

Seminar: „Unendliche Galois-Theorie“ im SoSe 09
11. Vortrag: Die maximale zyklotomische Erweiterung von \mathbb{Q}

Inhaltsverzeichnis

0	Einleitung	2
1	Endliche zyklotomische Erweiterungen von \mathbb{Q}	2
1.1	Kreisteilungskörper	2
1.2	Die Galois-Gruppe von $\mathbb{Q}(\zeta)$	5
2	Die maximale zyklotomische Erweiterung von \mathbb{Q}	7
3	Anhang	10
3.1	Literatur	10

Johannes Hölken, ES0222632000, 6. Semester, Mathematik D-II
Betreuung: Prof. Dr. Gabor Wiese und Dipl.-Math. Ralf Butenuth
Fehlermeldungen, Fragen oder Hinweise bitte an: uni@johuelken.de
Stand: 6. Juli 2009

0 Einleitung

Dieser Vortrag hat das Ziel, die Galoisgruppe der maximalen zyklotomischen Erweiterung über \mathbb{Q} zu beschreiben. Dazu werde ich zunächst die Galois-Erweiterungen von \mathbb{Q} betrachten, die durch Adjunktion von nur einer Einheitswurzel zu \mathbb{Q} entsteht.

Mit dem Satz von Kronecker-Weber, den ich in diesem Vortrag nicht beweisen werde, sind mit der Beschreibung der maximalen zyklotomischen Erweiterung alle endlichen abelschen Erweiterungen von \mathbb{Q} beschrieben.

1 Endliche zyklotomische Erweiterungen von \mathbb{Q}

1.1 Kreisteilungskörper

Definition 1.1:

Sei K ein Körper, \bar{K} sein algebraischer Abschluss und $n \in \mathbb{N}$, dann bezeichne $\mu_n(\bar{K})$ die Menge der Nullstellen von $X^n - 1 \in K[X]$ in \bar{K} . Wie in Algebra 1 gezeigt ist $\mu_n(\bar{K})$ die Gruppe¹ der n -ten Einheitswurzeln von \bar{K} .

Weiter heißt $\zeta \in \mu_n(\bar{K})$ primitive n -te Einheitswurzel, wenn für alle $d \in \mathbb{N}$ mit $d|n$ gilt:

$$(\zeta_n)^d - 1 \neq 0$$

Körper, die durch Adjunktion einer Einheitswurzel zu \mathbb{Q} entstehen, nennen wir „Kreisteilungskörper“.

Bemerkung 1.2

Sei $\bar{\mathbb{Q}}$ ein algebraischer Abschluss von \mathbb{Q} und $\zeta \in \bar{\mathbb{Q}}$ eine primitive n -te Einheitswurzel, dann gilt:

$\mathbb{Q}(\zeta)/\mathbb{Q}$ ist eine Galois-Erweiterung.

Beweis:

Es gilt:

$$X^n - 1 = \prod_{i=1}^n (X - \zeta^i) \in \bar{\mathbb{Q}}[X]$$

Also ist $\mathbb{Q}(\zeta)$ ein Zerfällungskörper von $X^n - 1$. Weiter gilt $\text{char}(\mathbb{Q}) = 0$, also ist $X^n - 1$ separabel.

□

¹Siehe [L1], Seite 182

Definition 1.3 (n -tes Kreisteilungspolynom)

Sei $n \in \mathbb{N}$ und fixiere $\bar{\mathbb{Q}}$ einen algebraischen Abschluss von \mathbb{Q} . Weiter bezeichne $\rho_n := \{\zeta_n \in \mu_n(\bar{\mathbb{Q}}) \mid \zeta_n \text{ ist primitiv}\}$ eine Teilmenge der Gruppe der n -ten Einheitswurzeln. Dann heißt

$$\Phi_n(X) := \prod_{\zeta \in \rho_n} (X - \zeta) \in \bar{\mathbb{Q}}$$

das n -te Kreisteilungspolynom.

