Körpertheorie

Erinnerung: Ringhomomorphismus = Abb. $\phi : R \to S$ zwischen Ringen R, S mit $\phi(1_R) = 1_S$, $\phi(a+b) = \phi(a) + \phi(b)$ und $\phi(ab) = \phi(a)\,\phi(b)$, jeweils für alle $a, b \in R$.

Def i) Ein Ringhom. $\phi : K \to L$ zwischen Körpern K, L wird auch **Körperhomomorphismus** genannt. (Es gilt dann $\phi(a^{-1}) = a^{-1}$

phismus genannt. (Es gilt dann $\phi(a^{-1}) = a^{-1}$ für alle $a \in K^\times$. Hinweis: Körperhomomorphismen sind immer injektiv.)

(ii) Erinnerung: Die Notation $L|K$ bedeutet für Körper K und L, dass diese eine Körpererweiterung bilden, d.h. dass K ein Teilkörper von L ist.

Seien L und M beides Erweiterungskörper eines weiteren Körpers K. Dann ist ein K-Homomorphismus von L nach M ein

Körperhom. $\phi : L \to M$ mit $\phi(a) = a \; \forall a \in K$.

Def: Sei $L|K$ eine Körpererweiterung. Dann existiert auf L die Struktur eines K-Vektorraums (Vektoraddition $L \times L \to L$, $(\alpha, \beta) \mapsto \alpha + \beta$, skalare Multiplikation $K \times L \to L$, $(a, \alpha) \mapsto a\alpha$) Die Dimension dieses K-Vektorraums L ist der Grad $[L:K]$ der Erweiterung.

Bsp: $[\mathbb{C}:\mathbb{R}] = 2$, denn $\{1, i\}$ ist eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum

H24T1A4 (a) Sei $K|\mathbb{Q}$ eine Körpererweiterung. Zeigen Sie, dass jeder Körperhomomorphismus $\varphi: K \to K$ ein $\mathbb{Q}$-Homomorphismus ist.

(b) Sei $K|\mathbb{Q}$ eine endliche Erw. (d.h. der Grad $[K:\mathbb{Q}]$ ist endlich). Zeigen Sie: dass φ bijektiv ist.

(c) Geben Sie ein Beispiel für eine Körpererw. $K|\mathbb{Q}$ und einen $\mathbb{Q}$-Hom. $K \to K$ an, der nicht bijektiv ist

zu (a) ϕ Körperhom. $\Rightarrow \phi(0) = 0$, $\phi(1) = 1$

Beh.: $\phi(n) = n \quad \forall n \in \mathbb{N}_0$ Do Ind.-anfang ist bereits erledigt Ind.-schritt: Sei $n \in \mathbb{N}_0$, setze $\phi(n) = n$ voraus. $\Rightarrow \phi(n+1) = \phi(n) + \phi(1) = n + 1$. ($\Rightarrow$ Beh.)
↑ ϕ Körperhom

Für jedes $m \in \mathbb{N}$ gilt $\phi(-m) = -\phi(m) = -m$, insgesamt also $\phi(a) = a \quad \forall a \in \mathbb{Z}$
↑ ϕ Körperhom.

Sei nun $r \in \mathbb{Q}$, $r = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$
$\Rightarrow \phi(r) = \phi(a b^{-1}) = \phi(a)\phi(b)^{-1} \overset{s.o.}{=}$
↑ ϕ Körperhom

(ii)

zu (i)

$\mathbb{Q}[t]$

$\Rightarrow u$

$u'(t^2)$

zu (ii) Je

$a = \frac{a}{1}$,

von $\mathbb{Q}[t$

$\Rightarrow \gamma(a) =$

Seien α, β

$aG^{-1} = r$. $\forall r \in \mathbb{Q}: \phi(r) = r \Rightarrow \phi$ ist ein $\mathbb{Q}$-Homomorphismus.

zu (b) Laut Vorlesung sind alle Körperhom. injektiv, somit auch ϕ. Die Abbildung $\phi: K \to K$ ist linear, also ein Homomorphismus von $\mathbb{Q}$-Vektorräumen, denn für alle $\alpha, \beta \in K$ gilt $\phi(\alpha+\beta) = \phi(\alpha) + \phi(\beta)$ (ϕ Körperhom.) und für alle $a \in \mathbb{Q}$ und $\alpha \in K$ auch $\phi(a\alpha) = \phi(a)\phi(\alpha) = a\phi(\alpha)$ (Teil (a), ϕ ist $\mathbb{Q}$-Hom.). Als injektive lineare Abbildung zwischen Vektorräumen derselben endlichen Dimension ist ϕ laut Lineare Algebra auch bijektiv (Das wurde dort aus dem Dimensionssatz für lineare

ϕ ist

...ehom.

...bildung

...omomorphis-

... für alle α, β

... und für alle

$\phi(a)\phi(x) \overset{\text{Teil (a)}}{=} \phi(ax)$

ϕ ist $\mathbb{Q}$-Hom.

