H25T1A1

In den ersten beiden Aufgabenteilen wurde gezeigt

(a) Die Menge der normierten, irreduziblen Polynome in $\mathbb{F}_3[x]$ vom Grad 2 ist gegeben durch

$$\{x^2 + \bar{1}, x^2 + x + \bar{2}, x^2 + \bar{2}x + \bar{2}\}.$$

(b) Der Faktorring $K = \mathbb{F}_3[x]/(x^2 + \bar{1})$ ist ein Körper bestehend aus 9 Elementen.

zu (c) Bestimmen Sie eine Darstellung von $f = x^8 - \bar{1} \in \mathbb{F}_3[x]$ als Produkt irreduzibler Faktoren.

Sei $\mathbb{F}_3^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_3$ und $\mathbb{F}_9$ der eindeutig bestimmte Zwischenkörper von $\mathbb{F}_3^{\mathrm{alg}}|\mathbb{F}_3$ mit 9 Elementen. (Die Körper K und $\mathbb{F}_9$ sind zueinander isomorph, weil für jede Primzahlpotenz $q > 1$ bis auf Isomorphie genau ein Körper mit q Elementen existiert.)

Die multiplikative Gruppe $\mathbb{F}_9^\times$ ist eine zyklische Gruppe der Ordnung 8. Für jedes $\alpha \in \mathbb{F}_9^\times$ gilt also $\alpha^8 = 1$. Dies zeigt, dass jedes dieser Elemente eine Nullstelle von f ist. Wegen $\mathrm{grad(f)} = 8$ folgt daraus, dass f über $\mathbb{F}_9$ in Linearfaktoren zerfällt, und dass f nur einfache Nullstellen besitzt.

Wir zeigen nun, dass alle irreduziblen Faktoren von f vom Grad 1 oder 2 sind. Sei $g \in \mathbb{F}_3[x]$ ein normierter irreduzibler Faktor von f. Mit f zerfällt auch g über $\mathbb{F}_9$ in Linearfaktoren, und insbesondere enthält $\mathbb{F}_9$ eine Nullstelle α von g. Das Polynom g stimmt dann auf Grund seiner Eigenschaften mit dem Minimalpolynom $\mu_{\alpha,\mathbb{F}_3}$ überein. Weil $\mathbb{F}_3(\alpha)$ ein Zwischenkörper von $\mathbb{F}_9|\mathbb{F}_3$ ist, können wir die Gradformel anwenden und erhalten

$$2 \;=\; [\mathbb{F}_9 : \mathbb{F}_3] \;=\; [\mathbb{F}_9 : \mathbb{F}_3(\alpha)] \cdot [\mathbb{F}_3(\alpha) : \mathbb{F}_3].$$

Daraus folgt $\mathrm{grad(g)} = [\mathbb{F}_3(\alpha) : \mathbb{F}_3] \in \{1, 2\}$. Wegen $\{\bar{1}, \bar{2}\} \subseteq \mathbb{F}_9^\times$ sind $\bar{1}$ und $\bar{2}$ Nullstellen von f und $(x - \bar{1})(x - \bar{2})$ somit ein Teiler von f. Es gibt also ein Polynom $h \in \mathbb{F}_3[x]$ vom Grad 6 mit

$$f \;=\; (x - \bar{1}) \cdot (x - \bar{2}) \cdot h.$$

Wegen $f(\bar{0}) \neq \bar{0}$, und weil f kein mehrfachen Nullstellen hat, gibt es keine weiteren Teiler vom Grad 1. Das Polynom h zerfällt also in drei irreduzible Faktoren vom Grad 2. Diese sind paarweise verschieden, weil f ansonsten in $\mathbb{F}_9$ mehrfache Nullstellen hätte. Also ist h das Produkt der drei irreduziblen Polyome vom Grad 2, die in Teil (a) bestimmt wurden. Die Zerlegung von f ist also insgesamt gegeben durch

$$(x - \bar{1}) \cdot (x - \bar{2}) \cdot (x^2 + \bar{1}) \cdot (x^2 + x + \bar{2}) \cdot (x^2 + \bar{2}x + \bar{2}).$$

Bem.:

(1) In dieser Situation kann man auch $x^8-\bar{1}$ zunächst in $(x^4-\bar{1})(x^4+\bar{1})$ zerlegen, dann $x^4-\bar{1}$ in $(x^2+\bar{1})(x^2-\bar{1}) = (x^2+\bar{1})(x-\bar{1})(x+\bar{1})$. Durch Probieren findet man mittels Teil (a) die Zerlegung $x^4+\bar{1} = (x^2+x+\bar{2})(x^2+2x+\bar{2})$.

ist

$+\bar{2})\cdot$

in

auch

$\bar{1})$ zer-

$-\bar{1}) =$

en findet

$x^4+\bar{1} =$

(2) Die Methode hier lässt sich allgemeiner anwenden. Beispielsweise kann man zeigen, dass das Polynom $x^{63}-\bar{1} \in \mathbb{F}_2[x]$ in einen irred. Faktor vom Grad 1, einem irred. Faktor vom Grad 2, 2 irred. Faktoren vom Grad 3 und 9 irreduzible Faktoren vom Grad 6 zerfällt (Übung).