Bemerkung 1.4

Das n -te Kreisteilungspolynom $\Phi_n(X)$ liegt bereits in $\mathbb{Q}[X]$

Beweis:

Bezeichne $G := \text{Gal}(\mathbb{Q}(\mu_n(\bar{\mathbb{Q}}))/\mathbb{Q})$. Es gilt: G permutiert die Menge der primitiven n -ten Einheitswurzeln, d.h. für alle $\zeta \in \rho_n$ und für alle $\sigma \in G$ gilt $\sigma(\zeta) \in \rho_n$. Insbesondere gilt also für alle $\sigma \in G$

$$\sigma(\Phi_n(X)) = \sigma\left(\prod_{\zeta \in \rho_n} (X - \zeta)\right) = \prod_{\zeta \in \rho_n} (X - \sigma(\zeta)) = \Phi_n(X)$$

$\Phi_n(X)$ ist also invariant unter G . Nach dem Hauptsatz der Galois-Theorie gilt, dass die Koeffizienten von $\Phi_n(X)$ bereits in $[\mathbb{Q}(\mu_n(\bar{\mathbb{Q}}))]^G = \mathbb{Q}$ liegen.

□

Lemma 1.5

Es gilt: $\langle \bar{a} \rangle = \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists \bar{u} \in \mathbb{Z}/n\mathbb{Z} : \bar{1} = \bar{u}\bar{a}$

$\Leftrightarrow \exists u, r \in \mathbb{Z} : 1 = au + nr \Leftrightarrow \text{ggT}(a, n) = 1$

□

Satz 1.6 (Irreduzibilität des Kreisteilungspolynoms)

Sei $\Phi_n(X)$ das n -te Kreisteilungspolynom, dann gilt für alle $n \in \mathbb{N}$:

$\Phi_n(X) \in \mathbb{Z}[X]$ ist irreduzibel.

Beweis:

1. $\Phi_n(X) \in \mathbb{Z}[X]$ induktiv über n :

IND-ANFANG ($n = 1$): trivial, denn $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$

IND-SCHRITT ($n - 1 \curvearrowright n$): Betrachte:

$$\begin{aligned} X^n - 1 &= \prod_{\substack{d|n \\ d>0}} \Phi_d(X) \\ &= \Phi_n(X) \cdot \prod_{\substack{d|n \\ 0 < d < n}} \Phi_d(X) \end{aligned}$$

Es gilt: $X^n - 1 \in \mathbb{Z}[X]$. Nach Induktionsannahme gilt aber auch:

$$\prod_{\substack{d|n \\ 0 < d < n}} \Phi_d(X) \in \mathbb{Z}[X]$$

Wir können also schließen, dass $\Phi_n(X) \in \mathbb{Z}[X]$ ist.

2. Irreduzibilität von $\Phi_n(X)$:

Sei hierzu $\Phi_n = f \cdot g \in \mathbb{Z}[X]$ mit f irreduzibel. Weiter sei ζ eine primitive n -te Einheitswurzel mit $f(\zeta) = 0$.

Behauptung 1: Für alle Primzahlen p mit $p \nmid n$ gilt: $f(\zeta^p) = 0$, denn sonst gelte $g(\zeta^p) = 0$, da ζ^p eine primitive n -te Einheitswurzel ist. Nach Voraussetzung sind p, n teilerfremd, mit *Lemma 1.5* gilt dann $p \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.

Es folgte dann, dass ζ eine Nullstelle von $g(X^p)$ wre. Aber das Minimalpolynom von ζ ist nach Voraussetzung f . Es gelte $f|g(X^p)$, also $g(X^p) = f \cdot h$ mit $h \in \mathbb{Z}[X]$.

Wir reduzieren die Polynome modulo p , und betrachten diese in $\mathbb{F}_p[X]$. Mit dem Frobenius-Automorphismus gelte dann:

$$\bar{g}(X^p) = (\bar{g}(X))^p = \bar{f} \cdot \bar{h}$$

und somit: $ggT(\bar{f}, \bar{g}) \neq 1$.

Hiermit haben wir einen Widerspruch, denn $\bar{f} \cdot \bar{g} = \overline{\Phi_n}$ und $\overline{\Phi_n}$ teilt $\overline{X^n - 1}$. Es gilt aber: $\overline{X^n - 1}$ ist separabel in $\mathbb{F}_p[X]$, denn $p \nmid n$ nach Voraussetzung, und hat keine mehrfachen Faktoren.

Behauptung 2: Jede primitive n -te Einheitswurzel ν ist Nullstelle von f .

