Bsp zu Körpermorphismen

Wir betrachten die Körpererweiterung

$\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$. Es ist $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$.

(1) Wir wollen Lemma 189 anwenden.

Sei $K = \mathbb{Q}$.

Sei $L = \mathbb{Q}(\sqrt{2})$. Sei $b = \sqrt{2}$

Sei $\Pi = \mathbb{C}$, Sei $c = -\sqrt{2}$.

Es ist $\mu_{\sqrt{2},\mathbb{Q}}(-\sqrt{2}) = (-\sqrt{2})^2 - 2 = 0$.

Also gibt es den Körpermorphismus

$$\varphi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}$$
$$f(\sqrt{2}) \longmapsto f(-\sqrt{2}),$$

wobei $f(X) \in \mathbb{Q}[X]$.

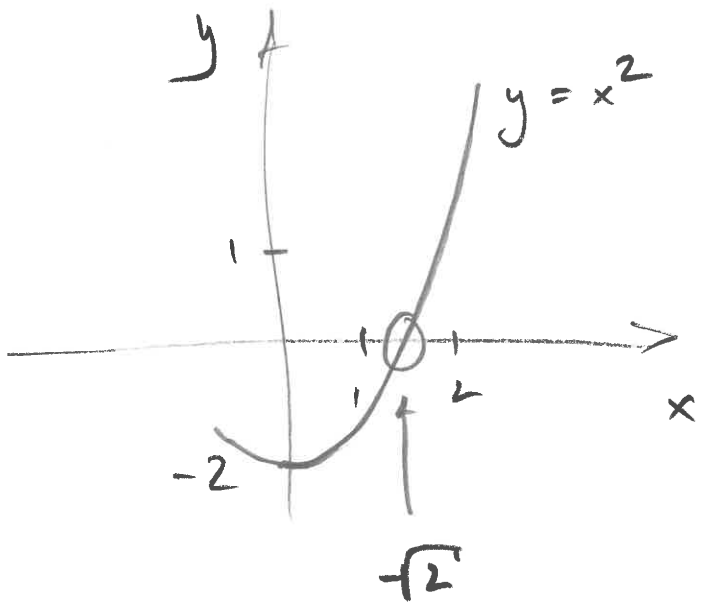
Dieser hat das Bild

$$\mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Es gilt

$$\varphi(a_0 + a_1\sqrt{2}) = a_0 + a_1(-\sqrt{2})$$
$$= a_0 - a_1\sqrt{2}.$$

(2) In der Analysis kann man $\sqrt{2}$ z.B. mit dem Zwischenwertsatz:



Man kann aber in $\mathbb{Q}(\sqrt{2})$ rechnen mit der bloßen Kenntnis, daß $(\sqrt{2})^2 = 2$ sein soll. Genauere Konstruktionen sind nicht nötig.

- In der Praxis:

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$$

$$= \{ a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q} \}$$

$$(a_0 + a_1\sqrt{2})(\tilde{a}_0 + \tilde{a}_1\sqrt{2})$$

$$= a_0\tilde{a}_0 + a_0\tilde{a}_1\sqrt{2} + a_1\tilde{a}_0\sqrt{2} + 2a_1\tilde{a}_1$$

$$= (a_0\tilde{a}_0 + 2a_1\tilde{a}_1) + (a_0\tilde{a}_1 + a_1\tilde{a}_0)\sqrt{2}$$

- In der Theorie: Wir haben den Körperisomorphismus

$$\overline{\varphi}: \mathbb{Q}[X]/(X^2+2) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})$$
$$f(X) + (X^2+2) \longmapsto f(\sqrt{2})$$

Und zur Konstruktion der linken Seite genügt die Angabe des irreduziblen Polynoms

$$X^2+2 \in \mathbb{Q}[X].$$

Bsp zu Körpermorphismen

Auf Seite 16.06.20 - 8 haben wir

$\mathbb{F}_8 = \mathbb{F}_2(\beta)$ konstruiert,

mit $\mu_{\beta,\mathbb{F}_2}(X) = X^3 + X + 1$.

Es gilt also:

$$0 = 2$$

$$\beta^3 = -\beta - 1 = \beta + 1$$

Es gilt $\mathbb{F}_8 = \{a_0 + a_1\beta + a_2\beta^2 : a_0, a_1, a_2 \in \mathbb{F}_2\}$

Wir haben den Frobenius-

Automorphismus ...

