KAPITEL 7

Einheitswurzeln - Kreisteilungskörper

1. Einheitswurzeln

Für einen Körper K bezeichnet K^* die multiplikative Gruppe, also $K \setminus \{0\}$ mit der Multiplikation. Ein Element $\zeta \in K$ hat **endliche Ordnung**, wenn ein $n \in \mathbb{N}$ existiert mit $\zeta^n = 1$. Man nennt dann ζ auch eine **n-te Einheitswurzel**, da die Gleichung $\zeta^n = 1$ an $\zeta = \sqrt[n]{1}$ denken lässt. Die Elemente endlicher Ordnung in K^* sind also die Einheitswurzeln von K. Die Menge der n-ten Einheitswurzeln in K schreibt man auch als

$$\mu_n(K) = \{\zeta \in K : \zeta^n = 1\}.$$

$\mu_n(K)$ ist eine Untergruppe von K^*. Da die n-ten Einheitswurzeln die Nullstellen des Polynoms $x^n - 1$ sind, ist klar, dass

$$|\mu_n(K)| \leq n$$

gilt.

Beispiele:

(1) Für jeden Körper K gilt $\mu_1(K) = \{1\}$ und $\mu_2(K) = \{1, -1\}$. (Ist $\mathrm{char}(K) = 2$, so ist $1 = -1$ und daher $\mu_2(K) = \{1\}$.)

(2) Es ist

$$\mu_n(\mathbb{R}) = \begin{cases} \{1, -1\}, & \text{falls } n \equiv 0 \bmod 2, \\ \{1\}, & \text{falls } n \equiv 1 \bmod 2 \end{cases}$$

(Ist $\zeta^n = 1$, so folgt $|\zeta|^n = 1$, und damit $|\zeta| = 1$, also $\zeta \in \{\pm 1\}$.)

Wir erinnern an die **Ordnung** eines Elements g einer multiplikativ geschriebenen Gruppe G (mit neutralem Element 1):

$$\mathrm{ord}\,(g) = \begin{cases} \min\{m \in \mathbb{N} : g^m = 1\}, & \text{falls } \{m \in \mathbb{N} : g^m = 1\} \neq \emptyset, \\ \infty & \text{sonst.} \end{cases}$$

Das folgende Lemma stellt nochmals ein paar Eigenschaften zusammen:

LEMMA. *Sei G eine multiplikativ geschriebene Gruppe mit neutralem Element 1 und $g \in G$ von endlicher Ordnung.*

(1) *Für $k \in \mathbb{Z}$ gilt:*

$$g^k = 1 \quad \Longleftrightarrow \quad \mathrm{ord}\,(g) \mid k.$$

(2) *Für $k, l \in \mathbb{Z}$ gilt:*

$$g^k = g^l \quad \Longleftrightarrow \quad k \equiv l \bmod \mathrm{ord}\,(g).$$

(3) *Die von g erzeugte Untergruppe ist*

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{\mathrm{ord}\,(g)-1}\} \quad \textit{mit} \quad |\langle g \rangle| = \mathrm{ord}\,(g).$$

(4) *Für $k \in \mathbb{Z}$ gilt*

$$\mathrm{ord}\,(g^k) = \frac{\mathrm{ord}\,(g)}{\mathrm{ggT}(\mathrm{ord}\,(g), k)}.$$

(5) *Hat auch $h \in G$ endliche Ordnung und ist $gh = hg$, so gilt die Implikation.*

$$\mathrm{ggT}(\mathrm{ord}\,(g), \mathrm{ord}\,(h)) = 1 \quad \Longrightarrow \quad \mathrm{ord}\,(gh) = \mathrm{ord}\,(g)\mathrm{ord}\,(h).$$

Datei: kt_ew.tex. Version vom 24.6.2024

(6) *Ist G endlich, so gilt*

$$\operatorname{ord}(g) \mid |G|.$$

Beispiel: Durch Ausprobieren findet man in $\mathbb{F}_{11}$:

$\zeta \in \mathbb{F}_{11}^*$	1	2	3	4	5	6	7	8	9	10
$\operatorname{ord}(\zeta)$	1	10	5	5	5	10	10	10	5	2

Ein Element $\zeta \in K^*$ nennt man eine **primitive n-te Einheitswurzel**, wenn $\operatorname{ord}(\zeta) = n$ gilt.

Der folgende Satz beschreibt $\mu_n(K)$, also die Gruppe der n-ten Einheitswurzel im Fall, dass eine primitive n-te Einheitswurzel existiert.

SATZ. *Sei K ein Körper und $n \in \mathbb{N}$. Es existiere eine primitive n-te Einheitswurzel ζ in K. Dann gilt:*

(1) *Alle n-ten Einheitswurzeln liegen in der von ζ erzeugten Untergruppe:*

$$\mu_n(K) = \langle\zeta\rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} \quad \text{und} \quad |\mu_n(K)| = n.$$

(2) *Für $k \in \mathbb{Z}$ gilt:*

$$\zeta^k \text{ ist eine primitive } n\text{-te Einheitswurzel} \iff \operatorname{ggT}(k, n) = 1.$$

(3) *Die Menge der primitiven n-ten Einheitswurzeln in K ist*

$$\{\zeta^k : 0 \le k \le n-1 \text{ und } \operatorname{ggT}(n, k) = 1\}.$$

Es gibt daher $\varphi(n)$ primitive n-te Einheitswurzeln. (Dabei bezeichnet $\varphi(n)$ die Eulersche φ-Funktion)

Beweis:

(1) Die von ζ erzeugte Untergruppe enthält n Elemente und ist in $\mu_n(K)$ enthalten. Da die Elemente von $\mu_n(K)$ Nullstellen des Polynoms $x^n - 1$ sind, hat $\mu_n(K)$ Elemente. Daher folgt sofort $\mu_n(K) = \langle\zeta\rangle$.