Es gilt: $\nu = \zeta^r$ für $r \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$. Betrachte die Primfaktorzerlegung von r :

$$r = \prod_{i=1}^t p_i^{e_i(r)}$$

Für alle i gilt: $p_i \nmid n$. Nach der 1. Behauptung gilt nun

$$0 = f(\zeta) = f((\zeta^{p_1})^{p_2}) = \dots = f(\zeta^r) = f(\nu)$$

Hieraus folgt nun, dass $g(X) = 1$ ist, also gilt: $f(X) = \Phi_n(X)$.

□

1.2 Die Galois-Gruppe von $\mathbb{Q}(\zeta)$

Definition 1.7 (Zyklotomischer (bzw. kreisteilungs) Charakter χ)

Sei $n \in \mathbb{N}$ und K ein Körper mit $\text{char}(K) = 0$ oder $\text{char}(K) \nmid n$. Weiter sei $\zeta \in \bar{K}$ eine primitive n -te Einheitswurzel, dann heißt die Abbildung

$$\chi : \text{Gal}(K(\zeta)/K) \rightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

mit $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ für $\sigma \in \text{Gal}(K(\zeta)/K)$, n -ter zyklotomischer (bzw. kreisteilungs) Charakter.

Satz 1.8

Die Abbildung χ aus 1.7 ist wohldefiniert, weiter ist χ sogar injektiver Gruppenhomomorphismus.

Beweis:

Bezeichne $G := \text{Gal}(K(\zeta)/K)$ und sei $\sigma \in G$, dann gilt: $\sigma(\zeta) = \zeta^i$ für $i \in \{1, \dots, n\}$. Betrachte den folgenden Gruppen-Isomorphismus:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\rightarrow \mu_n(\bar{K}) \\ r &\mapsto \zeta^r \end{aligned}$$

Sei nun y ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$, dann ist mit *Lemma 1.5* $y \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Diese Aussage ist äquivalent damit, dass ζ^y die Gruppe der n -ten Einheitswurzeln erzeugt, denn für $d|n$ ist $y \cdot d$ ein Vielfaches von n . Es gilt: i mit $\zeta^i = \sigma(\zeta)$ ist ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$, also $i \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Nach Definition ist $\chi(\sigma) = i$, also ist χ Wohldefiniert.

Wie leicht nachzurechnen ist, ist χ ein Gruppen-Homomorphismus, denn seien $\sigma, \tau \in G$, dann

$$\chi(\sigma\tau) = \sigma \circ \tau(\zeta) = \sigma(\zeta^{\chi(\tau)}) = (\zeta^{\chi(\sigma)})^{\chi(\tau)} = \zeta^{\chi(\sigma) \cdot \chi(\tau)}$$

Zum Nachweis, dass χ injektiv ist, betrachten wir nun den Kern von χ :

$$\sigma \in \ker(\chi) \Rightarrow \sigma(\zeta) = \zeta^1 = \zeta \Rightarrow \sigma = \text{id}_{K(\zeta)} = \text{id}$$

□

Folgerung 1.9

Sei K ein Körper mit $\text{char}(K) = 0$ und \bar{K} ein algebraischer Abschluss von K , weiter sei $\zeta \in \bar{K}$ eine n -te Einheitswurzel, dann gelten:

$$G := \text{Gal}(K(\zeta)/K) \text{ ist abelsch und } [K(\zeta)/K] \mid \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

Beweis:

Fasse G vermöge χ als Untergruppe von $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ auf. Untergruppen abelscher Gruppen sind abelsch, also ist G abelsch. Weiter gilt dann:

$$[K(\zeta)/K] := \#G \mid \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*.$$

□

Folgerung 1.10

Der Grad des n -ten Kreisteilungspolynoms ist

$$\deg(\Phi_n(X)) = \#(\mathbb{Z}/n\mathbb{Z})^*$$

Beweis:

$\Phi_n(X) \in \mathbb{Q}[X]$ besitzt paarweise verschiedene Nullstellen, damit folgt die Behauptung aus dem Beweis von *Satz 1.8*.

□

Satz 1.11

Sei $\zeta_n \in \overline{\mathbb{Q}}$ eine primitive n -te Einheitswurzel, dann ist der Kreisteilungscharakter χ ein Gruppenisomorphismus. Insbesondere gilt also:

$$G := \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Beweis:

$\Phi_n(X)$ ist Minimalpolynom von ζ_n , denn $\Phi_n(X)$ ist nach *Satz 1.6* irreduzibel über \mathbb{Q} und $\Phi_n(\zeta_n) = 0$. Nach *Folg. 1.10* gilt:

$$\#G = \deg(\Phi_n(X)) = \#(\mathbb{Z}/n\mathbb{Z})^*$$

In *Folg. 1.9* haben wir gezeigt, dass G Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ ist, daher folgt die Behauptung.

