Einheitswurzeln

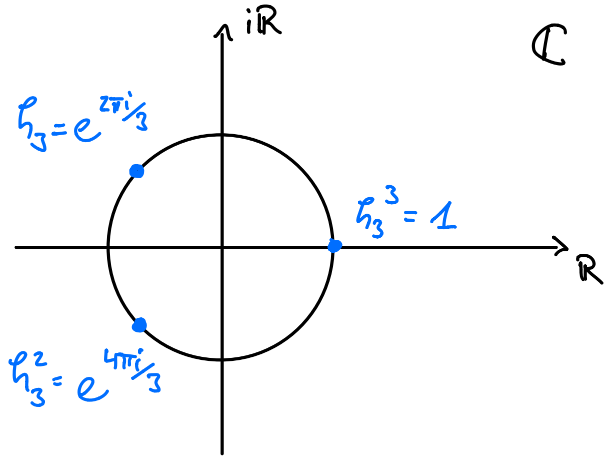
Definition 92

Sei $n \in \mathbb{N}$.

(1) Wir definieren $\zeta_n := e^{\frac{2\pi i}{n}}$.

ζ_n heißt n-te Einheitswurzel.

(2) $\Phi_n(X) = X^n - 1 \in \mathbb{Q}[X]$ heißt das n-te Kreisteilungspolynom.



Lemma 93

(1) $\Phi_n(X) = \prod_{i=0}^{n-1} (X - \zeta_n^i)$

(2) $\mathbb{Q}(\zeta_n) = \mathrm{ZFK}(\Phi_n)$

Beweis

Zu (1): Sei $0 \leq i \leq n-1$. Dann ist $\Phi_n(\zeta_n^i) = (\zeta_n^i)^n - 1 = (\underbrace{\zeta_n^n}_{=1})^i - 1 = 0$

$\Rightarrow$ $\zeta_n^0, \zeta_n^1, \dots, \zeta_n^{n-1}$ sind alles Nullstellen von Φ_n.

Für $0 \leq i < j \leq n-1$ gilt: Ang.: $\zeta_n^i = \zeta_n^j \Rightarrow \zeta_n^{j-i} = 1$

Aber $\zeta_n^{j-i} = e^{2\pi i \cdot \frac{j-i}{n}} \neq 1$, da $0 < (j-i)/n < 1$.

$\Rightarrow$ $\zeta_n^0, \zeta_n^1, \dots, \zeta_n^{n-1}$ sind alle verschieden.

$\Rightarrow$ $\zeta_n^0, \zeta_n^1, \dots, \zeta_n^{n-1}$ sind n verschiedene Nullstellen von $\Phi_n(X) = X^n - 1$

$\Rightarrow$ $\Phi_n(X) = \prod_{i=0}^{n-1} (X - \zeta_n^i)$

Zu (2): $\mathrm{ZFK}(\Phi_n) = \mathbb{Q}(\zeta_n^0, \zeta_n^1, \dots, \zeta_n^{n-1}) \overset{!}{=} \mathbb{Q}(\zeta_n)$ da alle anderen ζ_n^i durch Potenzierung aus ζ_n entstehen.

Was ist die Galois-Gruppe $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$?

Per Definition: $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = Hom_{\mathbb{Q}}(\mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_n))$.

Sei $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Wir wissen aus der Vorlesung, dass σ durch Angabe von $\sigma(\zeta_n)$ eindeutig bestimmt ist.

Wir wissen auch $\sigma(\zeta_n)$ ist eine Nullstelle von $\Phi_n(X)$, da

$$\Phi_n(\sigma(\zeta_n)) = \sigma(\zeta_n)^n - 1 = \sigma(\zeta_n^n - 1) = \sigma(0) = 0$$

$\Rightarrow \quad \exists \; 0 \leq i \leq n-1 \quad$ mit $\sigma(\zeta_n) = \zeta_n^i$.

Aber nicht alle $0 \leq i \leq n-1$ ergeben ein Element in $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Falls $\sigma(\zeta_n) = \zeta_n^i$ und $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, dann ist σ invertierbar und es existiert ein $\tau \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $\tau(\zeta_n^i) = \zeta_n$.

