8.15 Def Sei $L \supset K$ eine endliche Körpererweiterung. Ein Element $a \in L$ heißt primitives Element der Körpererweiterung $L \supset K$, falls $L = K[a]$.

8.16 Satz (von primitiven Element)
Jede endliche Körpererweiterung besitzt ein primitives Element.

Beispiel $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$

$a = \sqrt{2} + \sqrt{3}$; $a^2 = 2 + 3 + 2\sqrt{6}$ $(a^2 - 5)^2 = 24$

$x^4 - 10x + 1 \in \mathbb{Q}[x]$ ist das Minimalpolynom von a.

Also $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$

und $[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}] = 4$

$\Rightarrow \mathbb{Q}[\sqrt{2} + \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ □

Beweis: Sei $\tilde{L} \subset L = K[a_1, \dots, a_n] \supset K$ der Zerfällungskörper von $f = f_1 \cdot \dots \cdot f_n$, wobei f das Produkt der Minimalpolynome von den a_k über K ist. $\tilde{L}$ ist dann auch der Zerfällungskörper von f über K, also $\tilde{L} \supset K$ eine Galoiserweiterung mit Gruppe $G = \mathrm{Aut}(\tilde{L}; K)$. Da G endlich ist hat G nur endlich viele Untergruppen und dabei $\tilde{L}_G \supset K$ nur endlich viele Zerfällungskörper. Das gleiche trifft auch auf $L \supset K$ zu.
Die Zerfällungskörper von $L \supset K$ entsprechen den UG die $\mathrm{Aut}(\tilde{L}, L)$ umfassen

$$z \longleftrightarrow \mathrm{Aut}(\tilde{L}, z)$$

$L \supset z$ $\qquad$ $\mathrm{Aut}(\tilde{L}; L)$

Da G endlich ist, hat G nur endlich viele Untergruppen und daher $\tilde{L}$ nur endlich viele ~~Unterkörper~~ Zwischenkörper
Das gleiche trifft auf $L^{\circ K}_{zu}$.
Die Zwischenkörper von $L \supset K$ entsprechen Untergruppen, die $Aut(\tilde{L}, \overset{\circ\circ}{L})$ umfassen.

$$Z \overset{1:1}{\leftrightarrow} Aut(\tilde{L}; Z)$$

$L \supset Z$ $\qquad$ $Aut(\overset{\cup}{\tilde{L}}, L)$

L hat also endlich viele echte Zwischenkörper

$L \supsetneq Z \supset K$ etwa $Z_1, \dots, Z_m$

Wir zeigen, dass eine $a \in L$ existiert mit $a \notin Z_1 \cup \dots \cup Z_m$.
Da $K[a]$ ein Zwischenkörper ist $\neq Z_j$ muss

$K[a] = L$ gelten

8.16 Satz Sei K ein unendlicher Körper, $V \cong K^n$ ein endlich dimensionaler K-VR, $V_1, \dots, V_m \subsetneq V$ echte Untervektorräume. Dann gilt

$V \supsetneq V_1 \cup \dots \cup V_m$

Bem

i) Im Fall K ein unendlicher Körper impliziert Satz 8.16 den Satz 8.15:

$$L \supsetneq Z_1 \cup \dots \cup Z_m$$

da $Z_i \supset K$ K-Vektorräume sind.

ii) Im Fall $|K| = q < \infty$ ist auch $L \supset K$ ein endlicher Körper und jeder Erzeuger der zyklischen Gruppe $L^\times$ ist ein primitives Element von $L \supset K$ von Null verschiedenes

8.17 Satz Sei $f \in K[x_1, \dots, x_n]$ ein Polynom mit n Variablen über einem unendlichen Körper K.
Dann existiert ein Tupel $a = (a_1, \dots, a_n) \in K^n$ so dass $f(a) \neq 0$

Beweis von 8.17 $\Rightarrow$ 8.16.