... $\mathrm{Fr}_{\mathbb{F}_8} : \mathbb{F}_8 \longrightarrow \mathbb{F}_8 :$

$$a_0 + a_1\beta + a_2\beta^2 \longmapsto (a_0 + a_1\beta + a_2\beta^2)^2$$

$$= a_0^2 + a_1^2\beta^2 + a_2^2\beta^4$$

$$= a_0 + a_1\beta^2 + a_2(\beta^2 + \beta)$$

$$= a_0 + a_2\beta + (a_1 + a_2)\beta^2$$

Dies ist insbesondere eine $\mathbb{F}_2$-lineare Abbildung von $\mathbb{F}_8$ nach $\mathbb{F}_8$, welche bezüglich der Standardbasis $(\beta^0, \beta^1, \beta^2)$:

$$\begin{array}{c} \\ \beta^0 \\ \beta^1 \\ \beta^2 \end{array} \begin{array}{c} \begin{array}{ccc} \beta^0 & \beta^1 & \beta^2 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \in \mathbb{F}_2^{3\times 3}$$

Es gilt

$$\left(Fr_{\mathbb{F}_8}\right)^3 = id_{\mathbb{F}_8},$$

da $\left(Fr_{\mathbb{F}_8}\right)^3(\beta) = \beta^8$

$$= (\beta^4)^2$$

$$= (\beta^2 + \beta)^2$$

$$= \beta^4 + \beta^2$$

$$= \beta^2 + \beta + \beta^2$$

$$= \beta,$$

und da folglich

$$\left(Fr_{\mathbb{F}_8}\right)^3 (a_0 + a_1\beta + a_2\beta^2)$$

$$= a_0 + a_1 Fr_{\mathbb{F}_8}(\beta) + a_2 Fr_{\mathbb{F}_8}(\beta)^2$$

$$= a_0 + a_1\beta + a_2\beta^2$$

$$\ldots = a_0 + a_1 \beta + a_2 \beta^2 \quad \text{Ist.}$$

Die Lineare Algebra bestätigt dies: es ist auch

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^3$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_3 .$$

Bsp für Multiplikativität der Grade.

Wir wollen zeigen, daß es

keinen Körper Z gibt

mit $\mathbb{F}_8 \mid Z \mid \mathbb{F}_2$

und mit $\mathbb{F}_2 \subsetneq Z \subsetneq \mathbb{F}_8$.

Annahme, doch.

Es ist

$$3 = [\mathbb{F}_8 : \mathbb{F}_2] \overset{L193}{=} [\mathbb{F}_8 : Z] \cdot [Z : \mathbb{F}_2]$$

3 prim $\Longrightarrow$ $[\mathbb{F}_8 : Z] = 1$ oder $[Z : \mathbb{F}_2] = 1$

$\Rightarrow$ $\mathbb{F}_8 = Z$ oder $Z = \mathbb{F}_2$. ↯

Insbesondere gibt es in $\mathbb{F}_8$ keinen Teilkörper mit 4 Elementen.

Dies wollen wir auch noch durch Angabe der Minimalpolynome aller Elemente von $\mathbb{F}_8$ nochmals bestätigen:

$b \in \mathbb{F}_8$	$\mu_{b,\mathbb{F}_2}(X) \in \mathbb{F}_2[X]$
0	X
1	$X+1$
β	X^3+X+1
$1+\beta$	X^3+X^2+1
$\vdots$	

ist irreduzibel und hat Nullstelle $1+\beta$

⋮

β^2	$X^3 + X + 1$
$1 + \beta^2$	$X^3 + X^2 + 1$
$\beta + \beta^2$	$X^3 + X + 1$
$1 + \beta + \beta^2$	$X^3 + X^2 + 1$

Sei nun $\mathbb{F}_8 \mid Z \mid \mathbb{F}_2$

mit $Z \subsetneq \mathbb{F}_8$ gegeben.

Dann darf <u>keines</u> der Elemente

$\beta,\ 1+\beta,\ \beta^2,\ 1+\beta^2,\ \beta+\beta^2,\ 1+\beta+\beta^2$

in Z liegen :

Annahme, doch.

Dann gibt es in Z ein Element b mit $\mu_{b,\mathbb{F}_2}(X)$ vom Grad 3.

Es folgt :

$$[\mathbb{F}_8 : \mathbb{F}_2] \geq [Z : \mathbb{F}_2] \geq [\mathbb{F}_2(b) : \mathbb{F}_2]$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$3 \qquad\qquad\qquad\qquad \deg\left(\mu_{b,\mathbb{F}_2}(X)\right)$$

$$\|$$

$$3$$

Also $[Z : \mathbb{F}_2] = 3$.

Also $Z = \mathbb{F}_8$. ↯

Bem. Multiplikativität von Graden.

Man kann nun für eine endliche Körpererweiterung $L|K$ vom Grad $n := [L:K]$ allgemein feststellen:

Ist $L|Z|K$, ist also Z ein Zwischenkörper von $L|K$, dann ist der Grad $[Z:K]$ ein Teiler von n.

Dies schränkt bei der Suche nach Zwischenkörpern den ...

... Suchbereich deutlich ein.

Ist z.B. n prim, so

gibt es außer den

Zwischenkörpern L und K

keine weiteren Zwischenkörper.