$K \subseteq L$

$v \in L$

$K[v] = \{A(v) | A \in K[X]\}$

v algebraisch über K, wenn ein $A \neq 0$ existiert mit $A(v) = 0$

$M = M_v$ Minimalpolynom von v irreduzibel

$K[v] = K(v) \hat{=} K_M = K_m[X]$, $m = \operatorname{grad} M$

$A \cdot_m B = \rho_M(AB)$

7.7. $[K(v) : K] = \operatorname{grad} M$ und $1, v, ..., v^{m-1}$ ist Basis von $K(v)_K$

Beispiel:

$K = \mathbb{Q}$, $L = \mathbb{C}$

$v = \sqrt{2}, M_v = X^2 - 2$

$1, \sqrt{2}$ ist Basis von $K[\sqrt{2}]$ über K

$a = a_0 + a_1\sqrt{2}$, $a_i \in K$, $A = a_0 + a_1 X$

$b = b_0 + b_1\sqrt{2}$ $B = b_0 + b_1 X$

$a + b = (a_0 + b_0) + (a_1 + b_1)\sqrt{2}$ $|A + B$

$a \cdot b = (a_0 + a_1\sqrt{2})(b_0 + b_1\sqrt{2}) = (a_0 b_0 + 2a_1 b_1) + (a_0 b_1 + b_0 a_1)\sqrt{2}$

$A \cdot B = (a_0 + a_1 X)(b_0 + b_1 X) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + a_1 b_1 X^2$

$\rho_M(AB) = (a_0 b_0 + 2a_1 b_1) + (a_0 b_1 + a_1 b_0) X$

$M = X^2 - 2$

$X^2 = M + 2$

$\rho_M(X^2) = 2$

Beispiel:

$K = \underset{\mathbb{R}}{\mathbb{Q}}$, $L = \mathbb{C}$

$v = i$ $1, i$ Basis von $K(v)_K$

$M = X^2 + 1$

$\rho_M(X^2) = -1$

Definition:

a) L heißt **algebraische Erweiterung** von K, wenn jedes Element $v \in L$ algebraisch über K $\left(L \in \mathrm{E}_{\mathrm{alg}}(K)\right)$

b) K heißt **algebraisch abgeschlossen**, wenn jedes $A \in K[X]$, $\operatorname{grad} A \geq 1$, eine Nullstelle in K hat

c) $\bar{K} \in \mathrm{E}(K)$ heißt **algebraischer Abschluss** von K, wenn

a. $\bar{K}$ ist algebraisch über K $\left(\bar{K} \in \mathrm{E}_{\mathrm{alg}}(K)\right)$

b. $\bar{K}$ ist algebraisch abgeschlossen

Hauptsatz der Algebra:

$\mathrm{E}_{\mathrm{alg}}(\mathbb{C}) = \mathbb{C}$

$\overline{\mathbb{C}} = \mathbb{C} \qquad \left(\overline{\mathbb{R}} = \mathbb{C}\right)$

7.8. a) $L \in \mathrm{E}_{\mathrm{end}}(K) \Rightarrow L \in \mathrm{E}_{\mathrm{alg}}(K)$

Beweis: $v \in L, [L:K] = n$

$\underbrace{1, v, v^2, ..., v^n}_{n+1}$ sind linear unabhängig in L_K

$0 = \sum_{i=0}^{n} a_i v^i, \ a_i \in K$, nicht alle $a_i = 0$

$A = \sum_{i=0}^{n} a_i X^i \neq 0$

$A(v) = 0$

b) $v_1, ..., v_n \in L$ und v_i algebraisch über K, $\quad i = 1, ..., n$

$K(v_1, v_2, ..., v_n) \in \mathrm{E}_{\mathrm{end}}(K) \subseteq \mathrm{E}_{\mathrm{alg}}(K)$

$[K(v_1) : K] = \operatorname{grad} M_{v_1} < \infty$

v_2 algebraisch über (v_1)

$K(v_1)(v_2) = K(v_1, v_2) \in \mathrm{E}_{\mathrm{end}}(K(v_1))$

Gradformel: $K(v_1, v_2) \in \mathrm{E}_{\mathrm{end}}(K)$

$K(v_1, v_2)(v_3) = K(v_1, v_2, v_3)$ .... usw.....

c) Sei $K \underset{\mathrm{alg}}{\subseteq} L \underset{\mathrm{alg}}{\subseteq} H, \ H \in \mathrm{E}(L)$

$L \in \mathrm{E}_{\mathrm{alg}}(K), \ H \in \mathrm{E}_{\mathrm{alg}}(L)$

$\Rightarrow H \in \mathrm{E}_{\mathrm{alg}}(K)$

$v \in H$

n.V. $\sum_{i=1}^{n} a_i v^i = 0, \ a_i \in L$

$a_0, a_1, ..., a_n \in L$

$$K(a_0,a_1,...,a_n)\in \mathrm{E}_{\mathrm{end}}(K)$$
$$v\in\big(K(a_0,a_1,...,a_n)\big)(v)\in \mathrm{E}_{\mathrm{end}}(K)...$$
$$\overset{\text{a)}}{\Rightarrow}\ v \text{ algebraisch}$$

7.9. Es existiert der algebraische Abschluss $\overline{K}$

Beweisskizze:

Ich tue so, als sei $\mathrm{E}_{\mathrm{alg}}(K)$ eine Menge, die durch Inklusion geordnet ist! (ist aber nicht so!)

