K Körper, $n > 1$

- K_n der Zerfällungskörper von $x^n - 1 \in K[x]$.
- $E_n(K) \subset K_n$ die Gruppe der n-ten Einheitswurzeln.
- $PE_n(K)$, primitive n-ten Einheitswurzeln die Erzeuger von $E_n(K)$
- $\mathrm{char}(K) = p$, $n = p \cdot m$

$$x^n - 1 = (x^m)^p - 1^p = (x^m - 1)^p$$

gilt $K_n = K_m$ OE $\mathrm{char}(K) \nmid n$ $\quad K_n \supset K$ galoisch.

9.5 <u>Satz</u> Sei n teilerfremd zu $\mathrm{char}(K)$

Dann ist die Galoisgruppe $\mathrm{Aut}(K_n, K)$ isomorph zu einer Untergruppe der Einheitengruppe $(\mathbb{Z}/n)^\times$ des Rings $\mathbb{Z}/n$. Im Fall $K = \mathbb{Q}$ gilt

$$\mathrm{Aut}(\mathbb{Q}_n ; \mathbb{Q}) \cong (\mathbb{Z}/n)^\times$$

$$\left(\mathbb{Q}_n = \mathbb{Q}[e^{\frac{2\pi i}{n}}]\right)$$

<u>Beweis</u>: Sei ζ eine primitive n-te Einheitswurzel und $\varphi \in \mathrm{Aut}(K_n ; K)$. Dann ist wegen $(\varphi(\zeta))^n = \varphi(\zeta^n) = \varphi(1) = 1$ $\quad \varphi(\zeta)$ ebenfalls eine n-te Einheitswurzel und wegen $1 = (\varphi(\zeta))^d = \varphi(\zeta^d)$ für $d \mid n$.

$$\Leftrightarrow 1 = \zeta^d$$ ebenfalls eine primitive n-te Einheitswurzel

Die Abbildung $\mathrm{Aut}(K_n ; K) \to (\mathbb{Z}/n)^\times$

$$\varphi \mapsto k + n\mathbb{Z}$$

wobei $\varphi(\zeta) = \zeta^k$ mit $ggT(k, n) = 1$ ist wohldefiniert.

und injektiv, da φ durch $K_n = K[\zeta] \to K[\zeta]$

$$\zeta \mapsto \zeta^k$$

eindeutig festgelegt ist.

Sie ist ein Gruppenhomomorphismus, da für $\psi \in \mathrm{Aut}(K_n ; K)$ ein weiterer Automorphismus mit etwa $\psi(\zeta) = \zeta^l$

$$(\varphi \circ \psi)(\zeta) = \varphi(\psi(\zeta)) = \psi(\zeta^k) = (\psi(\zeta))^k = (\zeta^l)^k = \zeta^{lk}$$

gilt, also $\varphi \circ \psi \mapsto l \cdot k + n\mathbb{Z}$

$\overset{\shortparallel}{(l+n\mathbb{Z})(k+l\mathbb{Z})}$ gilt.

Die letzte Aussage zeigen wir später $\square$

8.6 Def Die Abbildung $\varphi: \mathbb{N}_{\geq 2} \to \mathbb{N}$

$n \mapsto |\{1 \leq k < n \mid \mathrm{ggT}(k,n) = 1\}|$

heißt Eulersche φ-Funktion.

Also $\varphi(n) = |(\mathbb{Z}/n)^\times|$ (Ergänzend setzt man $\varphi(1) = 1$)

8.7 Satz (Eigenschaften der Eulerschen φ-Funktion)

1) $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$ für teilerfremde n, m

2) Für p Primzahl und $k \geq 1$ gilt
$\varphi(p^k) = p^k - p^{k-1}$

3) Für $n = p_1^{k_1} \cdots p_r^{k_r}$ die Primfaktorzerlegung gilt
$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_r^{k_r} - p_r^{k_r-1})$
$= n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right)$

Beweis: 1) Für n, m teilerfremd gilt
$\mathbb{Z}/n \cdot m \cong \mathbb{Z}/n \times \mathbb{Z}/m$ und deshalb
$(\mathbb{Z}/n \cdot m)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$

2) Die Nichteinheiten in $\mathbb{Z}/p^k\mathbb{Z}$ bilden das Ideal
$p\mathbb{Z}/p^k\mathbb{Z}$. Es gibt also p^{k-1} Nichteinheiten
und damit $p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ Einheiten.