(2) Mit der Formel $\operatorname{ord}(\zeta^k) = \frac{\operatorname{ord}(\zeta)}{\operatorname{ggT}(\operatorname{ord}(\zeta), k)}$ erhält man

$$\begin{aligned} \zeta^k \text{ primitive } n\text{-te Einheitswurzel} &\iff \operatorname{ord}(\zeta^k) = n \iff \frac{n}{\operatorname{ggT}(n,k)} = n \iff \\ &\iff \operatorname{ggT}(n, k) = 1, \end{aligned}$$

wie behauptet.

(3) Dies folgt sofort aus (2), wenn man beachtet, dass nach Definition der Eulerschen φ-Funktion

$$\varphi(n) = |\{k \in \{0, 1, \ldots, n-1\} : \operatorname{ggT}(n, k) = 1\}|$$

gilt. ■

Bemerkung: Die Eulersche φ-Funktion $\varphi : N \to \mathbb{N}$ wird für $n \in \mathbb{N}$ durch

$$\varphi(n) = |\{k \in \{0, 1, \ldots, n-1\} : \operatorname{ggT}(n, k) = 1\}|$$

definiert. Wir erinnern an ein paar Eigenschaften:

- Für $n \in \mathbb{N}$ gilt
$$\varphi(n) = n \prod_{p \mid n} (1 - \frac{1}{p}).$$
- Ist $n = p_1^{e_1} \ldots p_r^{e_r}$ die Primfaktorzerlegung von n mit $e_1, \ldots, e_r \ge 1$, so gilt
$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1).$$
- Für $m, n \in \mathbb{N}$ gilt:
$$\operatorname{ggT}(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n).$$

- Für $n \in \mathbb{N}$ gilt

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|,$$

insbesondere gilt für $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Da die Einheitswurzeln in $\mathbb{C}$ eine wichtige Rolle spielen, formulieren wir wesentliche Aussagen als Satz:

SATZ. *Sei $n \in \mathbb{N}$. In $\mathbb{C}$ gilt:*

(1) $\zeta_n = e^{\frac{2\pi i}{n}}$ *ist eine primitive n-te Einheitswurzel.*
(2) *Die n-ten Einheitswurzeln in $\mathbb{C}$ sind*

$$\mu_n(\mathbb{C}) = \{\zeta_n^k : 0 \le k \le n-1\} = \{e^{\frac{2\pi i}{n} \cdot k} : 0 \le k \le n-1\}.$$

(3) $\zeta_n^k = e^{\frac{2\pi i}{n} \cdot k}$ *ist genau dann eine primitive n-te Einheitswurzel, wenn* $\mathrm{ggT}(n,k) = 1$ *gilt.*

Beweis: Wir müssen nur (1) zeigen, der Rest folgt aus dem allgemeinen Satz. Wir brauchen dafür die Charakterisierung

$$e^z = 1 \quad \Longleftrightarrow \quad z = 2\pi i \cdot m \text{ für ein } m \in \mathbb{Z}.$$

Daher gilt

$$\begin{aligned} \operatorname{ord}(\zeta_n) \mid m \quad &\Longleftrightarrow \quad \zeta_n^m = 1 \quad \Longleftrightarrow \quad e^{\frac{2\pi i}{n} \cdot m} = 1 \quad \Longleftrightarrow \quad \frac{2\pi i}{n} \cdot m = 2\pi i \cdot k \text{ für ein } k \in \mathbb{Z} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad m = nk \text{ für ein } k \in \mathbb{Z} \quad \Longleftrightarrow \quad n \mid m. \end{aligned}$$

Dies beweist $\operatorname{ord}(\zeta_n) = n$, d.h. ζ_n ist eine primitive n-te Einheitswurzel. ■

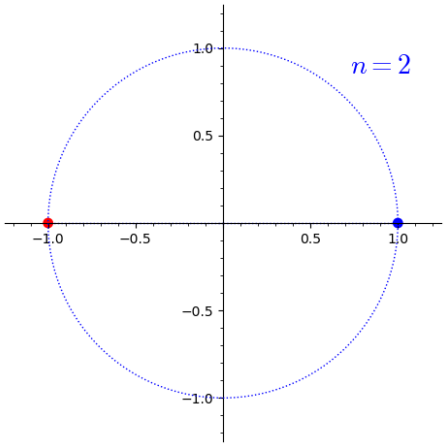
Beispiel: Einige komplexe Einheitswurzel lassen sich einfach angeben:

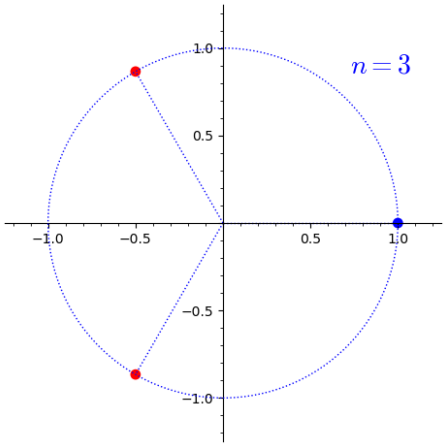
$$\zeta_1, \quad \zeta_2 = -1, \quad \zeta_3 = \frac{-1 + i\sqrt{3}}{2}, \quad \zeta_4 = i, \quad \zeta_6 = \frac{1 + i\sqrt{3}}{2}, \quad \zeta_8 = \frac{1+i}{\sqrt{2}}.$$

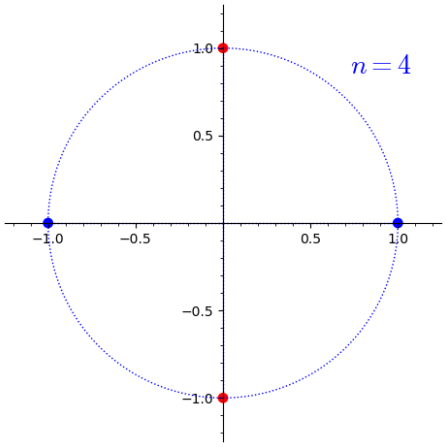
Hierbei ist ζ_n eine primitive n-te Einheitswurzel.

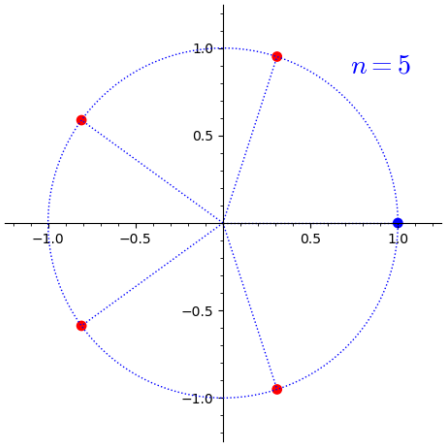
Beispiele: Zeichnet man die n-ten Einheitswurzeln in $\mathbb{C}$, so erhalt man ein regelmäßiges n-Eck (im Fall $n \ge 3$). Es gilt

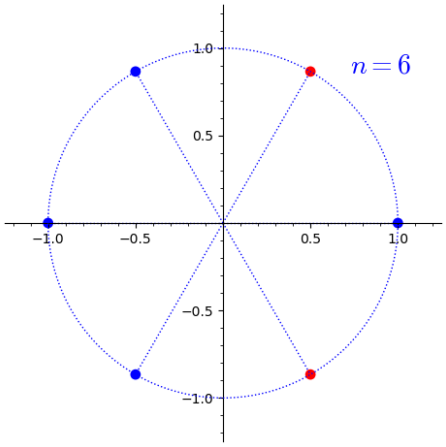
$$e^{\frac{2\pi i}{n} \cdot k} = \cos(\frac{2\pi}{n} \cdot k) + i \cdot \sin(\frac{2\pi}{n} \cdot k).$$

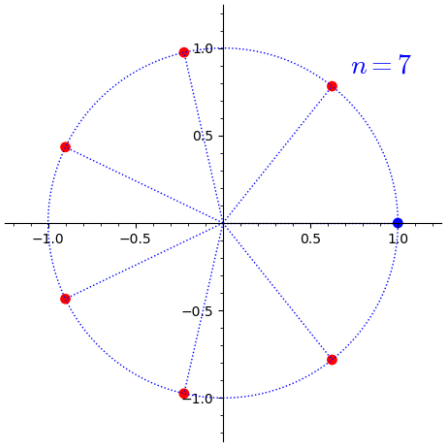

$n = 2$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0

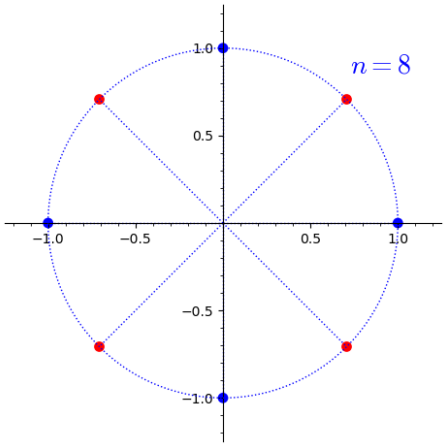

$n = 3$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0

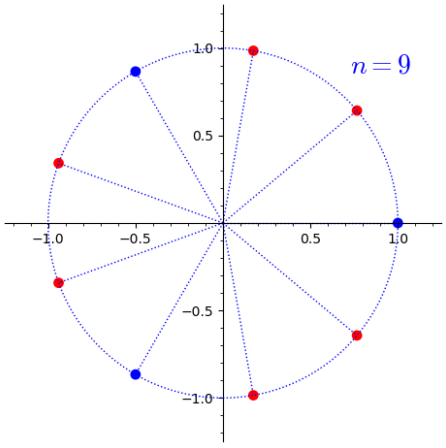

$n = 4$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0


$n = 5$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0


$n = 6$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0


$n = 7$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0


$n = 8$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0


$n = 9$
1.0
0.5
−1.0
−0.5
0.5
1.0
−0.5
−1.0

Aussagen über n-te Einheitswurzeln gelten auch in anderen algebraisch abgeschlossenen Körpern, wenn die Charakteristik des Körpers die Zahl n nicht teilt:

SATZ. *Sei K ein Körper und $n \in \mathbb{N}$, sodass die Charakteristik von K die Zahl n nicht teilt, d.h. $n \neq 0$ in K. Dann gilt im algebraischen Abschluss $\overline{K}$:*

(1) *$\mu_n(\overline{K})$ ist eine zyklische Gruppe der Ordnung n.*
(2) *Ist $\zeta \in \mu_n(\overline{K})$ ein Erzeuger von $\mu_n(\overline{K})$, so ist ζ eine primitive n-te Einheitswurzel.*
(3) *Es gibt genau $\varphi(n)$ primitive n-te Einheitswurzeln in $\overline{K}$, nämlich ζ^k mit $0 \leq k \leq n-1$ und* $\mathrm{ggT}(n,k) = 1$.

Beweis:

(1) Die Elemente von $\mu_n(\overline{K})$ sind gerade die Nullstellen des Polynoms $f = x^n - 1 \in K[x]$ im algebraischen Abschluss. Nun ist $f' = nx^{n-1}$, sodass aus $n \neq 0$ in K sofort $\mathrm{ggT}(f, f') = 1$ folgt. Das Polynom f ist also separabel, besitzt also n verschiedene Nullstellen in $\overline{K}$. Daher ist $|\mu_n(\overline{K})| = n$. $\mu_n(K)$ ist eine endliche Untergruppe von $\overline{K}^*$. Nun ist aber jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch. Daher ist $\mu_n(\overline{K})$ zyklisch, und es folgt die Behauptung.

(2) und (3) Dies ist klar. ■

In Charakteristik p existieren keine p-ten Einheitswurzeln (außer 1):

SATZ. *Ist K ein Körper der Charakteristik p, so gilt*

$$\mu_p(K) = \{1\}.$$

Beweis: Ist $\alpha \in \mu_p(K)$, so gilt $\alpha^p = 1$. Es folgt

$$0 = \alpha^p - 1 = \alpha^p - 1^p = (\alpha - 1)^p, \quad \text{also} \quad \alpha = 1.$$

Dies beweist die Behauptung. ■

2. Kreisteilungspolynome

Im Folgenden sei K ein Körper, der $\mathbb{Q}$ enthält, d.h. K hat Charakteristik 0.. Mit $\overline{K}$ bezeichnen wir wie üblich einen algebraischen Abschluss von K. Dann enthält $\overline{K}$ eine primitive n-te Einheitswurzel ζ_n. Es ist

$$\mu_n(\overline{K}) = \langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} \quad \text{mit} \quad |\mu_n(\overline{K})| = n.$$

Wir können zerlegen

$$\mu_n(\overline{K}) = \bigcup_{d|n} \{\zeta \in \overline{K}^* : \mathrm{ord}\,(\zeta) = d\}.$$

$\mu_n(\overline{K})$ ist die Nullstellenmenge des Polynoms $x^n - 1$. Daher gilt

$$x^n - 1 = \prod_{\substack{\zeta \in \overline{K} \\ \zeta^n = 1}} (x - \zeta) = \prod_{d|n} \left(\prod_{\substack{\zeta \in \overline{K}^* \\ \mathrm{ord}\,(\zeta) = d}} (x - \zeta) \right).$$

Wir setzen

$$\Phi_d(x) = \prod_{\substack{\zeta \in \overline{K}^* \\ \mathrm{ord}\,(\zeta) = d}} (x - \zeta)$$

und nennen Φ_n das n-te **Kreisteilungspolynom**. Wir erhalten dann

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

Da es genau $\varphi(n)$ Einheitswurzel der Ordnung n gibt, gilt

$$\mathrm{grad}(\Phi_n(x)) = \varphi(n).$$

Wir berechnen einige Polynome $\Phi_n(x)$ mittels der Formel $x^n - 1 = \prod_{d|n} \Phi_d(x)$, indem wir $x^n - 1$ zu faktorisieren versuchen:

$$\begin{aligned}
x-1 &= \Phi_1(x), \quad \text{also } \Phi_1(x) = x-1,\\
x^2-1 &= (x-1)(x+1) = \Phi_1(x)(x+1), \quad \text{also} \quad \Phi_2(x) = x+1,\\
x^3-1 &= (x-1)(x^2+x+1) = \Phi_1(x)(x^2+x+1), \quad \text{also} \quad \Phi_3(x) = x^2+x+1,\\
x^4-1 &= (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1) = \Phi_1(x)\Phi_2(x)(x^2+1),\\
&\quad \text{also} \quad \Phi_4(x) = x^2+1,\\
x^5-1 &= (x-1)(x^4+x^3+x^2+x+1) = \Phi_1(x)(x^4+x^3+x^2+x+1),\\
&\quad \text{also} \quad \Phi_5(x) = x^4+x^3+x^2+x+1,\\
x^6-1 &= (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x+1)(x^2-x+1) =\\
&= \Phi_1(x)\Phi_2(x)\Phi_3(x)(x^2-x+1),\\
&\quad \text{also} \quad \Phi_6(x) = x^2-x+1.
\end{aligned}$$