Wir wählen eine Basis von V und bezeichnen mit $x_1, \dots, x_n \in V^*$ die duale Basis. Für jeden Untervektorraum $V_i \subsetneq V$ wählen wir eine von Null verschiedene Linearform $\neq 0$, $l_i \in K[x_1, \dots, x_n]$ so dass l_i eine der definierenden Gleichungen von $V_i \subset V$ ist. Also $a \in V_i \Rightarrow l_i(a) = 0$

Es sei $F = l_1 \cdot \dots \cdot l_m \in K[x_1, \dots, x_n]$.

Nach 8.17 existiert ein $a = (a_1, \dots, a_n) \in V \cong K^n$ so dass $F(a) \neq 0$ und damit $l_i(a) \neq 0$ und $a \notin V_i \; \forall i$ □

Beweis von Satz 8.17 Induktion nach n

Für $n=1$ hat ein Polynom $F \in K[x_1]$ nur endlich viele Nullstellen. Da $|K| = \infty$ gibt es eines mit $F(a) \neq 0$

Induktionsschritt: Sei

$F \in K[x_1, \dots, x_n] = K[x_1, \dots, x_{n-1}][x_n]$

von Null verschieden und

$g \in K[x_1, \dots, x_{n-1}]$ sein Leitkoeffizient.

Dann existieren $(a_1, \dots, a_{n-1}) \in K^{n-1}$, sodass

$g(a_1, \dots, a_{n-1}) \neq 0$

$f(a_1, \dots, a_{n-1}, x_n) \in K[x_n]$ ist dann nicht das Nullpolynom. Also $\exists a_n \in K$ mit

$f(a_1, \dots a_{n-1}, a_n) \neq 0$ □

Bem Satz 8.16 & 8.17 gelten nicht für endliche Körper. Zum Beispiel ist $f = \prod_{a \in F} (x-a) \in F[x]$ ein Polynom ~~ohne Nullstellen in F~~ welches $\forall a \in F$ eingesetzt 0 ergibt. ($= x^q - x$ für $q = |F|$)

und $F^n = \bigcup_{V \text{ 1-dim UVR}} V$ und in F^n gibt es lediglich

$$\frac{q^n - 1}{q - 1}$$ 1-dimensionale UVR gibt.

8.18 Def Sei R ein Integritätsring und $\sigma \in S_n$ eine Permutation.

S_n operiert auf $R[x_1, \dots, x_n]$ dem Polynomring mit n Variablen durch $\sigma \mapsto \varphi_\sigma : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$, $x_i \mapsto x_{\sigma(i)}$

Ein Polynom f in $R[x_1, \dots x_n]$ heißt symmetrisch, wenn $\varphi_\sigma(f) = f \quad \forall \sigma \in S_n$

Beispiele sind die elementarsymmetrischen Polynome

$$s_1 = x_1 + x_2 + \dots + x_n$$

$$s_2 = x_1 x_2 + x_2 x_3 + \dots + x_{n-1} x_n$$

$$\vdots$$

$$s_k = \sum_{1 \le i_1 < \dots < i_k \le n} \prod_{j=1}^{k} x_{i_k}$$

$$\vdots$$

$$s_n = x_1 \cdots x_n$$

Die Menge der symmetrischen Funktionen bildet einen Unterring $S \subset R[x_1, \dots, x_n]$

8.19 Satz Der Ring der symmetrischen Funktionen ist

$$S = R[s_1, \dots, s_n]$$

Mit anderen Worten: Jede symmetrische Funktion ist ein Polynom in $s_1, \dots, s_n$.