(nämlich $\tau = \sigma^{-1}$).

Mit der gleichen Argumentation wie oben: $\exists \; 0 \leq j \leq n-1$ mit $\tau(\zeta_n) = \zeta_n^j$.

$$\Rightarrow \quad \tau(\zeta_n^i) = \tau(\zeta_n)^i = (\zeta_n^j)^i = \zeta_n^{j \cdot i} = \zeta_n$$

$\Rightarrow \quad j \cdot i \equiv 1 \mod n \qquad$ (weil $\zeta_n^{j \cdot i} = \zeta_n^{j \cdot i + kn}$ für alle k).

$\Rightarrow \quad i$ ist in $\mathbb{Z}/n\mathbb{Z}$ multiplikativ invertierbar,

d.h. $i \in \{ j \in \mathbb{Z}/n\mathbb{Z} \mid \exists \; j' \in \mathbb{Z}/n\mathbb{Z} : j \cdot j' \equiv 1 \mod n \}$

Korollar 94

$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{ \sigma_i \mid i \in \mathbb{Z}/n\mathbb{Z}$ multiplikativ invertierbar $\}$, wobei
$\sigma_i(\zeta_n) := \zeta_n^i$.

Definition 95

$\varphi(n) := \# \{ i \mid 0 \leq i \leq n-1 : ggT(i,n) = 1 \}$ ist die Euler'sche Phi-Funktion.

Satz 96

$\# Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \varphi(n)$

Beweis

Es genügt zu zeigen, dass $i \in \mathbb{Z}/n\mathbb{Z}$ genau dann multiplikativ invertierbar ist, wenn $ggT(i,n) = 1$.

(1) Falls $ggT(i,n) = 1 \overset{\text{Euklid's Alg.}}{\Rightarrow} \exists j, \ell \in \mathbb{Z}$ mit $i \cdot j - n \cdot \ell = 1$.

$\Rightarrow i \cdot j \equiv 1 \mod n$

$\Rightarrow i \in \mathbb{Z}/n\mathbb{Z}$ ist multiplikativ invertierbar.

(2) Sei $i \in \mathbb{Z}/n\mathbb{Z}$ multiplikativ invertierbar mit $i \cdot j \equiv 1 \mod n$.

Angenommen $\ell := ggT(i,n) > 1$. Dann definieren wir $k := \frac{n}{\ell}$

Es gilt: $1 \leq k < n$. Wir haben dann $k \cdot i = \frac{n}{\ell} \cdot i = n \cdot \underbrace{\frac{i}{\ell}}_{\in \mathbb{Z}}$

$\Rightarrow k \cdot i \equiv 0 \mod n$.

$\Rightarrow k \cdot i \cdot j \equiv 0 \mod n \Rightarrow k \equiv 0 \mod n$ ↯

$\Rightarrow ggT(i,n) = 1$ $\square$

Korollar 97

$[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$. D.h., dass das Minimalpolynom von ζ_n den Grad $\varphi(n)$.

Satz 98

$[\mathbb{Q}(\zeta_n + \zeta_n^{-1}):\mathbb{Q}] = \frac{\varphi(n)}{2}$

Beweis

$\mathbb{Q}(\zeta_n + \zeta_n)^{-1}$ ist in $\mathbb{Q}(\zeta_n)$ der Fixkörper von $H \subseteq Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $H = \langle \sigma_{n-1} \rangle$ (wobei $\sigma_{n-1}(\zeta_n) = \zeta_n^{n-1} = \zeta_n^{-1}$).

Da $\# H = 2$ folgt mit dem Hauptsatz der Galoistheorie, dass $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$.

Mit dem Gradsatz folgt:
$$[\mathbb{Q}(\zeta_n):\mathbb{Q}] = [\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n + \zeta_n^{-1})] \cdot [\mathbb{Q}(\zeta_n + \zeta_n^{-1}):\mathbb{Q}]$$

$\Rightarrow [\mathbb{Q}(\zeta_n + \zeta_n^{-1}):\mathbb{Q}] = \frac{\varphi(n)}{2}$. $\square$