□

2 Die maximale zyklotomische Erweiterung von \mathbb{Q}

Definition 2.1 (Die maximale zyklotomische Erweiterung von \mathbb{Q})

$\tilde{\mathbb{Q}} := \mathbb{Q}(\zeta_i \mid \zeta_i \in \mu_i(\bar{\mathbb{Q}}) \text{ primitiv}, i = 1, \dots, \infty)$ ist die Körpererweiterung von \mathbb{Q} , welche durch adjunktion aller Einheitswurzeln entsteht. Die zugehörige Menge der \mathbb{Q} -Automorphismen $\text{Aut}_{\mathbb{Q}}(\tilde{\mathbb{Q}})$ sei im Folgenden mit \tilde{G} bezeichnet.

Satz 2.2

$\tilde{\mathbb{Q}}/\mathbb{Q}$ ist galoisch. Insbesondere ist \tilde{G} die Galoisgruppe von $\tilde{\mathbb{Q}}/\mathbb{Q}$.

Beweis:

Induktiv über n . Der Induktionsanfang mit $n = 1$ ist trivial, denn $\zeta_1 = 1$, den Beweis zu $n = 2$ haben wir im ersten Abschnitt geführt. Wir betrachten den Schritt von n auf $n + 1$. Zur besseren Lesbarkeit bezeichne:

$$\mathbb{Q}((\zeta)_{n+1}) := \mathbb{Q}(\zeta_i \mid \zeta_i \in \mu_i(\bar{\mathbb{Q}}) \text{ primitiv}, i = 1, \dots, n + 1)$$

Es gilt: $\mathbb{Q}((\zeta)_{n+1}) = \mathbb{Q}((\zeta)_n)(\zeta_{n+1})$. Nach Induktionsannahme ist $\mathbb{Q}((\zeta)_n)/\mathbb{Q}$ galoisch. Weiter ist $\mathbb{Q}((\zeta)_n)(\zeta_{n+1})/\mathbb{Q}((\zeta)_n)$ nach dem ersten Abschnitt galoisch, also folgt die Behauptung. □

Definition und **Satz 2.3** (Prüfer Ring)

Betrachte die Ringe $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$. Vermöge der Teilbarkeitsrelation $n_1 \mid n_2 \mid n_3 \mid \dots$ werden diese zu einem projektiven System bezüglich der Projektionen

$$\mathbb{Z}/n_1\mathbb{Z} \leftarrow \mathbb{Z}/n_2\mathbb{Z} \leftarrow \mathbb{Z}/n_3\mathbb{Z} \leftarrow \dots$$

Wir bezeichnen mit

$$\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

den Prüfer Ring.

Beweis:

Wir wollen zeigen, dass $\hat{\mathbb{Z}}$ ein Ring ist, dazu betrachten wir $\hat{\mathbb{Z}}$ Komponentenweise bezüglich der $\mathbb{Z}/n\mathbb{Z}$ -Additionen bzw. Multiplikationen.

$$\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \left\{ (x_1, x_2, x_3, \dots) \in \bigotimes_{n \in \mathbb{N}} (\mathbb{Z}/n\mathbb{Z}) \mid \varphi_{n_1, n_2}(x_{n_2}) = x_{n_1} \quad \forall n_1, n_2 \in \mathbb{N} \text{ mit } n_1 \mid n_2 \right\}$$

wobei $\varphi_{n_1, n_2} : \mathbb{Z}/n_2\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z}$ die natürliche Projektion bezeichne. Für $\underline{x} := (x_i)_{i \in \mathbb{N}}, \underline{y} := (y_i)_{i \in \mathbb{N}} \in \hat{\mathbb{Z}}$ betrachte $\underline{x} \cdot \underline{y} := (x_i \cdot y_i)_{i \in \mathbb{N}}$, es gilt:

$$\forall n_1, n_2 \in \mathbb{N} \text{ mit } n_1 \mid n_2 : x_{n_1} \cdot y_{n_1} = \varphi_{n_1, n_2}(x_{n_2}) \cdot \varphi_{n_1, n_2}(y_{n_2}) = \varphi_{n_1, n_2}(x_{n_2} \cdot y_{n_2}) \in \hat{\mathbb{Z}}$$

