Zerfällungskörper von f (denn $f=(X-\alpha)(X-\beta)$ in $L[X] \rightsquigarrow \beta \in L$)

Dann ord $Gal(L/K) = [L:K] = \text{grad } f = 2 \rightsquigarrow Gal(L/K) = \mathbb{Z}/2\mathbb{Z}$

$= \{ Id, \alpha \mapsto \beta \}$.

(ii) Sei char $K \neq 2,3$, $f = X^3 + aX + b \in K[X]$

($g = X^3 + c_1X^2 + c_2X + c_3 \overset{ch \neq 3}{\rightsquigarrow} g\left(X - \frac{1}{3}c_1\right) = X^3 + \underbrace{(c_1 - c_1)}_{=0}X^2 + \dots$

hat Gestalt wie f und derselbe Zerfkö und gleiche Galoisgruppe)

Angenommen f hat keine Nst. in $K \overset{grad=3}{\rightsquigarrow} f$ irred.

Also ist f separabel (hat keine Nst von Vielfachheit 2 oder 3 wegen 3.5.4 oder Blatt 12 und char $K \neq 2,3$).

Sei $\alpha \in \overline{K}$ eine Nst. von f. Dann $[K(\alpha):K] = 3$.

1. Fall $L = K(\alpha)$ Zerfällungskörper von f. Dann $Gal(L/K) \cong \mathbb{Z}/3\mathbb{Z}$.

2. Fall Sonst sei $L \supset K(\alpha)$ der Zerf körper von $f \rightsquigarrow L$ Zerfkö über $K(\alpha)$ von $f/(X-\alpha) = g$ irred über $K(\alpha)$. Also

$[L:K] = [L:K(\alpha)][K(\alpha):K] = 2.3 = 6 \rightsquigarrow$ ord $Gal(L/K) = 6$

Da $Gal(L/K) \hookrightarrow S_3 \rightsquigarrow Gal(L/K) \cong S_3$

Wie kann man entscheiden, ob 1. oder 2. Fall eintreten?

Sei $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in L$ und $\Delta := \delta^2$

Vieta-Formeln: $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = a$,

$\alpha_1\alpha_2\alpha_3 = -b \rightsquigarrow \Delta = -4a^3 - 27b^2$, δ ist Wurzel von Δ.

Es gilt: $\forall \sigma \in Gal(L/K): \sigma(\delta) = \delta \iff \sigma|_{\{\alpha_1,\alpha_2,\alpha_3\}}$ gerade Perm.

$\Updownarrow$ $\qquad\qquad$ $\Updownarrow$

$\delta \in K \qquad\qquad Gal(L/K) = A_3$

Also $Gal(L/K) \cong A_3 \cong \mathbb{Z}_3 \iff \Delta$ hat eine Wurzel in K.

4.3. Einheitswurzeln und Konstruktionen mit Zirkel und Lineal

Sei K Körper, $\overline{K}$ alg. Abschluss von K.

4.3.1 Def Sei $n \in \mathbb{N}$. Setze $U_n = \{\text{Nullstellen von } X^n - 1 \text{ in } \overline{K}\}$
U_n heißt Gruppe der n-ten Einheitswurzeln in $\overline{K}$ (ist Gruppe!)

4.3.2 Satz (i) U_n ist zyklisch
(ii) Falls $\operatorname{char} K \nmid n$, so $\operatorname{ord} U_n = n$, also $U_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$
(iii) Falls $\operatorname{char} K = p \mid n = p^r \cdot n'$ mit $\operatorname{ggT}(p, n) = 1$ so ist
$X^{n'} - 1$ separabel und $U_n = U_{n'}$

Beweis (i) U_n endliche Untergruppe von $\overline{K}^*$ $\overset{\text{ÜBlatt 11}}{\rightsquigarrow}$ U_n zyklisch
(ii) $(X^n - 1)' = nX^{n-1} \neq 0$, da $n \neq 0$
(iii) $(X^{n'} - 1)^{p^r} = X^n - 1$ und Blatt 12. ▤