3) Folgt mit 1) und 2). $\square$

8.8 Def Für char$(K) \nmid n$ gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln in K_n. Das n-te Kreisteilungspolynom

$\Phi_n(x) = \prod (x-\varepsilon) \quad \varepsilon \in PE_n(K)$

Also $\deg \Phi_n(x) = \varphi(n)$.
Da $\mathrm{Aut}(K_n ; K)$ die primitiven n-ten Einheitswurzeln permutiert, gilt

$$\Phi_n(x) \in K[x]$$

Sie liegen sogar im Primkörper von K.

<u>3.9 Satz</u>

1) Es gilt
$$n = \sum_{d|n} \varphi(d)$$

2) $$X^n - 1 = \sum_{d|n} \Phi_d(x).$$

<u>Bemerkung</u>: Die Φ_n lassen sich mit dieser Formel rekursiv berechnen.

$$\Phi_1 = x-1$$
$$\Phi_2 = x+1 = (x^2-1):(x-1)$$
$$\Phi_3 = x^2+x+1 = (x^3-1):(x-1)$$
$$\Phi_4 = x^2+1 = (x^4-1):(x-1)(x+1)$$
$$\Phi_5 = x^4+x^3+x^2+x+1$$
$$\Phi_6 = x^2-x+1, \text{ da } (x^6-1):(x^2-1) = x^4+x^2+1$$
$$x^4+x^2+1 : \Phi_3 = x^2-x+1$$
$$\vdots$$

<u>Bem</u>: Berechnet man $\Phi_1, \dots, \Phi_{100}$ so könnte man zu der Vermutung gelangen, dass alle Koeffizienten ± 1 oder 0 sind. Dies ist jedoch falsch, Φ_{105} hat zwei Koeffizienten -2.
Man weiß: Die Menge der Koeffizienten aller Kreisteilungspolynome ist unbeschränkt.

<u>Beweis</u>: Jede n-te Einheitswurzel ist eine primitive d-te Einheitswurzel für genau einen Teiler d von n.
Also $E_n(x) = \dot{\bigcup}_{d|n} PE_d(x)$

und $x^n - 1 = \prod_{d|n} \Phi_d$ 1) folgt aus 2) $\square$

§. 10 Satz $\Phi_n \in \mathbb{Q}[x]$ ist irreduzibel und deshalb $[\mathbb{Q}_n : \mathbb{Q}] = n$ und $Aut(\mathbb{Q}_n ; \mathbb{Q}) \cong (\mathbb{Z}/n)^{\times}$

<u>Beweis:</u> $\Phi_n \in \mathbb{Z}[x]$ nach der Rekursion und ist normiert und $\Phi_n \in \mathbb{Q}[x]$ irreduzibel

$\Leftrightarrow \Phi_n \in \mathbb{Z}[x]$ irreduzibel nach Gauss.

Sei $f \in \mathbb{Z}[x]$ ein irreduzibler Faktor.

<u>Beh.:</u> Für jede Nullstelle ξ von f und jede Primzahl p mit $p \nmid n$ ist auch ξ^p eine Nullstelle von f.

Aus der Behauptung folgt $f = \Phi_n$.

Ist nämlich ξ^k eine primitive Einheitswurzel

$k = p_1 \cdot \ldots \cdot p_r < n$ so ist wegen der Behauptung auch ξ^{p_1} Nullstelle von f und $\xi^{p_1 \cdot p_2}$ usw. bis ξ^k NS von f

Also f hat wenigstens $\varphi(n)$ viele Nullstellen und daher $f = \Phi_n$ aus Gradgründen.