Analog folgt wegen der Homomorphieeigenschaft von φ_{n_1, n_2} die Abgeschlossenheit unter der Addition. □

Definition und **Satz 2.4**

Bezeichne $\mathbb{P} \subseteq \mathbb{Z}$ die Menge der positiven Primzahlen in \mathbb{Z} sowie \mathbb{Z}_p die p -adischen (ganzen) Zahlen, dann existiert ein Ringisomorphismus, so dass

$$\hat{\mathbb{Z}} \cong \bigotimes_{p \in \mathbb{P}} \mathbb{Z}_p$$

Beweis:

Sei $n \in \mathbb{N}$ mit der Primfaktorzerlegung

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

Der *chinesische Restatz*² liefert einen Isomorphismus zwischen

$$\mathbb{Z}/n\mathbb{Z} \cong \bigotimes_{p \in \mathbb{P}} \mathbb{Z}/p^{\nu_p(n)}\mathbb{Z} \quad (1)$$

derart, dass wir einen kanonischen Homomorphismus

$$\phi_n : \bigotimes_{p \in \mathbb{P}} \mathbb{Z}_p \rightarrow \bigotimes_{p \in \mathbb{P}} \mathbb{Z}/p^{\nu_p(n)}\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

erhalten. Für alle $n_1, n_2 \in \mathbb{N}$ mit $n_1 | n_2$ sind die ϕ_n mit den Projektionen φ_{n_1, n_2} aus dem Beweis von *Satz 2.3* verträglich. Insbesondere sind die ϕ_n bezüglich der Produkttopologie stetig.

Es ist jetzt zu zeigen, dass $\bigotimes \mathbb{Z}_p$ mit den ϕ_n ein projektiver Limes der $\mathbb{Z}/n\mathbb{Z}$ ist. Hierzu sei R ein Ring, dann betrachte für $n \in \mathbb{N}$ Ringhomomorphismen

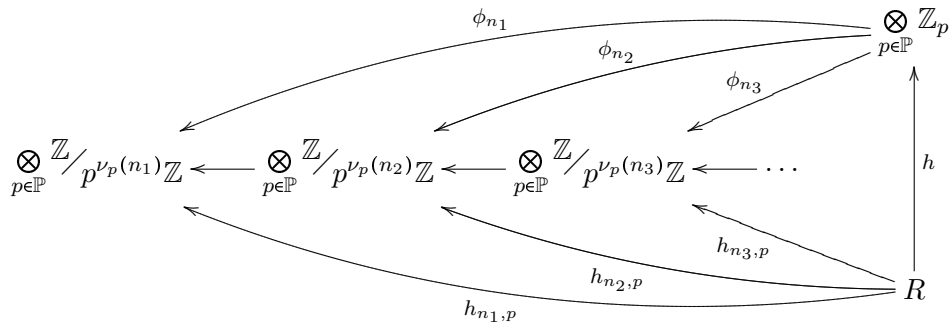
$$h_n : R \rightarrow \mathbb{Z}/n\mathbb{Z}$$

die mit den φ_{n_1, n_2} verträglich sind.

Durch Isomorphismen des Typs (1) wird für alle $p \in \mathbb{P}$ ein Homomorphismus

$$h_{n,p} : R \rightarrow \bigotimes_{p \in \mathbb{P}} \mathbb{Z}/p^{\nu_p(n)}\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

gegeben, welche mit den Restriktionshomomorphismen des projektiven Systems $(\mathbb{Z}/p^\nu\mathbb{Z})_{\nu \in \mathbb{N}}$ verträglich sind. Betrachte das folgende Diagramm:



²Vgl. [L3] Satz 7.16, Seite 26

Mit $h := (h_n)_{n \in \mathbb{N}}$ folgt aus der universellen Abbildungseigenschaft projektiver Limites die Behauptung. □