Beispiel Potenzsummen

$$P_k(x_1, \dots, x_n) = x_1^k + \dots + x_n^k$$

$P_2 = s_1^2 - 2 s_2$. Man kann zeigen

$$\mathbb{Q}[P_1, \dots, P_n] = \mathbb{Q}[S_1, \dots, S_n]$$

aber $\mathbb{Z}[P_1, \dots, P_n] \subsetneq \mathbb{Z}[S_1, \dots, S_n]$

Wir verwenden Galoistheorie

S_n operiert auch auf $K(x_1, \dots x_n) = \mathbb{Q}(R[x_1, \dots, x_n])$

wobei $K = Q(R)$

8.20 Satz $K(x_1, \dots, x_n) \supset K(S_1, \dots, S_n)$ ist eine Galoiserweiterung mit Gruppe S_n.

Beweis Betrachte $f \in K[x_1, \dots x_n][X]$

$$f = (X - x_1)(X - x_2) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \dots + (-1)^n s_n$$

$\in K[s_1, \dots, s_n][X]$

$K(x_1, \dots, x_n)$ ist also der Zerfällungskörper von $f \in K(s_1, \dots, s_n)[X]$ und separabel über $K(s_1, \dots, s_n)$, da die $x_i \neq x_j$ für $i \neq j$.

Also $[K(x_1, \dots, x_n) : K(s_1, \dots, s_n)] \leq n!$

Andererseits gilt

$\mathrm{Fix}(S_n) = K(s_1, \dots, s_n)$

und es gilt

$[K(x_1, \dots, x_n) : \mathrm{Fix}(S_n)] = |S_n| = n!$

$\Rightarrow \mathrm{Fix}(S_n) = K(s_1, \dots, s_n)$

Beweis für 2.1a Das Minimalpolynom von x_1

$$f = \prod_{i=1}^{n} (X - x_i) = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n$$

hat Koeffizienten in $R[s_1, \dots, s_n]$ und ist normiert vom Grad n.

$1, x_1, \dots, x_1^{n-1}$

bilden daher ein Erzeugendensystem von

$R[s_1, \dots, s_n, x_1]$ als $R[s_1, \dots, s_n]$-Modul

Als nächstes betrachten wir das Minimalpolynom von x_2 über $K(s_1, \dots, s_n, x_1)$

$f = (X - x_1) f_2$

f_2 entsteht aus f durch abdividieren von $(X - x_1)$

f_2 hat Koeffizienten in $R[s_1, \dots, s_n, x_1]$

$1, x_2, \dots, x_2^{n-2}$ ist ein Erzeugendensystem von

$R[s_1, \dots, s_n, x_1, x_2]$ als $R[s_1, \dots, s_n, x_n]$-Modul.

Induktiv erhalten wir

$x_1^{\nu_1} \dots x_n^{\nu_n}$ mit $0 \leq \nu_k \leq n - k$

bildet ein Erzeugendensystem von

$R[s_1, \dots, s_n, x_1, x_2 \dots x_n] = R[x_1, \dots, x_n]$ als

$R[s_1,\dots,s_n]$-Modul.

Diese n! vielen Elemente bilden auch ein Erzeugendensystem in $K(x_1,\dots,x_n)$ als $K(s_1,\dots,s_n)$-Vektorraum.

Also sind $x_1^{\nu_1}\cdots x_n^{\nu_n}$ $K(s_1,\dots,s_n)$-linear unabhängig und daher

$R[x_1,\dots,x_n]$ ein freier $R[s_1,\dots,s_n]$-Modul

mit diesen Monomen als Basis

Es folgt

$$K(s_1,\dots,s_n) \cap R[x_1,\dots,x_n] = R[s_1,\dots,s_n]$$

(und $K(s_1,\dots,s_n) \cap K[x_1,\dots,x_n] = K[s_1,\dots,s_n]$) □

§9 Anwendungen der Galoistheorie

1. Konstruktion mit Zirkel und Lineal.

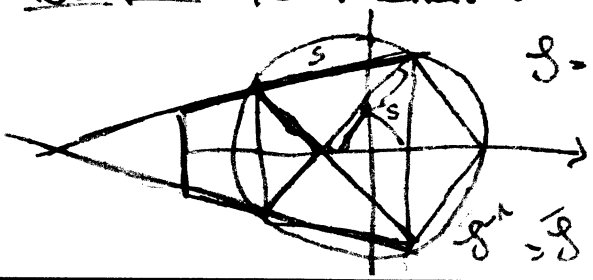
9.1 Def Eine Konstruktion mit Zirkel und Lineal besteht in jedem Konstruktionszustand aus endlich vielen Punkten $p \in \mathbb{R}^2$, Geraden und Kreisen, die einen Schritt wie folgt erweitert werden darf.