Für eine Primzahl p folgt aus

$$x^p - 1 = (x-1)(x^{p-1}+x^{p-2}+\cdots+x+1) = \Phi_1(x)(x^{p-1}+x^{p-2}+\cdots+x+1)$$

die Gleichung

$$\Phi_p(x) = x^{p-1}+x^{p-2}+\cdots+x+1.$$

Wir stellen die Ergebnisse nochmals zusammen:

$$\begin{aligned}
\Phi_1(x) &= x-1,\\
\Phi_2(x) &= x+1,\\
\Phi_3(x) &= x^2+x+1,\\
\Phi_4(x) &= x^2+1,\\
\Phi_5(x) &= x^4+x^3+x^2+x+1,\\
\Phi_6(x) &= x^2-x+1,\\
\Phi_p(x) &= x^{p-1}+x^{p-2}+\cdots+x+1 = \sum_{k=0}^{p-1} x^k \text{ für Primzahlen } p.
\end{aligned}$$

LEMMA. *$\Phi_n(x)$ ist ein normiertes Polynom aus $\mathbb{Z}[x]$ und kann rekursiv durch Polynomdivision mit der Formel*

$$\Phi_n(x) = \frac{x^n-1}{\prod_{\substack{d|n\\ d<n}} \Phi_d(x)}$$

berechnet werden, wenn man mit $\Phi_1(x) = x-1$ beginnt.

Beweis: Es ist $\Phi_1(x) = x-1$. Sei nun $n \geq 2$. Für alle $d \mid n$ und $d < n$ sei $\Phi_d(x)$ bereits bekannt. Da nach Voraussetzung $\Phi_d(x)$ ein normiertes Polynom aus $\mathbb{Z}[x]$ ist, ist auch

$$\prod_{\substack{d|n\\ d<n}} \Phi_d(x)$$

normiert und aus $\mathbb{Z}[x]$. Dividiert man $x^n - 1$ durch dieses Polynom, erhält man ein normiertes Polynom aus $\mathbb{Z}[x]$, nämlich $\Phi_n(x)$, der Rest ist 0. ■

SATZ. *Für $n \in \mathbb{N}$ ist das Polynom $\Phi_n(x) \in \mathbb{Z}[x]$ irreduzibel über $\mathbb{Q}$. Es gilt* $\operatorname{grad}(\Phi_n) = \varphi(n)$.

Beweis:

- Sei $f(x) \in \mathbb{Q}[x]$ ein irreduzibler (normierter) Teiler von $\Phi_n(x)$. Wir können zerlegen mit $\Phi_n(x) = f(x)g(x)$ mit $g(x) \in \mathbb{Q}[x]$. Wegen $\Phi_n(x) \in \mathbb{Z}[x]$ gilt auch $f(x), g(x) \in \mathbb{Z}[x]$.

- *Behauptung:* Gilt $f(\zeta) = 0$, so auch $f(\zeta^p) = 0$ für jede Primzahl p mit $p \nmid n$.
  Aus $f(\zeta) = 0$ folgt $\phi_n(\zeta) = 0$, d.h. ζ ist eine primitive n-te Einheitswurzel. Wegen $\mathrm{ggT}(n, p) = 1$ ist auch ζ^p eine primitive n-te Einheitswurzel. Also gilt $\Phi_n(\zeta^p) = 0$. Angenommen, $f(\zeta^p) \neq 0$. Dann folgt $g(\zeta^p) = 0$. Also ist ζ Nullstelle des Polynoms $g(x^p)$. Da f irreduzibel ist, ist f das Minimalpolynom von ζ, also folgt dann $f(x) \mid g(x^p)$. Es gibt also ein normiertes Polynom $h(x) \in \mathbb{Z}[x]$ mit $g(x^p) = f(x)h(x)$. Nun reduzieren wir modulo p, betrachten die Situation also in $\mathbb{F}_p[x]$: $\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$. Nun gilt aber $\overline{g}(x^p) = \overline{g}(x)^p$. Daher gilt $\overline{g}(x)^p = \overline{f}(x)\overline{h}(x)$. Es folgt $\mathrm{ggT}(\overline{f}, \overline{g}) \neq 1$. Das Polynom $\overline{\Phi_n}$ ist also nicht separabel, was aber nicht sein kann, da $x^n - 1$ modulo p separabel ist. Die Annahme war also falsch, d.h. es gilt $f(\zeta^p) = 0$, wie behauptet.
- *Behauptung:* Gilt $f(\zeta) = 0$ und für $k \in \mathbb{N}$ auch $\mathrm{ggT}(n, k) = 1$, so gilt $f(\zeta^k) = 0$.
  Beweis: Wir zerlegen $k = p_1 p_2 \dots p_r$ in ein Produkt von Primzahlen p_i mit $p_i \nmid n$. Nun wenden wir die zuvor bewiesene Aussage wiederholt an:

$$\begin{aligned} f(\zeta) = 0 \quad &\Longrightarrow \quad f(\zeta^{p_1}) = 0 \quad \Longrightarrow \quad f(\zeta^{p_1 p_2}) = f((\zeta^{p_1})^{p_2}) = 0 \quad \Longrightarrow \\ &\Longrightarrow \quad f(\zeta^{p_1 p_2 p_3}) = f((\zeta^{p_1 p_2})^{p_3}) = 0 \quad \Longrightarrow \quad \dots \\ &\Longrightarrow \quad f(\zeta^k) = f(\zeta^{p_1 p_2 \cdots p_r}) = f((\zeta^{p_1 \cdots p_{r-1}})^{p_r}) = 0. \end{aligned}$$

