.: (i): Nach 6.18 ist $\operatorname{disc}(\omega) = (-1)^{\frac{p-1}{2}} p^{p-2}$ ein Quadrat in $\mathbb{Q}(\omega)$.
- Falls $p \equiv 1(4)$: $\mathbb{Q}(\omega)$ enthält $\sqrt{p^{p-2}} = p^{\frac{p-3}{2}}\sqrt{p}$, also auch $\sqrt{p}$.
- Falls $p \equiv 3(4)$: $\mathbb{Q}(\omega)$ enthält $i\sqrt{p^{p-2}} = i\, p^{\frac{p-3}{2}}\sqrt{p}$, also $i\sqrt{p} = \sqrt{-p}$.

(ii): Sei $m \in \mathbb{Z} \setminus \{0,1\}$ quadfrei, $m = \pm p_1 \cdots p_s$, die p_i prim, sei $n = kgV(8, p_1, \dots, p_s)$.
Nach (i) ist $\sqrt{p_j} \in \mathbb{Q}(e^{2\pi i/p_j})$ für $p_j \equiv 1 \ (4)$, $i\sqrt{p_j} \in \mathbb{Q}(e^{2\pi i/p_j})$ für $p_j \equiv 3 \ (4)$,
im 2. Fall also $\sqrt{p_j} \in \mathbb{Q}(e^{2\pi i/8}, e^{2\pi i/p_j})$, da $i \in \mathbb{Q}(e^{2\pi i/8})$.
Weiter ist $\sqrt{2} \in \mathbb{Q}(e^{2\pi i/8})$, denn $\sqrt{2} = \left(\frac{1}{2}\sqrt{2} + \frac{i}{2}\sqrt{2}\right) - \left(-\frac{1}{2}\sqrt{2} + \frac{i}{2}\sqrt{2}\right) = e^{\frac{2\pi i}{8}} - \left(e^{\frac{2\pi i}{8}}\right)^3$.
Es folgt $\sqrt{m} \in \mathbb{Q}(e^{2\pi i/8}, e^{2\pi i/p_1}, \dots, e^{2\pi i/p_s}) = \mathbb{Q}(e^{2\pi i/n})$, also $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(e^{2\pi i/n})$.

□

6.24. **Bem.:** Es gilt der **Satz von Kronecker-Weber:** Jede abelsche (Galois-) Erweiterung von $\mathbb{Q}$ ist in einem Kreisteilungskörper enthalten.
[s. [A. Leutbecher: Zahlentheorie - Eine Einführung in die Algebra], §17.5 Satz 6]