... Abbildung

...en endlichen

...algebra auch bijektiv

...satz für lineare

Abbildungen hergeleitet.)

zu (c) Sei $K = \mathbb{Q}(t)$ der rationale Funktionenkörper über $\mathbb{Q}$, also der Quotientenkörper des Polynomrings $\mathbb{Q}[t]$. Betrachte die Abbildung

$\Psi: K \to K$ gegeben durch $\Psi\left(\frac{u}{v}\right) = \frac{u(t^2)}{v(t^2)}$

$\forall\, u \in \mathbb{Q}[t]$ und $v \in \mathbb{Q}[t] \setminus \{0\}$

Beh: (0) Ψ ist wohldefiniert, also unabh. von der Darstellung es Elements aus $\mathbb{Q}(t)$ als Quotient von Polynomen

(i) Ψ ist ein $\mathbb{Q}$-Hom.

$0) = 0 \,,\ \phi(1) = 1$

Ind.-anfang

chritt : Sei n

s. $\Rightarrow \phi(n+1)$

$(\Rightarrow$ Beh.$)$

$m) = -\phi(m)$

$\uparrow$ ϕ Körperhom.

$= a \ \forall\, a \in \mathbb{Z}$

$a \in \mathbb{Z},\ b \in \mathbb{N}$

$) \phi(b)^{-1} \overset{\text{s.o}}{=}$

rperhom.

(ii) φ ist nicht surjektiv (und somit auch nicht bijektiv)

zu (i) Seien $u, u' \in \mathbb{Q}[t]$ und $v, v' \in \mathbb{Q}[t] \setminus \{0\}$ mit $\frac{u}{v} = \frac{u'}{v'}$ in K

$\Rightarrow uv' = u'v \Rightarrow u(t^2)v'(t^2) = u'(t^2)v(t^2) \Rightarrow \frac{u(t^2)}{v(t^2)} = \frac{u'(t^2)}{v'(t^2)}$

zu (ii) Jedes $a \in \mathbb{Q}$ hat die Darstellung $a = \frac{a}{1}$, wobei wir $a, 1$ als Elemente von $\mathbb{Q}[t]$ bzw. $\mathbb{Q}[t] \setminus \{0\}$ betrachten

$\Rightarrow \varphi(a) = \varphi\left(\frac{a}{1}\right) = \frac{a(t^2)}{1(t^2)} = \frac{a}{1} = a$

Seien $\alpha, \beta \in K$, $\alpha = \frac{u}{v}$, $\beta = \frac{u'}{v'}$ mit

mit $u, u' \in \mathbb{Q}[t]$, $v, v' \in \mathbb{Q}[t] \setminus \{0\}$. $\frac{u}{v} + \frac{u'}{v'} = \frac{uv' + u'v}{vv'}$

$\Rightarrow \varphi(\alpha+\beta) = \varphi\left(\frac{uv'+u'v}{vv'}\right) = \frac{u(t^2)v'(t^2) + u'(t^2)v(t^2)}{v(t^2)v'(t^2)} =$

$\frac{u(t^2)}{v(t^2)} + \frac{u'(t^2)}{v'(t^2)} = \varphi(\alpha) + \varphi(\beta)$, $\varphi(\alpha\beta) = \varphi\left(\frac{uu'}{vv'}\right) = \frac{u(t^2)u'(t^2)}{v(t^2)v'(t^2)}$

$= \varphi(\alpha)\varphi(\beta)$

zu (ii) Seien $u, v \in \mathbb{Q}[t] \setminus \{0\}$. $m = \operatorname{grad}(u)$, $n = \operatorname{grad}(v)$

Seien $u', v' \in \mathbb{Q}[t] \setminus \{0\}$ mit $\frac{u'}{v'} = \varphi\left(\frac{u}{v}\right)$. $\Rightarrow$

$\frac{u'}{v'} = \frac{u(t^2)}{v(t^2)} \Rightarrow u'v(t^2) = u(t^2)v' \Rightarrow \operatorname{grad}(u') + 2n =$

$2m + \operatorname{grad}(v') \Rightarrow \operatorname{grad}(u') - \operatorname{grad}(v') = 2m - 2n$

$2m + \text{grad}(v') \Rightarrow \text{grad}(u') - \text{grad}(v') = 2m - 2n$

also: Ist $\frac{u'}{v'} \in K$ ein Element des Bildes von Ψ (mit $u', v' \in \mathbb{Q}[t] \setminus \{0\}$), dann ist $\text{grad}(u') - \text{grad}(v')$ immer eine gerade ganze Zahl. aber: $t = \frac{t}{1}$, $\text{grad}(t) = 1$, $\text{grad}(1) = 0$, $1 - 0 = 1$ ist ungerade. Somit ist $t \in K$ nicht im Bild von Ψ enthalten, und Ψ somit nicht surjektiv. □

Def. Sei $L|K$ eine Körpererweiterung

(i) Ein Element $\alpha \in L$ wird algebraisch über K genannt, wenn ein $f \in K[t] \setminus \{0\}$ mit $f(\alpha) = 0$ existiert.

(ii) Die Erweiterung $L|K$ heißt algebraisch, wenn jedes $\alpha \in L$ algebraisch über K ist.