- Aus dem letzten Punkt folgt, dass alle primitiven n-ten Einheitswurzeln Nullstellen von f sind. Dies impliziert aber sofort $f = \Phi_n$. Daher ist Φ_n irreduzibel über $\mathbb{Q}$. ■

Bemerkung: Die oben angegebenen Kreisteilungspolynome haben nur $1, 0, -1$ als Koeffizienten. Das erste Kreisteilungspolynom, bei dem das nicht der Fall ist, ist Φ_{105} (vom Grad $\varphi(105) = \varphi(3 \cdot 5 \cdot 7) = 2 \cdot 4 \cdot 6) = 48$). Es gilt

$$\begin{aligned} \Phi_{105}(x) \quad = \quad & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + \\ & + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + \\ & + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1 \end{aligned}$$

(SAGE liefert das n-te Kreisteilungspolynom mit `cyclotomic_polynomial(`n`)`.)

Es gibt auch eine Reihe von Rechenregeln für Kreisteilungspolynome, die wir in der Vorlesung aber nicht benötigen. Die folgenden Aussagen sind dem Algebra-Buch von S. Lang entnommen:

SATZ. *Φ_n bezeichne das n-te Kreisteilungspolynom in $\mathbb{Z}[x]$.*

(1) *Für eine Primzahl p gilt*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

und für $e \geq 1$

$$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}}).$$

(2) *Für $n = p_1^{e_1} \dots p_r^{e_r}$ (Primfaktorzerlegung von n mit $e_1, \dots, e_r \geq 1$) gilt*

$$\Phi_n(x) = \Phi_{p_1 \dots p_r}(x^{p_1^{e_1 - 1} \cdots p_r^{e_r - 1}}).$$

(3) *Für ungerade natürliche Zahlen $n > 1$ gilt*

$$\Phi_{2n}(x) = \Phi_n(-x).$$

(4) *Ist p eine Primzahl und $n \in \mathbb{N}$, dann gilt*

$$\Phi_{pn}(x) = \begin{cases} \frac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{falls } p \nmid n, \\ \Phi_n(x^p), & \text{falls } p \mid n. \end{cases}$$

3. Kreisteilungskörper

Als Grundkörper wählen wir $\mathbb{Q}$. Einheitwurzeln können wir uns als Elemente von $\overline{\mathbb{Q}}$ oder als Elemente von $\mathbb{C}$ in der Gestalt $e^{\frac{2\pi i}{n}\cdot k}$ vorstellen.

DEFINITION. *Ist $\zeta_n \in \overline{\mathbb{Q}}$ (oder $\zeta_n \in \mathbb{C}$) eine primitive n-te Einheitswurzel, so nennt man $\mathbb{Q}(\zeta_n)$ einen* **Kreisteilungskörper**.

SATZ. *Sei $n \in \mathbb{N}$ und $\zeta_n \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel.*

(1) *Das Minimalpolynom von ζ_n über $\mathbb{Q}$ ist das Kreisteilungspolynom $\Phi_n(x)$.*
(2) *Es gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*
(3) *$\mathbb{Q}(\zeta_n)|\mathbb{Q}$ ist eine Galoiserweiterung.*
(4) *Durch*
$$(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}), \quad \overline{a} \mapsto \sigma_a \quad \text{mit} \quad \sigma_a(\zeta_n) = \zeta_n^a$$
wird ein Gruppenisomorphismus definiert.
(5) *$\mathbb{Q}(\zeta_n)$ ist eine abelsche Erweitung von $\mathbb{Q}$.*

Beweis:

(1) Wir haben gezeigt, dass Φ_n irreduzibel über $\mathbb{Q}$ ist. Wegen $\Phi_n(\zeta_n) = 0$ ist daher Φ_n das Minimalpolynom von ζ_n.
(2) Es ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \mathrm{grad}(\Phi_n) = \varphi(n)$.
(3) $\mathbb{Q}(\zeta_n)$ ist Zerfällungskörper des Polynoms $x^n - 1 \in \mathbb{Q}[x]$, also ist $\mathbb{Q}(\zeta_n)$ normal über $\mathbb{Q}$, und damit galoissch.
(4)
- Es ist
$$\Phi_n(x) = \prod_{\substack{0 \le a \le n-1 \\ \mathrm{ggT}(n,a)=1}} (x - \zeta_n^a).$$
Daraus erhalten wir die $\varphi(n)$ Automorphismen
$$\sigma_a : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n), \quad \sigma_a(\zeta_n) = \zeta_n^a.$$
Wegen $\zeta_n^a = \zeta_n^b \iff a \equiv b \bmod n$ können wir für a irgendeinen Repräsentanten von $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ wählen, d.h.
$$(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}), \quad \overline{a} \mapsto \sigma_a$$
ist bijektiv.
- Wir zeigen, dass die eben definierte Abbildung ein Gruppenhomomorphismus ist:
$$(\sigma_a\sigma_b)(\zeta_n) \quad = \quad \sigma_a(\sigma_b(\zeta_n)) = \sigma_a(\zeta_n^b) = \sigma_a(\zeta_n)^b = (\zeta_n^a)^b = \zeta_n^{ab} = \sigma_{ab}(\zeta_n).$$
Also gilt $\sigma_a\sigma_b = \sigma_{ab}$.