Zum Beweis der Behauptung betrachten wir eine Zerlegung

$\Phi_n = f \cdot g \in \mathbb{Z}[x]$

Wir wollen die Annahme $f(\xi^p) \neq 0$ zu einem Widerspruch führen. Ist dies der Fall so folgt $g(\xi^p) = 0$

ξ ist also dann eine Nullstelle von

$g(x^p) \in \mathbb{Z}[x]$.

Da f das Minimalpolynom von ξ über $\mathbb{Q}$ ist folgt

$g(x^p) = f \cdot h$ mit $h \in \mathbb{Q}[x]$. Es gilt sogar

$h \in \mathbb{Z}[x]$. Division mit Rest (f ist normiert) liefert $g(x^p) = f \cdot q + r$

mit $\deg r < \deg f$ und $q, r \in \mathbb{Z}[x]$

Die Eindeutigkeit von Division mit Rest zeigt $r = 0$, $h = q$.

Wir betrachten die Koeffizientenreduktion $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$
$$f \mapsto \overline{f}$$

Aus $g(x^p) = f \cdot h$ folgt $(\overline{g}(x))^p = (\overline{g}(x^p)) = \overline{f} \cdot \overline{h}$

also $\overline{g}^p = \overline{f} \cdot \overline{h}$.

Da f normiert ist, ist $\overline{f}$ nicht das Nullpolynom und jeder irreduzibler Faktor $\overline{f_0}$ von $\overline{f}$ ist wegen
$\overline{g}^p = \overline{f} \cdot \overline{h}$ auch ein Faktor von $\overline{g}$.

Also $\overline{f_0}^2$ ist ein Faktor von $\overline{\Phi_n} = \overline{f} \cdot \overline{g}$ und damit auch ein Faktor von $x^n - 1$, da $\overline{\Phi}_n \mid x^n - 1$.

Aber $x^n - \overline{1}$ hat keine mehrfachen Faktoren, da $p \nmid n$ ein Widerspruch. □

9.11 Folgerung

Das reguläre n-Eck lässt sich mit Zirkel und Lineal aus $\{0, 1\}$ konstruieren genau dann, wenn
$\varphi(n)$ eine 2-Potenz ist.

Beweis: ~~Wohldefinie~~ Notwendigkeit ist klar, da
$[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.

Dies ist auch hinreichend, da $G := Aut(\mathbb{Q}_n ; \mathbb{Q})$ zyklisch ist und deshalb eine Auflösung
$G = N_0 \supset N_1 \supset \ldots \supset N_r = \{e\}$, wobei $[N_{i-1} ; N_i] = 2$
d.h. N_{i-1} ist Normalteiler von index 2.
$\mathbb{Q} = Fix(G) \subset Fix(N_1) \subset \ldots \subset Fix(N_r) = \mathbb{Q}_n$ sind jeweils quadratische Körpererweiterungen. □

9.12 Def. + Satz

Eine Primzahl der Gestalt $p = 2^n + 1$ heißt Fermatsche Primzahl. Primzahlen dieser Gestalt haben alle die Form
$p = 2^{2^k} + 1$ also $n = 2^k$

Bew: Ist $n = m \cdot 2^r$, m ungerade so gilt
$-p = -2^{m \cdot 2^r} - 1 = (-2^{2^r})^m - 1$

was von $-2^{2^r}-1$ geteilt wird und deshalb p keine Primzahl.

9.12 <u>Satz</u> Das reguläre n-Eck lässt sich mit Zirkel und Lineal genau dann konstruieren, wenn n die Gestalt $n = 2^k p_1 \cdots p_r$, wobei $p_1, \dots, p_r$ paarweise verschiedene Fermat'sche Primzahlen sind.

<u>Bew:</u> Für solche Zahlen ist
$$\varphi(n) = \underbrace{(2^k - 2^{k-1})}_{2^{k-1}} \cdot 2^{2^{k_1}} \cdots 2^{2^{k_r}}$$
eine 2-Potenz. Für andere Zahlen nicht.