4.3.3. Def Eine primitive Einheitswurzel ist $\zeta \in U_n$ mit $\langle \zeta \rangle = U_n$.

4.3.4. Korollar Falls $\operatorname{char} K \nmid n$, so gibt es genau $\operatorname{ord} (\mathbb{Z}/n\mathbb{Z})^* = \varphi(n) := \#\{a \in \{1, \dots, n\} : \operatorname{ggT}(a, n) = 1\}$ primitive Einheitswurzeln in $\overline{K}$. Ist $\zeta \in U_n$ primitiv, so ζ^r primitiv $\Leftrightarrow \operatorname{ggT}(r, n) = 1$

Beweis $\hat{a} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \operatorname{ggT}(a, n) = 1$ □

4.3.5 Satz Sei $K = \mathbb{Q}$, $\zeta \in \overline{\mathbb{Q}}$ primitive n-te EHW.
Dann ist der *n-te Kreisteilungskörper* $\mathbb{Q}(\zeta)$ galois/$\mathbb{Q}$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Beweis $\mathbb{Q}(\zeta)$ enthält $\zeta, \zeta^2, \dots, \zeta^n = 1$ also $U_n \rightsquigarrow \mathbb{Q}(\zeta)$ ist Zerfällungskörper zu $X^n - 1 \in \mathbb{Q}[X]$.
$X^n - 1$ separabel $\underset{4.1.2(ii)}{\rightsquigarrow}$ $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ galois. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$
Übung ▤

Ist also $f \in \mathbb{Q}[X]$ das Minpol. zu ζ, so $\operatorname{grad} f = \varphi(n)$.
Seien $\zeta_1, \dots, \zeta_{\varphi(n)}$ die primitiven EHW in $\overline{\mathbb{Q}} \subset \mathbb{C}$.
Das Minpol. $f = (X-\zeta_1)\dots(X-\zeta_{\varphi(n)})$ heißt <u>n-tes Kreisteilungspolynom</u> über $\mathbb{Q}$.

Z.B. $n=2, \varphi(2)=1, \zeta=-1, f=X+1$
$n=3, \varphi(3)=2, \zeta = e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}, f = X^2+X+1$
$n=4, \varphi(4)=2, \zeta = \pm i, f = X^2+1$
$n=5, \varphi(5)=4, \zeta = e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}},$
$f = X^4+X^3+X^2+1$

<u>4.3.6 Satz</u> K Körper, $\operatorname{char} K \nmid n$, $\zeta \in \overline{K}$ primitive n-te EHW. Dann gilt

(i) $K \subset K(\zeta)$ galois, $\operatorname{Gal}(K(\zeta)/K)$ abelsch, $[K(\zeta):K] \le \varphi(n)$

(ii) $\forall \sigma \in \operatorname{Gal}(K(\zeta)/K)\ \exists!\ \hat{r} = \hat{r}_\sigma \in (\mathbb{Z}/n\mathbb{Z})^*$: $\sigma(\zeta) = \zeta^r$
($r = r_\sigma$ ist unabhängig von ζ)

(iii) ψ: $\operatorname{Gal}(K(\zeta)/K) \to (\mathbb{Z}/n\mathbb{Z})^*$, $\sigma \mapsto r_\sigma$ ist ein injekt. Homom. und Isom. falls $K = \mathbb{Q}$.

<u>Beweis</u> (i) $K \subset K(\zeta)$ galois, da $K(\zeta)$ Zerfällungskörper des seperablen Pol. X^n-1. Rest nach (iii).

(ii) Da ζ primitiv, ist auch $\sigma(\zeta)$ primitiv $\rightsquigarrow \exists r \in \{1,\dots,n-1\}$ $\operatorname{ggT}(r,n)=1$ mit $\sigma(\zeta)=\zeta^r$. Ist $\zeta^r = \zeta^s$, so $r \equiv s \pmod n$ da $\langle\zeta\rangle = U_n \cong \mathbb{Z}/n\mathbb{Z} \rightsquigarrow \hat{r}$ eindeutig bestimmt.
Unabh. von ζ: sei ζ^m andere prim. EHW, $\sigma(\zeta) = \zeta^r$
$\rightsquigarrow \sigma(\zeta^m) = \sigma(\zeta)^m = (\zeta^r)^m = (\zeta^m)^r$.