(5) Dies ist nun klar, da die Galoisgruppe abelsch ist. ■

Bemerkung zum Rechnen: Sei ζ eine primitive n-te Einheitswurzel, wobei wir $n \ge 3$ voraussetzen.

(1) Für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(n, a) = 1$ ist σ_a ein Automorphismus von $\mathbb{Q}(\zeta)$, der durch $\sigma_a(\zeta) = \zeta^a$ festgelegt ist. Es ist $\sigma_a = \sigma_b \iff a \equiv b \bmod n$.
(2) Ist $a_1, \ldots, a_{\varphi(n)}$ ein Repräsentantensystem von $(\mathbb{Z}/n\mathbb{Z})^*$, so gilt also
$$\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = \{\sigma_{a_1}, \ldots, \sigma_{a_{\varphi(n)}}\}.$$
(3) Ist (beispielsweise)
$$\zeta = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\,\sin(\frac{2\pi}{n}),$$
so ist
$$\overline{\zeta} = \cos(\frac{2\pi}{n}) - i\,\sin(\frac{2\pi}{n}) = \cos(-\frac{2\pi}{n}) + i\,\sin(-\frac{2\pi}{n}) = e^{-\frac{2\pi i}{n}} = \zeta^{-1} = \sigma_{-1}(\zeta).$$
Da die komplexe Konjugation auch ein Körperautomorphismus ist, folgt
$$\sigma_{-1} = \text{ komplexe Konjugation.}$$

(Natürlich gilt $\sigma_{-1} = \sigma_{n-1}$.)

(4) Für $a, b \in \mathbb{Z}$ gilt
$$\zeta^a = \zeta^b \quad \Longleftrightarrow \quad a \equiv b \bmod n.$$
Dies kann manchmal beim Rechnen hilfreich sein.

(5) Eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta)$ ist $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1}$. Manchmal kann auch die Wahl einer anderen Basis für das Rechnen vorteilhaft sein, wie wir in Beispielen sehen werden.

Beispiele: Sei ζ_n eine primitive n-te Einheitswurzel.

(1) Es ist $\varphi(n) = 1 \iff n \in \{1, 2\}$. Daher ist $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2) = \mathbb{Q}$. Für $n \geq 3$ gilt also $\mathbb{Q} \subsetneq \mathbb{Q}(\zeta_n)$.

(2) In den Übungen wird gezeigt: $\varphi(n) = 2 \iff n \in \{3, 4, 6\}$. Wegen
$$\zeta_3 = \frac{-1 + i\sqrt{3}}{2}, \quad \zeta_4 = i, \quad \zeta_6 = \frac{1 + i\sqrt{3}}{2}$$
ist
$$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{3}) \quad \text{und} \quad \mathbb{Q}(\zeta_4) = \mathbb{Q}(i).$$
$\mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(\sqrt{-3})$ sind also die einzigen quadratischen Kreisteilungskörper.

Beispiel: Wir betrachten $\mathbb{Q}(\zeta_5)$ mit einer primitiven 5-ten Einheitswurzel ζ_5. Wir schreiben kurz $\zeta = \zeta_5$. Es ist
$$(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} \quad \text{und} \quad \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\},$$
wobei $\sigma_a = \sigma_b \iff a \equiv b \bmod 5$ gilt. σ_1 ist das neutrale Element der Galoisgruppe, $\sigma_4 = \sigma_{-1}$ entspricht der komplexen Konjugation. Nun gilt
$$\sigma_2^2 = \sigma_2\sigma_2 = \sigma_4, \quad \sigma_2^3 = \sigma_4\sigma_2 = \sigma_8 = \sigma_3, \quad \sigma_2^4 = \sigma_3\sigma_2 = \sigma_6 = \sigma_1.$$
Also hat σ_2 Ordnung 4 und erzeugt die Galoisgruppe:
$$\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = \langle\sigma_2\rangle.$$
Eine zyklische Gruppe der Ordnung 4 hat genau eine nichttriviale Untergruppe, nämlich eine Untergruppe der Ordnung 2, also hier die Gruppe $\langle\sigma_{-1}\rangle$. Wir wollen den zugehörigen Fixkörper bestimmen. Das Minimalpolynom von ζ ist $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, sodass $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ gilt. Eine $\mathbb{Q}$-Basis ist $1, \zeta, \zeta^2, \zeta^3$. Wir wählen stattdessen die Basis $\zeta, \zeta^2, \zeta^3, \zeta^4$ und schreiben sie in der Form
$$\zeta, \quad \zeta^2, \quad \zeta^{-2}, \quad \zeta^{-1}.$$
σ_{-1} vertauscht ζ und ζ^{-1}, also bleibt
$$\alpha = \zeta + \zeta^{-1}$$
fest unter σ_{-1}. Wie finden wir das Minimalpolynom von α über $\mathbb{Q}$? Wir betrachten alle Konjugierten:
$$\sigma_2(\alpha) = \zeta^2 + \zeta^{-2}, \quad \sigma_3(\alpha) = \zeta^3 + \zeta^{-3} = \zeta^2 + \zeta^{-2}.$$
Daher wird das Polynom
$$f(x) = (x - (\zeta + \zeta^{-1})(x - (\zeta^2 + \zeta^{-2})$$
Koeffizienten in $\mathbb{Q}$ haben. Es ist
$$\zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$$
und
$$(\zeta + \zeta^{-1})(\zeta^2 + \zeta^{-2}) = \zeta^3 + \zeta^{-1} + \zeta + \zeta^{-3} = -1,$$
also
$$f(x) = x^2 + x - 1.$$
f hat die Nullstellen $\frac{-1 \pm \sqrt{5}}{2}$. Es folgt
$$\mathbb{Q}(\zeta)^{\langle\sigma_{-1}\rangle} = \mathbb{Q}(\sqrt{5}).$$