1) Die Hinzunahme einer Geraden durch 2 schon konstruierte Punkte

2) Die Hinzunahme eines Kreises mit Mittelpunkt eines schon konstruierten Punkt mit Radius Abstand zweier schon konstruierter Punkte

3) Hinzunahme eines Schnittpunkts zweier schon konstruierter Geraden Gerade und Kreis oder zweier Kreise.

Beispiel Konstruktion des regulären 5-Ecks



$\zeta = e^{\frac{2\pi i}{5}}$

$\zeta^5 = 1$

Korrektheit $\mathbb{R}^2 = \mathbb{C}$

Es gilt $\zeta^5 = 1$ und $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$

$a = \zeta + \zeta^{-1} = 2 \operatorname{Re} \zeta$

$x^2 + a - 1 = \zeta^2 + \zeta^{-2} + 2 + \zeta + \zeta^{-1} - 1 = \frac{\zeta^5 - 1}{\zeta - 1 / \zeta^2} = 0$

$a = -\frac{1}{2} + \sqrt{\frac{1}{4} + 1} = \frac{1}{2}(-1 + \sqrt{5})$

$\operatorname{Re} \zeta = \frac{a}{2} = \frac{1}{4}(-1 + \sqrt{5})$

$1 - \frac{1}{4} + \frac{i}{2} = \sqrt{\left(\frac{1}{4}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{1}{4}\sqrt{5}$

Also $-\frac{1}{4} + \frac{1}{4}\sqrt{5} = \operatorname{Re} \zeta$

Gegeben endliche viele Punkte $M \subset \mathbb{C}$. Welche Punkte lassen sich aus M in endl. vielen Schritten mit Zirkel und Lineal konstruieren?

Für ~ 2000 J war die folgende Aufgabe offen

1) Delisch Problem (430 B.C.) Verdopplung des Würfels: Konstruktion von $\sqrt[3]{2}$ aus $\{0,1\}$

2) Dreiteilung des Winkels

3) Quadratur des Kreises: Konstruktion $\sqrt{\pi}$ aus $\{0,1\}$

4) Konstruktion von regulären n-Ecken $n \geq 7$

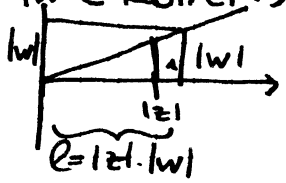
9.2 Satz Es sei $\{0,1\} \subset M \subset \mathbb{C}$. Die Menge der aus M durch Zirkel und Lineal konstruierbaren Punkte $\operatorname{Kon}(M) \subset \mathbb{C}$ bildet einen Unterkörper von $\mathbb{C}$.
$\operatorname{Kon}(M)$ ist abgeschlossen unter Quadratwurzeln.

Bew: 1) $z \in \operatorname{kon}(M) \Leftrightarrow \operatorname{Re} z, \operatorname{Im} z \in \operatorname{Kon}(M)$.
Wir können mit Zirkel und Lineal das Lot fällen und die Senkrechte errichten.

2) $z, w \in \operatorname{Kon}(M) \Rightarrow z + w \in \operatorname{Kon}(M)$ wegen 1)
reicht die Addition von $\begin{matrix} \operatorname{Re} z + \operatorname{Re} w \\ \operatorname{Im} z + \operatorname{Im} w \end{matrix}$ zu konstruieren.