$n = p^\ell \cdot m$ mit p, m teilerfremd, $p > 2$, $\ell \geq 2$

so wird $\varphi(n) = (p^\ell - p^{\ell-1}) \cdot \varphi(m)$ von p geteilt. $\square$

<u>Bem:</u> Bezeichne $F_k = 2^{2^k}+1$ so sind $F_0 = 2^{2^0}+1 = 3$, $F_1 = 2^2+1 = 5$ $F_2 = 2^4+1 = 17$, $F_3 = 2^8+1 = 257$ $F_4 = 2^{16}+1 = 65537$ Primzahlen

$F_5 = 2^{32}+1$ hat aber 641 als Teiler (Euler) ist also keine Fermat'sche Primzahl. Weitere sind nicht bekannt

3. Auflösung durch Radikale

<u>Motivation</u>: Eine quadratische Gleichung $x^2+px+q=0$ kann man mit der Formel $x_{1,2} = -\frac{p \pm \sqrt{p^2-4q}}{2}$ lösen.

Bei kubischen Gleichungen $x^3+ax^2+bx+c=0$ kann man den 2. höchsten Koeffizienten durch den Koordinatenwechsel $x \mapsto x - \frac{a}{3}$ auf die Gestalt

(*) $x^3+3px+2q=0$ bringen ($\operatorname{char} K \neq 2,3$)

<u>Cardanosche Formeln</u>

Es sei $u = \sqrt[3]{-q+\sqrt{q^2+p^3}}$, $v = \sqrt[3]{-q-\sqrt{q^2+p^3}}$ und ζ eine primitive 3-te Einheitswurzel, wobei die 3-ten Wurzeln so gewählt sind, dass $u \cdot v = -p$ gilt.

Dann sind $u+v$, $\zeta u+\zeta^2 v$, $\zeta^2 u+\zeta v$

die drei Nullstellen von (*)

<u>Bew:</u> $(u+v)^3 = u^3+v^3+3uv(u+v)$

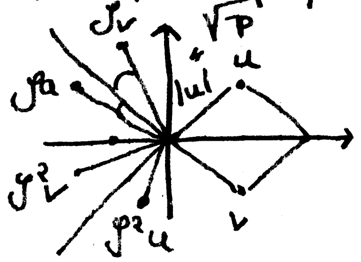
$$= -2q - 3p(u+v) \quad \square$$

<u>Bem:</u> Im Fall $K=\mathbb{R}$ kann man falls $q^2+p^3\geq 0$ u und v reell wählen.

Dann ist $u+v\in\mathbb{R}$ die reelle Lösung und $\overline{\zeta u+\zeta^2 v} = \bar{\zeta} u+\bar{\zeta}^2 v = \zeta^2 u+\zeta v$ ein Paar von konjugiert komplexen Lösungen.

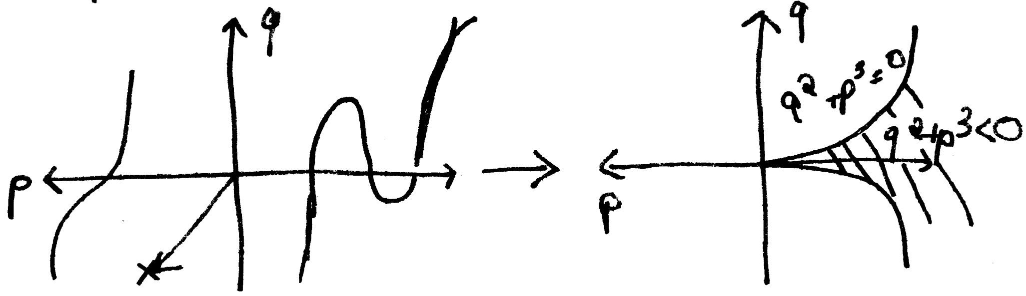
Im Fall $q^2+p^3<0$ ($\Rightarrow p<0$) brauchen wir komplexe Zahlen

$|u|^3 = |-q + i\sqrt{-q^2-p^3}\,| = \sqrt{q^2-q^2-p^3} = \sqrt{-p^3}$, $|u|=\sqrt{-p}$