Lemma 2.5

Sei I eine Menge, derart dass $\{\mathbb{Q}(\zeta_i) \mid i \in I\}$ die Menge der endlichen zyklotomischen Galois-Erweiterungskörper über \mathbb{Q} ist. Dann wird $\text{Gal}(\mathbb{Q}(\zeta_i)/\mathbb{Q})$ zusammen mit den f_i , die im sechsten Vortrag definiert wurden ein projektives System. Es gilt:

$$\tilde{G} := \text{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{i \in I} \text{Gal}(\mathbb{Q}(\zeta_i)/\mathbb{Q})$$

Beweis:

I ist geordnet, denn

$$\zeta_i \leq \zeta_j \Leftrightarrow \mathbb{Q}(\zeta_i) \subseteq \mathbb{Q}(\zeta_j)$$

Ordne also I durch $i \leq j$. Weiter wurde im sechsten Vortrag gezeigt, dass für alle $i \in I$ die Galoisgruppen $\text{Gal}(\mathbb{Q}(\zeta_i)/\mathbb{Q})$ topologische Gruppen sind, und dass die f_i die geforderten Eigenschaften erfüllen.

Im neunten Vortrag wurde gezeigt, dass

$$\text{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{\tilde{\mathbb{Q}}/L/\mathbb{Q}} \text{Gal}(L/\mathbb{Q})$$

für endliche Körpererweiterungen L gilt. Hieraus folgt bereits die Behauptung, denn es ist klar, dass zu jedem $L \subseteq \tilde{\mathbb{Q}}$ ein ζ_i existiert, so dass $L \subseteq \mathbb{Q}(\zeta_i)$. □

Satz 2.6

Es gilt:

$$\tilde{G} := \text{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^* \cong \bigotimes_{p \in \mathbb{P}} \mathbb{Z}_p^*$$

Beweis:

Sei I wie in Lemma 2.5, es gilt $I = \mathbb{N}$ und somit:

$$\begin{aligned} \tilde{G} &= \varprojlim_{i \in I} \text{Gal}(\mathbb{Q}(\zeta_i)/\mathbb{Q}) \\ &= \varprojlim_{n \in \mathbb{N}} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ &\cong \varprojlim_{n \in \mathbb{N}} \left(\mathbb{Z}/n\mathbb{Z} \right)^* \\ &= \left(\varprojlim_{i \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} \right)^* = \hat{\mathbb{Z}}^* \end{aligned}$$

Wir dürfen hier den Limes in die Einheitengruppe hinein ziehen, da wir die Einheiten komponentenweise in den Ringen $\mathbb{Z}/n\mathbb{Z}$ betrachten.

Die Isomorphie von $\hat{\mathbb{Z}}$ und $\bigotimes_{p \in \mathbb{P}} \mathbb{Z}_p$ haben wir bereits in *Satz 2.4* gezeigt. \square

Anmerkung

Im zehnten Vortrag wurde \mathbb{Z}_p durch unendliche Summen

$$\sum_{i=0}^{\infty} a_i p^i \quad \text{mit } a_i \in \{0, \dots, p-1\}$$

beschrieben. Die Einheitengruppe können wir ebenso beschreiben, durch

$$\mathbb{Z}_p^* = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\} \wedge a_0 \neq 0 \right\}$$

Für $z \in \mathbb{Z}$ haben wir dies bereits im neunten Vortrag gesehen, denn

$$\frac{1}{z} \in \mathbb{Z}_p \Leftrightarrow p \nmid z \Leftrightarrow a_0 \neq 0$$

Anmerkung (Satz von Kronecker-Weber)

Jede endliche abelsche Erweiterung L/\mathbb{Q} ist enthalten in einem mit einer Einheitswurzel ζ gebildeten Körper $\mathbb{Q}(\zeta)$.

Der Beweis dieses Satzes ist nicht Thema dieses Vortrags³, jedoch sind mit diesem Satz und der soeben gelieferten Beschreibung der Galoisgruppe der maximalen zyklotomischen Erweiterung auch alle endlichen abelschen Galoisgruppen von Zahlkörpern beschrieben.

3 Anhang

3.1 Literatur

[L1] **S. Bosch**, Algebra, Springer-Verlag

[L2] **J. Neukirch**, Algebraische Zahlentheorie, Springer-Verlag

[L3] **G. Wiese**, VL: Algebra I im WS 08/09

<http://uni.johoelken.de/algebra/Algebra1-WS0809-Wiese.pdf>

³Zum Beweis siehe: [L2] Seite 341 Theorem 1.10