(d) Bestimmen Sie ein $g \in \mathbb{F}_3[x]$, so dass $g+(x^2+\bar{1})$ in K eine primitive achte Einheitswurzel ist. Sei $u = x^2+\bar{1}$.

]

ng
dann
$L) =$

$= \{x \in L |$
t genannt.

Allgemein gilt: Ist $g \in \mathbb{F}_3[x]$ mit $u \nmid g$, dann liegt $g+(u)$ in $K^\times$ (da $u \nmid g \Leftrightarrow g \in (u)$ $\Leftrightarrow g+(u) \neq \bar{0}+(u)$) Wegen $|K^\times| = 8$ gilt $(g+(u))^8 = 1_K = \bar{1}+(u)$. Das Element $g+(u)$ hat somit genaue Ordnung 8 genau dann, wenn $(g+(u))^4 \neq 1_K$ ist.

Überprüfe $g = x+\bar{1}$. $(g+(u))^2 = (x+\bar{1})^2 + (u) =$
$x^2+\bar{2}x+\bar{1}+(u) = x^2+\bar{2}x+\bar{1}-\underbrace{(x^2+\bar{1})}_{=u}+(u) =$
$\bar{2}x+(u)$. $\Rightarrow (g+(u))^4 = (\bar{2}x+(u))^2 = (\bar{2}x)^2+(u)$
$= \bar{4}x^2+(u) = x^2+(u) = x^2-(x^2+\bar{1})+(u) = -\bar{1}+(u)$
$\neq \bar{1}+(u)$, da $1-(-\bar{1}) \notin (u)$. Also hat das

...e

...loiserw.

... sei

von G

...körper

...$\mapsto L^U$ und

...M) zueinander

gilt:

$\Leftrightarrow L^{U_1} \supseteq L^{U_2}$

$\Leftrightarrow \mathrm{Gal}(L|M_1)$

Polynom $g = x + \bar{1}$ die gewünschte Eigenschaft. $\square$

Galoistheorie

Erinnerung: Galoiserweiterung = normale und separable Erweiterung

Ist $L|K$ eine solche Erweiterung, dann nennt man $\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(a) = a \ \forall a \in K\}$ die Galoisgruppe der Erweiterung.

Ist $U \leq \mathrm{Gal}(L|K)$, dann wird $L^U = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in U\}$ der Fixkörper von U genannt.

All...

dan...

$\Leftrightarrow$ g...

$(g + (u$...

hat so...

$(g + (u$...

überprü...

$x^2 + \bar{2}x +$...

$\bar{2}x + (u$...

$= \bar{4}x^2$...

$+ \bar{1} + (u$...

Dann gilt

$= (G:U)$.

$: K]$

Dann gilt

$\Rightarrow M|K$

e der

$L = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

der Galoistheorie

nämlich die Körper

Hauptsatz der Galoistheorie

Sei $L|K$ eine <u>endliche</u> Galoiserw. und $G = \mathrm{Gal}(L|K)$. Weiter sei

$\mathcal{U}$ die Menge der Untergr. von G

$\mathcal{Z}$ die Menge der Zwischenkörper von $L|K$

Dann sind $\Phi : \mathcal{U} \to \mathcal{Z}$, $U \mapsto L^U$ und $\Psi : \mathcal{Z} \to \mathcal{U}$, $M \mapsto \mathrm{Gal}(L|M)$ zueinander inverse Bijektionen. Weiter gilt:

(1) $\forall U_1, U_2 \in \mathcal{U} : U_1 \subseteq U_2 \Leftrightarrow L^{U_1} \supseteq L^{U_2}$

$\forall M_1, M_2 \in \mathcal{Z} : M_1 \subseteq M_2 \Leftrightarrow \mathrm{Gal}(L|M_1) \supseteq \mathrm{Gal}(L|M_2)$

Polynom

Eigen

Galoist

Erinner

normale

Ist $L|K$

nennt man

$\{\sigma \in \mathrm{Aut}(L$

Galoisgrup

Ist $U \leq \mathrm{Ga}$

$\sigma(\alpha) = \alpha \ \forall \sigma \in$

lerprüfe.

$\Longrightarrow$

dnung 4

$G \cong (\mathbb{Z}/2\mathbb{Z})^2$.