$\overline{\zeta u+\zeta^2 v} = \zeta^2\bar{u} + \zeta\bar{v} = \zeta^2 v + \zeta u \in\mathbb{R}$

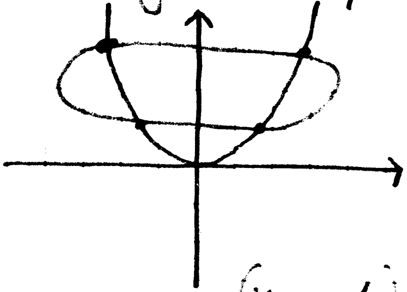
$2q = -3px - x^3$



Randbemerkung, die nichts mit Algebra zu tun hat.
Cardanos Formel hat Ferro und ~~Targlia~~ Tartaglia um 1515 entdeckt und zunächst geheim gehalten. 1545 hat Cardano die Formel veröffentlicht, was erheblichen Streit verursacht hat.

Für Polynome 4-ten Grades hat Ferrari ~1540 eine Formel entdeckt, die nur $\sqrt[3]{\ }$ und $\sqrt[2]{\ }$ beinhaltet:
$x^4+ax^2+bx+c=0$ zu betrachten. betrachten wir das

Gleichungssystem $y-x^2=0$ $y^2+ayx+by^2+cx+d=0$



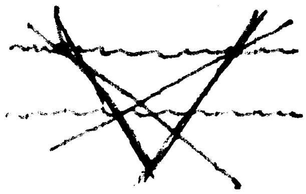
Im Beispiel:

$$q_t = t(y-x^2)+(yx+ay^2+bx+c)$$

gibt es drei reduzible Quadrate

$$(x,y,1)\underbrace{\begin{pmatrix} M \\ \text{linear \& const.} \\ \text{in } t \end{pmatrix}}_{3\times 3}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

det M ist ein kubisches Polynom in t mit 3 Nullstellen.



Kubische Gleichung lösen gibt eins der 3 Geraden Paare

1 Gerade auswählen (~ quadratische Gleichung)

1 der zwei Punkte auf dieser Geraden eine quadratische Gleichung.

Es stellt sich die Frage, ob für Polynome Grad $n \geq 4$ eine Formel für Nullstellen existiert, die nur $\sqrt[k]{\ }$ und Einheitswurzeln verwendet.

Die Antwort lautet: Nein, der Beweis beruht auf Galois-Theorie.

Der erste Schritt besteht darin Galoiserweiterungen mit zyklischer Galoisgruppe zu charakterisieren.

6.15 <u>Definition</u> Ein Polynom $f \in K[x]$ der Gestalt $f = x^n - a$, $a \in K \setminus \{0\}$ nennt man ein reines Polynom und jede Lösung ~~von~~ ~~f(x)~~ $f=0$ (in einem Oberkörper) eine n-te Wurzel aus a.

Ist char (K) kein Teiler von n, dann ist f separabel. Den Zerfällungskörper von f können wir dann in 2 Schritten bilden. Zunächst bilden wir den Zerfällungskörper von x^n-1 also den Körper $K_n = K[\zeta]$ ζ primitive n-te Einheitswurzel $L = K_n[b]$, ist der Zerfällungskörper, da $b, \zeta b, \dots, \zeta^{n-1} b$ die n verschiedenen

Nullstellen von f sind und L muss K_n umfassen, da die Quotienten $\frac{\varphi b}{b} = \zeta^k$ die Einheitswurzeln

8.16 <u>Satz</u> Sei $a \in K^\times$ und L der Zerfällungskörper von $X^n - a \in K[X]$. Dann gilt:

1) Das Polynom $X^n - 1$ zerfällt über L in Linearfaktoren. Wir können daher K_n als Unterkörper von L auffassen.

2) Ist b irgendeine n-te Wurzel aus a dann ist:

$$L = K_n[b]$$

3) Ist ζ eine primitive n-te Einheitswurzel; Dann gilt

$$X^n - a = \prod_{k=0}^{n-1} (x - \zeta^k b)$$

4) $L \supset K$, $L \supset K_n$ und $K_n \supset K$ sind Galoisch.