Sei $\{L_i\}_{i\in\mathbb{N}}$ Kette in $\mathrm{E}_{\mathrm{alg}}(K)$

$$L_i\subseteq L_{i+1}$$
$$L:=\bigcup_{i\in\mathbb{N}} L_i\in \mathrm{E}_{\mathrm{alg}}(K)$$
$$a,b\in L$$

$\exists$i mit $a,b\in L_i\in \mathrm{E}(K)$

$\Rightarrow\ a+b,\ ab,\ a^{-1}\in L_i\subseteq L$

$L\in \mathrm{E}_{\mathrm{alg}}(K)$ ist ein maximales Element

$(L_i\subseteq L\ \forall i)$

Zorn'sches Lemma $\Rightarrow \mathrm{E}_{\mathrm{alg}}(K)$ heißt **maximales Element**

Behauptung: L ist $\overline{K}$

1) v algebraisch über L, $L(v)$

$$K\underset{\text{alg}}{\subseteq} L\underset{\text{alg}}{\subseteq} L(v)\overset{\text{7.8.c)}}{\Rightarrow} L(v) \text{ algebraisch über } K\in \mathrm{E}_{\mathrm{alg}}(K)\Rightarrow L(v)=L$$

$\mathbb{Q}\subseteq\overline{\mathbb{Q}}\subseteq\mathbb{C}$ algebraisch abgeschlossen

$$\mathrm{E}_{\mathrm{alg}}(\mathbb{Q})"="\left\{L\,\middle|\begin{array}{l}L \text{ algebraisch über } \mathbb{Q}\\ L \text{ Teilkörper von } \mathbb{C}\end{array}\right\}$$

... $\underset{\subseteq\mathbb{C}}{\overline{\mathbb{Q}}}$ algebraischer Abschluss von $\mathbb{Q}$

Für den Augenblick $\overline{1}=1_K, \overline{0}=0_K$

$$i\in\mathbb{N}_0,\quad \overline{i}=\underbrace{\overline{1}+...+\overline{1}}_{i}\in K$$
$$-\overline{i}=-\overline{1}-...-\overline{1}=:\left(\overline{-i}\right)$$

$R := \{\overline{i} \mid i \in \mathbb{Z}\}$ ist nullteilerfrei

Unterring des Körpers K

$$\overline{i} + \overline{j} = \underbrace{(\overline{1} + ... + \overline{1})}_{i-\text{mal}} + \underbrace{(\overline{1} + ... + \overline{1})}_{j-\text{mal}} = \overline{i + j}$$

$$\overline{i} \cdot \overline{j} = \underbrace{(\overline{1} + ... + \overline{1})}_{i-\text{mal}} \cdot \underbrace{(\overline{1} + ... + \overline{1})}_{j-\text{mal}} = \underbrace{\overline{1} + ... + \overline{1}}_{i \cdot j-\text{mal}} = \overline{i \cdot j}$$

$\varphi : \mathbb{Z} \to \mathbb{R}$ und $i \to \overline{i}$

Ringhomomorphismus

$\ker \varphi$ ist Ideal in $\mathbb{Z}$ $\quad \left(R \cong \mathbb{Z}/\ker \varphi\right)$

1. Fall: $\ker \varphi = \{0\}$, d.h. $R \overset{\text{Isomorph}}{\cong} \mathbb{Z}$

Bilde quat $R = \left\{\frac{a}{b} \mid a, b \in R, b \neq 0\right\} \subseteq K \cong Q$

2. Fall: $\ker \varphi \neq 0$, $p := \min(\ker \varphi)$ ist die kleinste Zahl $i \in \mathbb{N}$ mit $\overline{i} = 0$

Kapitel 1: $\ker \varphi = \langle p \rangle$ Homomorphiesatz $\underbrace{\mathbb{Z}/\langle p \rangle}_{\mathbb{Z}_p} \cong R$

p ist Primzahl

($p = a - b$, $0 = \overline{p} = \overline{ab} = \overline{a}\overline{b} \quad \Rightarrow \overline{a} = 0$ oder $\overline{b} = 0$

widerspricht der Minimalität von p)

Bezeichnung: $p = \text{char } K$ (Charakteristik)

Im Fall $\ker \varphi = \{0\}$ ist $\text{char } K = 0$

7.10. Satz

Sei $p = \text{char } K$ und K_p der kleinste Teilkörper von K

Dann

a) Ist $p = 0$, so ist K_p isomorph zum Körper Q ($K_p = \text{quat } R$)

b) Ist $p \neq 0$, so ist K_p isomorph zum Körper $\mathbb{Z}_p$ (und $K_p = R$)

8. Endliche Körper

K endliche Körper, $q := |K|$, $p = \text{char } K$ Primzahl

Der Vektorraum K_{K_p} (über dem Körper $K_p \cong \mathbb{Z}_p$) ist endlich dimensional,
sei $n = [K : K_p]$, also $K_{K_p} \cong K_p^n \cong (\mathbb{Z}_p)^n$

8.1. Satz
$q = p^n$ **Primzahlpotenz**

Beispiel: $N \in \mathbb{Z}_p[X]$ irreduzibel
$K = (\mathbb{Z}_p)_N$ ist endlicher Körper mit p^n Elementen, $n = \text{grad } N$

8.2. Satz
Die multiplikative Gruppe K^* von K ist eine zyklische Gruppe der Ordnung $\underbrace{q-1}_{m}$

$z \in K^*$ heißt **primitives Element** von K, wenn $K^* = \langle z \rangle$

8.3. a) $K^* = \{1 = z^0, z, z^2, ..., z^{m-1}\}$
b) $z^i z^j = z^{i+mj}$
c) Ein Element $a = z^i$ ist genau dann primitiv, wenn $\text{ggT}(i, m) = 1$