3) $z, w \in \operatorname{Kon}(M) \Rightarrow z \cdot w \in \operatorname{Kon}(M)$

a) $|z| \cdot |w| \in Kon(M)$ sehen wir aus dem Strahlensatz



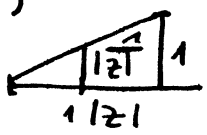
$|z| : 1 = \ell : |w|$

$\Rightarrow \ell = |z| \cdot |w|$

b) Können Winkel addieren

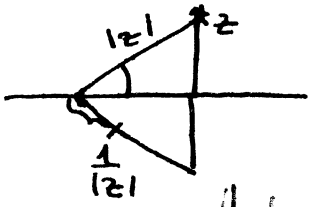
4) $z \in Kon(M), z \neq 0 \Rightarrow \frac{1}{z} \in Kon(M)$

a) $\frac{1}{|z|}$ geht mit dem Strahlensatz

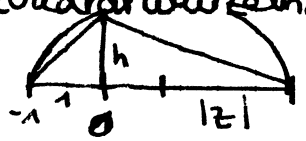


b) Können Winkel spiegeln

(-1) Multiplikation

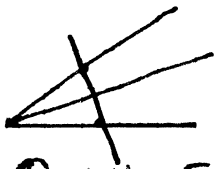


5) Quadratwurzeln a) $\sqrt{|z|}$ geht mit dem Höhensatz



$|h|^2 = 1 \cdot |z|$ Bew: 3 × Pythagoras

b) Können Winkel halbieren



9.3 Satz Sei $\{0,1\} \subset M \subset \mathbb{C}$ und $K = \mathbb{Q}(M)$. Ein Punkt $z \in \mathbb{C}$ lässt sich mit Zirkel und Lineal aus M konstruieren genau dann, wenn es eine Folge $z_1, \dots, z_n$ von Punkten gibt, so $K_i = K_{i-1}(z_i) \supset K_{i-1}$ mit $K_0 = K$, Quadratische Körpererweiterungen sind und $z \in K_n$. Insbesondere ist z algebraisch über K und $[K[z] : K] = 2^r$

9.4 Korollar (Wantzel, 1837). Die Verdopplung des Würfels mit Zirkel und Lineal ist unmöglich.

Bew Müssten $\sqrt[3]{2}$ mit Zirkel und Lineal konstruieren

Aber $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, da $x^3 - 2$ das Minimalpolynom ist

Wäre $\sqrt[3]{2}$ konstruierbar, so wär $\mathbb{Q}[\sqrt[3]{2}] \subset K_n$ mit $[K_n : \mathbb{Q}] = 2^n$, aber $3 \nmid n$ ein Widerspruch.

$$\underbrace{[K_n : \mathbb{Q}]}_{2^n} = [K_n : \mathbb{Q}[\sqrt[3]{2}]] \cdot \underbrace{[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]}_{3} \quad \lightning$$

Bew Vonsatz 8.3 Sei $w_1, \dots, w_N$ die Punkte, die wir sukzessive in einer Konstruktion von $w_N = z$ konstruieren.

Der Schnittpunkt zweier Geraden hat Koordinaten im gleichen Körper wie die Koeffizienten der Gleichung wie ~~die beiden~~ zu $p_1 = x_1 + iy_1, p_2 = x_2 + iy_2$ ist die Geradengleichung

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$ Koeffizienten in $\mathbb{Q}(\mathrm{Re}\,p_1, \mathrm{Re}\,p_2, \mathrm{Im}\,p_1, \mathrm{Im}\,p_2)$

also zwei Geraden, die schon konstruiert sind geben uns einen Punkt mit Real- und Imaginärteil im gleichen Körper. #

Bei Schnitt einer Geraden $ax + by + c = 0$ mit einem Kreis $(x - x_0)^2 + (y - y_0)^2 = r^2$ gibt einsetzen eine quadratische Gleichung für Realteil ($b \neq 0$) oder Imaginärteil ($a \neq 0$). Also reicht eine bestenfalls quadratische Körpererweiterung um die Koordinaten des Schnittpunktes zu bekommen. Für zwei Kreise

$$(x - x_1)^2 - (y - y_1)^2 = r_1^2, \quad (x - x_2)^2 + (y - y_2)^2 = r_2^2$$

liefert die Differenz die Geradengleichung mit Koeffizienten im Körper der $x_1, y_1, x_2, y_2, r_1, r_2$ enthält. Also $K(w_1, \dots, w_i) \subset K(w_1, \dots, w_{i+1})$ eine Körpererweiterung von Grad ≤ 2 und durch eventuelles weglassen finden wir $z_1, \dots, z_m$.

