F20T2A2

(a) Seien $m, d, n \in \mathbb{N}$ mit $n = dm$, wobei m ungerade ist. Zeigen Sie: $(x^d+1) \mid (x^n+1)$.

Für jedes $r \in \mathbb{N}$ und $f_r = x^r + 1$ gilt $ggT(f_r, f_r') = ggT(x^r+1, rx^{r-1}) = 1$. Also haben Polynome dieser Form keine mehrfachen komplexen Nullstellen. Es genügt deshalb zu überprüfen, dass jede Nullstelle von

$x^d + 1$ auch eine Nullst. von $x^n + 1$.

Beh. Ist $\alpha \in \mathbb{C}$ eine komplexe Nullstelle von f_r ist, dann ist α ein Element in $\mathbb{C}^\times$ mit $\operatorname{ord}(\alpha) \mid 2r$ und $\operatorname{ord}(\alpha) \nmid r$.

Es gilt $f_r \cdot (x^r - 1) = (x^r + 1)(x^r - 1) = x^{2r} - 1$

Sei nun $\alpha \in \mathbb{C}$ mit $f_r(\alpha) = 0$. Dann ist α auch eine Nullst. von $x^{2r} - 1 \Rightarrow \alpha^{2r} = 1 \Rightarrow \alpha \in \mathbb{C}^\times$ und $\operatorname{ord}(\alpha) \mid 2r$. Ang. $\operatorname{ord}(\alpha) \mid r \Rightarrow \alpha^r = 1$

$\Rightarrow 2 = 1 + 1 = \alpha^r + 1 = f_r(\alpha) = 0$ ↯ ($\Rightarrow$ Beh.)

Von der Beh. gilt auch die Umkehrung, d.h. jedes $\alpha \in \mathbb{C}^*$ mit $\operatorname{ord}(\alpha) \mid 2r$, $\operatorname{ord}(\alpha) \nmid r$ ist Nullstelle von f_r, denn:

$\operatorname{ord}(\alpha) \mid 2r \Rightarrow \alpha^{2r} = 1 \Rightarrow X^{2r} - 1 \overset{S.0}{=} f_r(\alpha) \cdot (\alpha^r - 1)$

Wegen $\operatorname{ord}(\alpha) \nmid r$ gilt $\alpha^r \neq 1$, also $\alpha^r - 1 \neq 0$, und es folgt $f_r(\alpha) = 0$

Sei nun α eine Nullstelle von f_d. S.0 $\Rightarrow \operatorname{ord}(\alpha) \mid 2d$, $\operatorname{ord}(\alpha) \mid d$. Es genügt nun z.Zg.: $\operatorname{ord}(\alpha) \mid 2n$, $\operatorname{ord}(\alpha) \nmid n$.

Aus $\operatorname{ord}(\alpha) \mid 2d$ und $d \mid n$ folgt $\operatorname{ord}(\alpha) \mid 2n$

Ang. $\operatorname{ord}(\alpha) \mid n \Rightarrow \operatorname{ord}(\alpha) \mid md$, $\operatorname{ord}(\alpha) \mid 2d$

m ungerade $\Rightarrow \operatorname{ggT}(2, m) = 1$ Bézout $\Rightarrow$

$\exists u, v \in \mathbb{Z}: 2u + mv = 1 \quad \operatorname{ord}(\alpha) \mid mdv,$

$\operatorname{ord}(\alpha) \mid 2du \Rightarrow \operatorname{ord}(\alpha)$ teilt $mdv + 2du =$

$d(mv + 2u) = d$ ↯

Aus $\operatorname{ord}(\alpha) \mid 2n, \operatorname{ord}(\alpha) \nmid n$ folgt $f_n(\alpha) = 0$.

(b) Sei $n \in \mathbb{N}$ mit der Eigenschaft, dass $x^n + 1$ irreduzibel ist. Zeigen Sie, dass n eine Zweierpotenz ist.

Ang. $x^n + 1$ ist irreduzibel, aber n keine Zweierpotenz.
Dann besitzt n einen ungeraden Primteiler p. $\rightarrow$
$\exists d \in \mathbb{N}$ mit $n = dp$, und p ist ungerade.

Teil (a) $\Rightarrow (x^d + 1) \mid (x^n + 1)$

$\Rightarrow \exists\, h \in \mathbb{Q}[x]$ mit $x^n + 1 \overset{(*)}{=} h \cdot (x^d + 1)$

Es gilt $\operatorname{grad}(x^d + 1) \geq 1$ und

$\operatorname{grad}(h) = n - d$. Wäre $n - d = 0$,

also $n = d$, dann würde $p = 1$ folgen

↯ da p Primzahl. Also ist $(*)$ eine

Zerlegung von $x^n + 1$ in Nichteinheiten

von $\mathbb{Q}[x]$, d.h. $x^n + 1$ ist reduzibel ↯

Satz (Galoistheorie des Kreisteilungskörper)

Sei $n \in \mathbb{N}$, $n \geq 2$ und $\zeta_n = e^{2\pi i/n}$.