) m und zwei

folgt aus

und zwei Un-

$\subsetneq U_1, U_2 \subsetneq G$

sein. Diese

(2) $L^G = K$

(3) Ist $U \in \mathcal{U}$ und $M = L^U$, dann gilt
$[L:M] = |U|$ und $[M:K] = (G:U)$.
Insbesondere gilt $|G| = [L:K]$

(4) Sei $U \in \mathcal{U}$ und $M = L^U$. Dann gilt die Äquivalenz
$U \trianglelefteq G \iff M|K$ ist normal $\iff M|K$ ist galoisch

Standardbeispiel zum Hauptsatz der Galoistheorie: Sei $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Dann hat $L|K$ laut Hauptsatz der Galoistheorie genau drei echte Zwischenkörper, nämlich die Körper

Ha

Sei

und

$\mathcal{U}$

$\mathcal{Z}$

Dann

$\Psi : \mathcal{Z}$

inverse

(1) $\forall U$

$\forall M$

$\supseteq$

$\neq \{(\bar{0},\bar{0})\}$,

$,\bar{1})\rangle, \langle(\bar{1},\bar{1})\rangle$

drei echte

$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$

wobei $\alpha = \sqrt[3]{3}$,

its bekannt:

$K|\mathbb{Q}$ nicht

e 13.01.26)

von $G = \mathrm{Gal}(L|\mathbb{Q})$

$[L:\mathbb{Q}] = 12$.

$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$

Vorgehensweise:

- Zeige $[L:K]=4$ und überprüfe, dass $L|K$ galoissch ist. $\Longrightarrow$

  $G = \mathrm{Gal}(L|K)$ ist von Ordnung 4

  4 Primzahlquadr.

  $\Longrightarrow$ $G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- Da $L|K$ mit $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ mind. zwei echte Zwischenkörper hat, folgt aus dem Hauptsatz, dass G mind. zwei Untergruppen U_1, U_2 mit $\{id\} \subsetneq U_1, U_2 \subsetneq G$ besitzt.
- Daraus folgt $G = (\mathbb{Z}/2\mathbb{Z})^2$ sein. Diese

(2)

(3)

[L

Ins

(4) Se

die

U

is

Standard

Galoisth

Dann ha

genau d

Gruppe hat genau drei Untergr. $\neq \{(\bar{0},\bar{0})\}$, $(\mathbb{Z}/2\mathbb{Z})^2$, nämlich $\langle(\bar{1},\bar{0})\rangle$, $\langle(\bar{0},\bar{1})\rangle$, $\langle(\bar{1},\bar{1})\rangle$

- Hauptsatz $\Rightarrow$ $L|K$ hat genau drei echte Zwischenkörper. Dies sind $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$

<u>H25T1A4</u>

geg. $K = \mathbb{Q}(\alpha,\beta)$, $L = K(\varepsilon)$, wobei $\alpha = \sqrt[3]{3}$, $\beta = \sqrt{3}$, $\varepsilon = e^{2\pi i/3}$ bereits bekannt: $[K:\mathbb{Q}] = 6$, $[L:\mathbb{Q}] = 12$, $K|\mathbb{Q}$ nicht galoisch, $L|\mathbb{Q}$ galoisch (siehe 13.01.26)

(c) Bestimmen Sie die Ordnung von $G = \mathrm{Gal}(L|\mathbb{Q})$

Da $L|\mathbb{Q}$ galoisch ist, gilt $|G| = [L:\mathbb{Q}] = 12$.

$\mathbb{Q}$

be

-

d

G

4 Ri

- Da [

echte

dem H

tergr

besit

- Deran

n) :
erung,
edn-
$\in L$
n $\sigma \in$
e
$), K = \mathbb{Q}$
ischenkörper
ois'sch
Nullstellen

(d) Zeigen Sie, dass G nicht abelsch ist.

Sei $U = \mathrm{Gal}(L|K)$. Dann gilt $K = L^U$ auf Grund des Hauptsatzes der Galoistheorie, und auf Grund der Ergänzungen zum Hauptsatz (siehe (4)) folgt aus der Tatsache, dass $K|\mathbb{Q}$ nicht galoissch ist, dass U kein Normalteiler von G ist.

In einer abelschen Gruppe sind alle Untergruppen Normalteiler. Also ist G nicht abelsch. $\square$

…ufe:
… $\mathbb{Q}(\sqrt{2})$
… $\sigma \in$
… $(\alpha) = \beta$
… Es gilt
… $\sqrt{2}$
… $\in G$ mit
… $\sqrt{3}) = \sqrt{3}$
… 4 folgt ins-
… $\tau, \sigma\tau\}$.

Fortsetzungssatz (für Galoiserweiterungen):

Sei $L|K$ eine endliche Galoiserweiterung, $G = \mathrm{Gal}(L|K)$, $f \in K[x]$ ein <u>irreduzibles</u> Polynom, und seien $\alpha, \beta \in L$ Nullstellen von f. Dann gibt es ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$.

Anwendung: Bestimmung der Elemente von $G = \mathrm{Gal}(L|K)$ mit $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$.
Da $L|K$ galoisch und $\mathbb{Q}(\sqrt{2})$ ein Zwischenkörper von $L|K$ ist, ist auch $L|\mathbb{Q}(\sqrt{2})$ galoisch.
Sei $\alpha = \sqrt{3}$ und $\beta = -\sqrt{3}$. Dies sind Nullstellen

(d)
Sei …
auf …
theo…
zum …
der Ta…
ist, da…
In eine…
Norma…