Korollar 3-teilung des Winkels ist unmöglich.

Beweis: ~~cos~~ $\cos(\alpha) = 4\cos^3\left(\frac{\alpha}{3}\right) - 3\cos\left(\frac{\alpha}{3}\right)$

folgt aus dem Additionstheorem für sin und cos

$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$ für $e^{i(\alpha+\beta)} = e^{i\alpha} \cdot e^{i\beta}$

$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha \cdot \sin\beta$

$$\cos\alpha = \cos\left(\frac{\alpha}{3} + \frac{2\alpha}{3}\right) = \cos\frac{\alpha}{3}\cos\frac{2\alpha}{3} - \sin\frac{\alpha}{3}\sin\frac{2\alpha}{3}$$

$$= \cos^3\frac{\alpha}{3} - \cos\frac{\alpha}{3}\sin^2\frac{2\alpha}{3} - 2\sin^2\frac{\alpha}{3}\cos\frac{\alpha}{3}$$

$$= \cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}\underbrace{\sin^2\frac{\alpha}{3}}_{1-\cos^2\frac{\alpha}{3}}$$

$$= 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}$$

$c = \cos\alpha$ vorgegeben sollen wir eine Lösung der Gleichung $4x^3 - 3x - c = 0$ konstruieren.

$\mathbb{Q}(c)[x]$

Für $c \in [-1,1]$ welches transzendent über $\mathbb{Q}$ ist, ist $4x^3 - 3x - c \in \mathbb{Q}[c,x]$ irreduzibel, da $\mathbb{Q}[c,x]/(4x^3-3x-c) \cong \mathbb{Q}[x]$

Also $4x^3 - 3x - c$ ein Primideal erzeugt.

$\Rightarrow$ Gauß $4x^3 - 3x - c \in \mathbb{Q}(c)[x]$ ist irreduzibel

also $[\mathbb{Q}(c)[\cos\frac{\alpha}{3}] : \mathbb{Q}(c)] = 3 \nmid 2^n$

2-ter Beweis: Zeigen, dass das reguläre 9-Eck nicht konstruierbar ist. $\vartheta = e^{\frac{2\pi i}{9}}$ $\vartheta^9 = 1$; $(\vartheta^9 - 1) : (\vartheta^3 - 1) = \vartheta^6 + \vartheta^3 + 1$

Also $x^6 + x^3 + 1 \in \mathbb{Q}[x]$ ist das Minimalpolynom

$\vartheta^3 + 1 + \vartheta^{-3} = 0$ $\quad a = \vartheta + \vartheta^{-1} = 2\,\mathrm{Re}\,\vartheta$,

$a^3 - 3a + 1 = 0$ $\quad x^3 - 3x + 1 \in \mathbb{Q}[x]$ ist Minimalpolynom von a, da ± 1 keine NST'en sind

Also $[\mathbb{Q}[a] : \mathbb{Q}] = 3 \nmid 2^n$

Satz (Lindemann) Die Quadratur des Kreises ist unmöglich, da $\sqrt{\pi}$ und π transzendent über $\mathbb{Q}$ sind.

Bsp: Reguläre 7-Ecke lässt sich nicht konstruieren

$\vartheta = e^{\frac{2\pi i}{7}}$ $\quad \vartheta^6 + \vartheta^5 + \vartheta^4 + \vartheta^3 + \vartheta^2 + \vartheta + 1 = 0$

$\vartheta^3 + \vartheta^2 + \vartheta + 1 + \vartheta^{-1} + \vartheta^{-2} + \vartheta^{-3} = 0$

$a = \vartheta + \vartheta^{-1} = 2\,\mathrm{Re}\,\vartheta$

$a^3 + a^2 - 2a - 1 = 0$ $\quad x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ irreduzibel

Also $[\mathbb{Q}[a] : \mathbb{Q}] = 3 \nmid 2^n$

Gauß 1796 als 18-jähriger

hat das reguläre 17-Eck lässt sich mit Zirkel und Lineal konstruieren.