(i) Der Körper $\mathbb{Q}(\zeta_n)$ ist ein Zerfällungskörper des n-ten Kreisteilungspolynoms Φ_n.

(ii) Die Erweiterung $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ ist galoissch mit $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

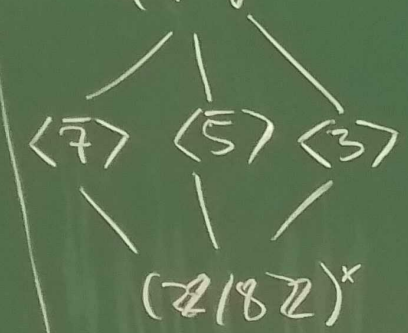
(iii) Ist $k \in \mathbb{Z}$ mit $\mathrm{ggT}(k, n) = 1$, dann existiert ein eindeutig bestimmtes $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ mit $\sigma_k(\zeta_n) = \zeta_n^k$. Jedes Element der Galoisgruppe hat diese Form. Ein Isomorphismus wie unter (ii) ist durch $\sigma_k \mapsto k + n\mathbb{Z}$ gegeben.

Beispiel: Galoisgruppe des achten Kreisteilungskörpers

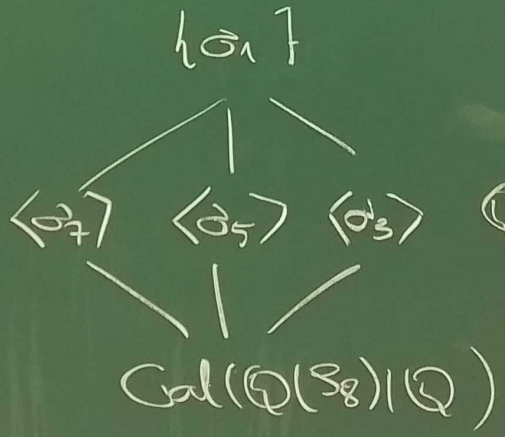
$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q}) = \{\sigma_1 = \mathrm{id}, \sigma_3, \sigma_5, \sigma_7\}$ leicht zu sehen: $\zeta_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

und $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$

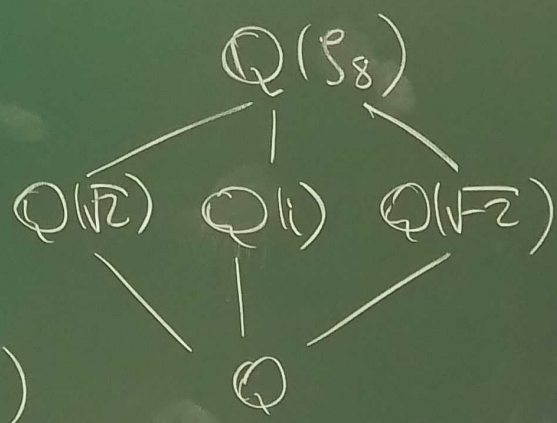
Untergr. von $(\mathbb{Z}/8\mathbb{Z})^\times$



Untergruppen der Galoisgr.



Zwischenkörper von $\mathbb{Q}(\zeta_8)|\mathbb{Q}$



F24T1A4 Sei p eine Primzahl mit der Eigenschaft, dass $p-1$ ein Produkt $p_1 \cdot \ldots \cdot p_r$ von r verschiedenen Primzahlen ist ($r \in \mathbb{N}$).

(a) Zeigen Sie, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ genau 2^r verschiedene Untergruppen hat.

Da p eine Primzahl ist, ist $(\mathbb{Z}/p\mathbb{Z})^\times$ eine zyklische Gruppe, von Ordnung $p-1$. Die Anzahl der Untergruppen einer zykl Gruppe der Ordnung n ist gleich der Anzahl der Teiler von n. Da $p_1, \ldots, p_r$ verschiedene Primzahlen sind, sind die verschiedenen Teiler von $p-1 = p_1 \cdot \ldots \cdot p_r$ gegeben durch $p_1^{\varepsilon_1} \cdot \ldots \cdot p_r^{\varepsilon_r}$ mit $\varepsilon_1, \ldots, \varepsilon_r \in \{0,1\}$. Für das Tupel $(\varepsilon_1, \ldots, \varepsilon_r)$ gibt es 2^r Möglichkeiten, also ist dies die Anzahl der Teiler, und zugleich die Anzahl der Untergruppen von $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Sei ζ_p eine primitive p-te Einheitswurzel. Bestimmen Sie die Anzahl der Zwischenkörper von $\mathbb{Q}(\zeta_p) | \mathbb{Q}$.