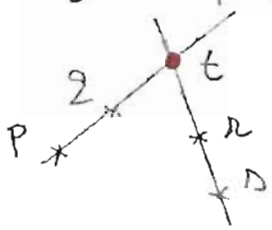
(iii) ψ Homom: $(\tau\sigma)(\zeta) = \tau(\zeta^{r_\sigma}) = \zeta^{r_\sigma r_\tau}$ ✓
ψ inj: $r_\sigma = 1 \rightsquigarrow \sigma(\zeta)=\zeta \rightsquigarrow \sigma(\zeta^k) = \zeta^k\ \forall k \rightsquigarrow \sigma = \mathrm{Id}_{K(\zeta)}$
$K = \mathbb{Q} \underset{4.3.5}{\rightsquigarrow}$ ord $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \varphi(n) \rightsquigarrow \psi$ auch surj. ∎

4.3.7 Korollar ζ primitive n-te EHW in $\overline{\mathbb{Q}} \rightsquigarrow \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

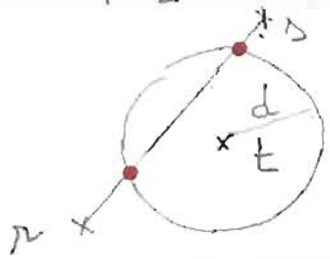
Bem. $(\mathbb{Z}/n\mathbb{Z})^*$ ist i. A. nicht zyklisch, z.B. $(\mathbb{Z}/8\mathbb{Z})^* = \{\hat{1},\hat{3},\hat{5},\hat{7}\} \cong V_4$, wohl aber wenn n prim ist, z.B. $(\mathbb{Z}/7\mathbb{Z})^* = \{\hat{1},\hat{2},\hat{3},\hat{4},\hat{5},\hat{6}\} = \langle\hat{2}\rangle = \ldots = \langle\hat{6}\rangle$.

4.3.8 Def. Sei $M \subset \mathbb{C}$. Ein Punkt $z \in \mathbb{C}$ heißt mit Zirkel und Lineal aus M konstruierbar: $\Leftrightarrow \exists M' \subset \mathbb{C}$ mit $M \cup \{z\} \subset M'$ so dass M' durch endlich viele Schritte der folgenden Typen aus M entsteht:

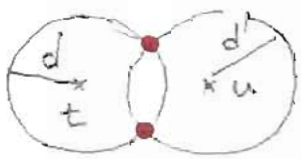
(1) $P, Q, R, S \in M$ und t = Schnitt der Geraden $\overline{PQ}$ und $\overline{RS}$, so füge M den Pkt t hinzu



(2) $P, Q, R, S, t \in M$, $d = d(P,Q) \rightsquigarrow$ füge M die Schnittpkt der Gerade $\overline{RS}$ mit dem Kreis $C_d(t)$.



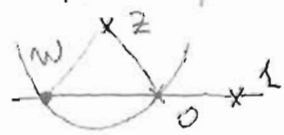
(3) $P, Q, R, S, t, u \in M$ $\quad d = d(P,Q)$, $d' = d(R,S)$

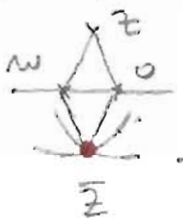


$\rightsquigarrow$ füge M die Schnittpkt. $C_d(t) \cap C_{d'}(u)$ hinzu.

Sei $K(M) = \{z \in \mathbb{C} : z \text{ mZu} \Sigma \text{ aus } M \text{ konstruierbar}\}$

Bem. Ist $0,1 \in M$, so $\overline{M} = \{\overline{z} : z \in M\} \subset K(M)$, insb. $K(M) = K(M \cup \overline{M})$

Beweis 

$\rightsquigarrow$ 

Typ (2) Typ (3)