Kreisteilungskörper

9.4 Definition K Körper und $n \in \mathbb{N}_{>0}$.
Es bezeichne in diesem Abschnitt K_n den Zerfällungskörper von $x^n - 1 \in K[x]$. Ein Element $\zeta \in K_n$ mit $\zeta^n = 1$ nennt man eine n-te Einheitswurzel und $E_n(K) \subset K_n$ bezeichne die Menge der n-ten Einheitswurzeln. $E_n(K)$ ist eine endliche Untergruppe von $(K_n^\times, \cdot)$.
Die Elemente von $E_n(K)$ die präzise die Ordnung n haben nennt man primitive n-te Einheitswurzeln und deren Mengen bezeichnen wir mit $PE_n(K)$.

Bem: $n \geq 1$
1) $E_n(\mathbb{Q}) = \{ e^{2\pi i \frac{\nu}{n}} \mid 0 \leq \nu < n \} \subset \mathbb{C}$
2) p Primzahl, $\mathbb{F}_q$ der Körper mit $q = p^r$-Elementen dann ist jedes Element von $\mathbb{F}_q^\times$ eine $(q-1)$-te Einheitswurzel.
3) Ist $d \mid n$, dann ist $x^d - 1$ ein Teiler von $x^n - 1$. Wir können daher K_d als einen Unterkörper von K_n auffassen.
4) ist K Körper mit $\mathrm{char}(K) = p > 0$ und $n = mp$ dann gilt: $E_m(K) = E_n(K)$ da $x^n - 1 = (x^m)^p - 1^p$
$= (x^m - 1)^p \in K[x]$.
5) $E_n(K)$ ist stets eine zyklische Untergruppe von $K_n^\times$. Die Ordnung ist n falls $\mathrm{char}(K) \nmid n$

Beweis: Sei $E \subset K^\times$ eine endliche Untergruppe mit Ordnung $|E| = r$. Dann ist E zyklisch.
$(E, \cdot) \cong \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2 \oplus \dots \oplus \mathbb{Z}/d_k$
mit $1 < d_1 \mid d_2 \mid d_3 \dots \mid d_k$ die Elementarteiler.
Dann gilt $r = d_1 \dots d_k$. Wäre $k > 1$, so hätte jedes Element $\zeta \in E$ eine Ordnung $s \leq d_k < r$, wäre also Nullstelle

von $x^g - 1$. Dieses Polynom hat nicht genügend Nullstellen, was $|E| = r$ entspricht

e) Für jeden Körper K ist $K_n \supset K$ eine Galoiserweiterung.

Beweis: Wegen $K_n = K_m$ für $n = p^r \cdot m$, $p \nmid m$ $p = \mathrm{char}(K)$ können wir uns auf $\mathrm{char}(K) \nmid n$ zurückziehen. Dann hat das Polynom $x^n - 1$ keine mehrf. NSTen und $K_m \supset K$ ist demzufolge Galoisch.

f) Ist $\zeta \in E_n(K)$ eine primitive n-te Einheitswurzel, dann ist ζ^k ebenfalls eine primitive n-te Einheitswurzel genau dann, wenn $ggT(k, n) = 1$

Bew $d = ggT(k, n) = uk + vn$.

$k = k_1 d$, $n = n_1 d$. Dann gilt

$(\zeta^k)^{n_1} = \zeta^{k_1 d n_1} = \zeta^{k_1 n} = 1^{k_1} = 1$

Also falls ζ_k hat Ordnung höchstens $n_1 < n$ falls $d > 1$

Da $\zeta^{ku} = \zeta^d$ Ordnung präzise n_1 hat kann ζ^k keine kleinere Ordnung als n_1 haben.