Laut Vorlesung ist $\mathbb{Q}(\zeta_p) | \mathbb{Q}$ eine Galoiserw., und für die Galoisgruppe G dieser Erweiterung gilt $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Nach Teil (a) hat $(\mathbb{Z}/p\mathbb{Z})^\times$ genau 2^r Untergruppen, also gilt dasselbe für G. Aus dem Hauptsatz der Galoistheorie folgt, dass $\mathbb{Q}(\zeta) | \mathbb{Q}$ genau 2^r Zwischenkörper hat. □

selbe für G. Aus dem Hauptsatz der Galoistheorie (b)

H24T3A5 Sei $\zeta_{16} = e^{\pi i/8}$.

(a) Begründen Sie, dass $\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i)$ eine Galois-erweiterung vom Grad 4 ist.

Lt. Vl. ist $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ mit $\zeta_n = e^{2\pi i/n}$ für jedes $n \in \mathbb{N}$ eine Galoiserweiterung, mit $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow \mathbb{Q}(\zeta_{16})|\mathbb{Q}$ ist galoisch, und $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q})$ ist isomorph zu $(\mathbb{Z}/16\mathbb{Z})^\times$. Allgemein gilt: Ist $L|K$ galoissch und M ein Zwischenkörper von $L|K$, dann ist auch $L|M$ galoisisch. Wegen $i = \zeta_{16}^4 \in \mathbb{Q}(\zeta_{16})$

Ist $\mathbb{Q}(i)$ ein Zwischenkörper von $\mathbb{Q}(\zeta_{16})|\mathbb{Q}$, also ist $\mathbb{Q}(\zeta_{16})|\mathbb{Q}$ galoissch.

Für jedes $n \in \mathbb{N}$ gilt $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

$\Rightarrow [\mathbb{Q}(\zeta_{16}):\mathbb{Q}] = \varphi(16) = 8$

Weil $-1 \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei und $i = \sqrt{-1}$ ist, gilt $[\mathbb{Q}(i):\mathbb{Q}] = 2$

Gradformel $\Rightarrow 8 = [\mathbb{Q}(\zeta_{16}):\mathbb{Q}] = [\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] \cdot [\mathbb{Q}(i):\mathbb{Q}] =$

$[\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] \cdot 2 \Rightarrow [\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] = \frac{8}{2} = 4$

(b) Bestimmen Sie das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$.

Das Polynom $f = x^4 - i \in \mathbb{Q}(i)[x]$ ist normiert und erfüllt $f(\zeta_{16}) = \zeta_{16}^4 - i = i - i = 0$. Daraus folgt $M_{\zeta_{16},\mathbb{Q}(i)} \mid f$.

$[\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] \cdot 2 \Rightarrow [\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)] = \frac{8}{2} = 4$

(b) Bestimmen Sie das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$.

Es gilt $\operatorname{grad} \mu_{\zeta_{16},\mathbb{Q}(i)} = [\mathbb{Q}(i)(\zeta_{16}) : \mathbb{Q}(i)] = [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(i)]$
$= 4 = \operatorname{grad}(f)$ Weil beide Polynome normiert sind, folgt
$\mu_{\zeta_{16},\mathbb{Q}(i)} = f = x^4 - i$.

(c) Entscheiden Sie begründet, ob $\operatorname{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i))$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $(\mathbb{Z}/2\mathbb{Z})^2$ ist. $[(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}]$
Laut Vl. ist $\operatorname{Gal}(\mathbb{Q}_{16}|\mathbb{Q}) = \{\sigma_k \mid 0 \le k < 15, \operatorname{ggT}(k,16) = 1\}$
$= \{\sigma_1, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}\}$, wobei σ_k jeweils durch $\sigma_k(\zeta_{16}) = \zeta_{16}^k$ gegeben ist. Es gilt $\sigma_3(i) = \sigma_3(\zeta_{16}^4)$
$= \sigma_{16}(\zeta_{16})^4 = (\zeta_{16}^3)^4 = \zeta_{16}^{12} = i^3 = -i \neq i \Rightarrow$
$\sigma_3 \notin \operatorname{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i))$. aber: $\sigma_5(i) = \sigma_5(\zeta_{16})^4 = (\zeta_{16}^5)^4$

Zerlegung von $X^{17}-1$ in Kreisteilungspolynome

$= \zeta_{16}^{20} = (\zeta_{16}^4)^5 = i^5 = i \Rightarrow \sigma_5 \in$
$\mathrm{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i))$. Das Bild von σ_5 unter dem Isom. $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}) \cong (\mathbb{Z}/16\mathbb{Z})^\times$ ist $\overline{5}$, und wegen $\overline{5}^2 = \overline{25} = \overline{9} + \overline{1}$, $\overline{5}^4 = \overline{9}^2 = \overline{81}$ $= \overline{1}$ ist dies ein Element der Ordnung 4. Also enthält $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i))$ ein Element der Ordnung 4. Weil die Ordnung der Gruppe gleich $[\mathbb{Q}(\zeta_{16}):\mathbb{Q}(i)]$ $= 4$ ist, folgt $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}(i)) \cong \mathbb{Z}/4\mathbb{Z}$. □

Aufgaben zum Hauptsatz der Galoistheorie:
H14T1A1, F15T3A4, F16T1A5,
H15T1A5 schwierige: H18T2A5