Erinnerung:

(i) Jede endliche Körpererweiterung ist algebraisch.

(ii) Nicht jede algebraische Erweiterung ist endlich (z.B. $\mathbb{Q}^{alg} | \mathbb{Q}$, wobei $\mathbb{Q}^{alg}$ einen algebraischen Abschluss von $\mathbb{Q}$ bezeichnet, oder $\mathbb{Q}(S) | \mathbb{Q}$ mit $S = \{\sqrt[n]{2} \mid n \in \mathbb{N}\}$) Übung: F22T1A5

(iii) Jede Erweiterung $L | K$, die von einer endlichen Teilmenge $S \subseteq L$ bestehend aus über K algebraischen Elementen ist

endlich und somit auch algebraisch.

Bsp: $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[5]{\sqrt{3}+\sqrt[3]{4}}) \mid \mathbb{Q}$ ist eine endliche Körpererweiterung.

Def. Sei $L \mid K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Das eindeutig bestimmte normierte Polynom minimalen Grades mit α als Nullstelle wird das Minimalpolynom von α über K genannt (Notation $\mu_{\alpha, K}$)

Erinnerung: $f \in K[x]$ normiert, irreduzibel über K, $f(\alpha) = 0 \Rightarrow f = \mu_{\alpha, K}$

Beispiele: (i) $\mu_{\sqrt{2},\mathbb{Q}} = x^2 - 2$,

$\mu_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$ (Polynome sind irreduzibel nach dem Eisenstein-Kriterium)

(ii) K bel. Körp., $a \in K \Rightarrow \mu_{a,K} = x - a$

(iii) $n \in \mathbb{N}$, $n \geq 3$, $\zeta = e^{2\pi i/n}$ (primitive n-te Einheitswurzel) $\Rightarrow$

$\mu_{\zeta,\mathbb{Q}} = \Phi_n$ n-tes Kreisteilungspolynom

F19T1A5

(a) Sei $\alpha = \sqrt[3]{2+\sqrt{2}}$. Bestimmen Sie das

Erinne

$\alpha \in L$ a

grad(f

elementge

jedes $\beta \in$

$\beta = a_0 + a$

$a_0, a_1, \ldots,$

$[K(\alpha) : K$

Bsp. Ist A

von $\mathbb{F}_2$ und

$f = x^3 + x +$

Minimalpolynom von α über $\mathbb{Q}$

$\alpha = \sqrt[3]{2+\sqrt{2}} \Rightarrow \alpha^3 = 2+\sqrt{2} \Rightarrow \alpha^3 - 2 = \sqrt{2}$

$\Rightarrow (\alpha^3-2)^2 = 2 \Rightarrow \alpha^6 - 4\alpha^3 + 4 = 2$

$\Rightarrow \alpha^6 - 4\alpha^3 + 2 = 0 \Rightarrow \alpha$ ist Nullstelle von $f = x^6 - 4x^3 + 2 \in \mathbb{Q}[x]$. Offenbar ist f normiert, außerdem auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 2) irreduzibel. Insgesamt gilt also $f = \mu_{\alpha,\mathbb{Q}}$.

Erinnerung: Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K, $f = \mu_{\alpha,K}$ und $n = \operatorname{grad}(f)$. Dann ist $\{1, \alpha, \dots, \alpha^{n-1}\}$ eine n-elementige Basis von $K(\alpha)$ als K-Vektorraum, d.h. jedes $\beta \in K(\alpha)$ hat eine eindeutige Darstellung

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$$ mit

$a_0, a_1, \dots, a_{n-1} \in K$. Insbesondere gilt

$$[K(\alpha) : K] = n.$$

Bsp. Ist $\mathbb{F}_2^{alg}$ ein algebraischer Abschluss von $\mathbb{F}_2$ und $\alpha \in \mathbb{F}_2^{alg}$ eine Nullstelle von $f = x^3 + x + 1$, dann ist $\mathbb{F}_2(\alpha)$ ein Körper

Bsp: Ist $\mathbb{F}_2^{alg}$ ein algebraischer Abschluss

Q.

$2 = \sqrt{2}$

$4 = 2$

Null-

$[x]$. Offen-

f Grund des

ndet auf die

esamt gilt

mit acht Elementen, also $\mathbb{F}_2(\alpha) = \mathbb{F}_8$.

Es ist $\mathbb{F}_8 = \{\bar{0}, \bar{1}, \alpha, \alpha + \bar{1}, \alpha^2, \alpha^2 + \bar{1}, \alpha^2 + \alpha, \alpha^2 + \alpha + \bar{1}\}$. Es genügt dafür zu überprüfen, dass $f = \mu_{\alpha, \mathbb{F}_2}$ gilt. klar: $f(\alpha) = \bar{0}$, f ist normiert. Außerdem ist f in $\mathbb{F}_2[x]$ irreduzibel, denn: $\text{grad}(f) = 3$, und wegen $f(\bar{0}) = f(\bar{1}) = \bar{1}$ hat f in $\mathbb{F}_2$ keine Nullstelle. $\square$