5) $\mathrm{Aut}(L; K_n)$ ist isomorph zu einer Untergruppe $\mathbb{Z}/n\mathbb{Z}$. Sie ist zyklisch und ihre Ordnung teilt n.

6) ist $X^n - a$ irreduzibel in $K_n[X]$ dann ist

$$\mathrm{Aut}(L; K_n) \cong \mathbb{Z}/n.$$

<u>Bew</u>: 1), 2) und 3) haben wir eingesehen.

4) $L \supset K_n$ und $K_n \supset K$ sind Zerfällungskörper von die separablen Polynom $x^n - a$ bzw. $x^n - 1$

5) Sei $\varphi \in \mathrm{Aut}(L; K_n)$. Dann gilt

$\varphi(b) = \zeta^k b$ Die Abbildung

$$\mathrm{Aut}(L; K) \to \mathbb{Z}/n$$
$$\varphi \mapsto k + n\mathbb{Z}$$

ist wohldefiniert und injektiv, da $L = K_n[b] \xrightarrow{\varphi} K_n[b]$ durch $b \mapsto \zeta^k b$ eindeutig bestimmt ist.

Ist $\psi \in \mathrm{Aut}(L; K_n)$ ein weiterer Automorphismus etwa $\psi(b) = \zeta^l \cdot b$ und es gilt

$$(\psi \circ \varphi)(b) = \psi(\zeta^k b) = \zeta^k \psi(b) = \zeta^{l+k} b$$

Also $Aut(L;K_n) \to \mathbb{Z}/n$ ist Gruppenhomomorphismus

b) Ist $X^n - a \in K_n[X]$ irreduzibel so gilt

$$n = [L : K_n] = |Aut(L;K_n)|,$$ also das

Bild die ganze Gruppe $\mathbb{Z}/n$.

<u>8.17 Corollar</u> Sei K Körper, $n \in \mathbb{N}$ mit $char(K) \nmid n$ und K enthalte eine primitive n-te Einheitswurzel ζ. Ist $L \supset K$ eine Galoiserweiterung vom Grad n mit zyklischer Galoisgruppe, dann existiert ein $b \in L^\times$ sodass $b^n \in K$. $L = K[b]$ ist dann der Zerfällungskörper von $X^n - b^n \in K[X]$.

<u>Beweis</u>: Sei $\varphi \in Aut(L;K)$ ein Erzeuger.

Also $Aut(L;K) = \{id, \varphi, \dots, \varphi^{n-1}\}$.

Wir betrachten für $c \in L$ die Lagrange Resolvente

$$b = c + \zeta\varphi(c) + \zeta^2\varphi^2(c) + \dots + \zeta^{n-1}\varphi^{n-1}(c)$$

Nach Artins Satz gibt es ein $c \in L$ sodass $b \neq 0$. Andernfalls wäre $id + \zeta\varphi + \dots + \zeta^{n-1}\varphi^{n-1} = 0$ eine Abhängigkeitsrelation von n paarweise verschiedenen Charakteren $L^\times \to L^\times$, was Artins Satz widerspricht.

Wir berechnen $\varphi(b)$

$$\varphi(b) = \underbrace{\varphi(c) + \zeta\varphi^2(c) + \dots + \zeta^{n-1}(\underbrace{\varphi^n(c)}_{=c})}_{=\zeta^{-1}b}$$

Es folgt $\varphi(b^n) = (\varphi(b))^n = (\zeta^{-1}b)^n = b^n \in Fix(\varphi) = K$

Also b ist eine Lösung der reinen Gleichung

$$X^n - b^n \in K[X]$$

und da $\varphi|_{K_n[b]} \in Aut(K_n(b);K_n)$ und $\varphi^k(b) = \zeta^{-k}b$ für $k = 0, \dots, n-1$ verschiedene Werte hat gilt $|Aut(K_n(b);K_n)| \geq n$

$$n = [L:K] = [L:K_n(b)]\underbrace{[K_n(b):K]}_{\geq n} \Rightarrow L = K_n[b]$$ $\square$