Damit erhalten wir folgendes Unterkörperdiagramm:

$$\begin{array}{c} \mathbb{Q}(\zeta_5) \\ | \\ \mathbb{Q}(\sqrt{5}) \\ | \\ \mathbb{Q} \end{array}$$

(ζ_5 genügt einer quadratischen Gleichung über $\mathbb{Q}(\sqrt{5})$. Welche Darstellung erhält man daraus für ζ_5?)

Dummit/Foote, S.597

SATZ. *Seien m, n teilerfremde natürliche Zahlen, ζ_m eine primitive m-te Einheitswurzel und ζ_n eine primitive n-te Einheitswurzel.*

(1) *Das Produkt $\zeta_m\zeta_n$ ist eine primitive mn-te Einheitswurzel.*
(2) *$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_m\zeta_n)$, d.h. $\mathbb{Q}(\zeta_m, \zeta_n)$ ist der mn-te Kreisteilungskörper.*
(3) *Es ist $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.*

$$\begin{array}{ccccc} & & \mathbb{Q}(\zeta_m\zeta_n) = \mathbb{Q}(\zeta_m\zeta_n) & & \\ & \swarrow & & \searrow & \\ \mathbb{Q}(\zeta_m) & & & & \mathbb{Q}(\zeta_n) \\ & \searrow & & \swarrow & \\ & & \mathbb{Q} = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) & & \end{array}$$

(4) *Die natürliche Abbildung*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n)|\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}), \quad \sigma \mapsto (\sigma|_{\mathbb{Q}(\zeta_m)}, \sigma|_{\mathbb{Q}(\sigma_n)}$$

ist ein Isomorphismus.

Beweis:

(1) Wir benutzen eine Aussage aus der Gruppentheorie:

$$\mathrm{ggT}(\mathrm{ord}\,(\zeta_m), \mathrm{ord}\,(\zeta_n)) = 1 \quad \Longrightarrow \quad \mathrm{ord}\,(\zeta_m\zeta_n) = \mathrm{ord}\,(\zeta_m)\mathrm{ord}\,(\zeta_n).$$

(2)
- $\supseteq$ Klar.
- Wir betrachten für $x \in \mathbb{Z}$

$$(\zeta_m\zeta_n)^x = \zeta_m^x\zeta_n^x.$$

Wir suchen ein x mit

$$x \equiv \begin{cases} 1 \bmod m, \\ 0 \bmod n \end{cases}$$

denn dann ist $(\zeta_m\zeta_n)^x = \zeta_m$. Solch ein x existiert aber nach dem chinesischen Restsatz. Analog finden wir ein y mit $(\zeta_m\zeta_n)^y = \zeta_n$. Daraus folgt dann $\subseteq$.

(3) Es ist

$$\begin{aligned} \varphi(m)\varphi(n) &= \varphi(mn) = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] \cdot [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \\ &= [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] \cdot \varphi(m), \end{aligned}$$

also

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(n).$$

Genauso sieht man

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = \varphi(m).$$

Nun ist aber

$$\begin{aligned}\varphi(m) &= [\mathbb{Q}(\zeta_m,\zeta_n):\mathbb{Q}(\zeta_n)] \leq [\mathbb{Q}(\zeta_m):\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)] = \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]} = \\ &= \frac{\varphi(m)}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]},\end{aligned}$$

woraus sofort $[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}] = 1$, also

$$\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) = \mathbb{Q}$$

folgt.

(4) Die linke und die rechte Seite der Abbildung haben gleich viele Elemente, nämlich $\varphi(mn) = \varphi(m)\varphi(n)$. Nun gilt für $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m,\zeta_n)|\mathbb{Q})$:

$$\begin{aligned}\sigma \in \mathrm{Kern} &\iff \sigma|_{\mathbb{Q}(\zeta_m)} = \mathrm{id}_{\mathbb{Q}(\zeta_m)} \text{ und } \sigma|_{\mathbb{Q}(\zeta_n)} = \mathrm{id}_{\mathbb{Q}(\zeta_n)} \iff \\ &\iff \sigma = \mathrm{id}_{\mathbb{Q}(\zeta_m,\zeta_n}.\end{aligned}$$

Also ist die Abbildung injektiv, und damit auch bijektiv. ■