

Teil III: Körper $\leadsto$ Körper = Ring R mit $R^\times = R \setminus \{0\}$

Bisher: $\underbrace{\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}}_{\text{Char. 0}}, \underbrace{\mathbb{F}_p}_{\text{Char. } p}$ Was gibt es noch?

A18: Algebraische Erweiterungen

18.1. Einleitung: Körpererweiterung $L|K$, $x \in L$ alg. über K
($x \in \mathbb{R}$ alg. über $\mathbb{Q}$)

18.2. Def.: Sei K Körper, betr. Ringhom. $\varphi: \mathbb{Z} \rightarrow K$, $m \mapsto m_K := m \cdot 1_K$.

Dann: $\varphi(\mathbb{Z}) \cong \mathbb{Z} / \ker \varphi$ mit $\ker \varphi = (r)$, $r \in \mathbb{N}_0$.

Charakteristik von K : $\text{Char } K := r$. $\uparrow$

r minimal mit $\underbrace{1_K + \dots + 1_K}_{r \text{ mal}} = 0_K$, falls $r > 0$

18.3. Lemma: (i) $r \neq 0$: $\varphi(\mathbb{Z})$ keine Nullteiler ($\neq 0$) $\Rightarrow$ $r = p$ prim.

$\uparrow$ r zus. ges. mit $r \cdot 1 = 0 \Rightarrow r = m \cdot k \Rightarrow \underbrace{m \cdot k \cdot 1}_m = 0 \subseteq$

Somit: $K_0 := \varphi(\mathbb{Z}) \cong \mathbb{F}_p$ Körper.

(ii) $r = 0$: φ injektiv. $K_0 := \left\{ \frac{\varphi(m)}{\varphi(n)} ; m, n \in \mathbb{Z}, n \neq 0 \right\}$
ist Quotientenkörper von $\varphi(\mathbb{Z})$.

Dann: $\mathbb{Z} \xrightarrow[\varphi]{\cong} \varphi(\mathbb{Z}) \subseteq K_0$

$\downarrow \quad \quad \quad \cong \quad \quad \quad \nearrow$
 $\mathbb{Q} \quad \quad \quad \varphi \quad \quad \quad$ (Univ. Eig. von Quot. Körpern)
 $\uparrow$ zunächst Ringiso $\leadsto$ Körperiso

Somit lässt sich φ erweitern zu Iso $\bar{\varphi}: \mathbb{Q} \cong K_0$. Ist Körper!

In beiden Fällen: K_0 ist kleinste Teilkörper von K .

18.4. Def.: K_0 heißt Primkörper von K . ($\rightarrow$ vgl. Primring in A11.25)

Erinnerung an A12.30: Univ. Eig. von Quot. Körpern: $\mathbb{Q} = \text{Quot}(R)$

$R \hookrightarrow Q'$		$\forall i: R \rightarrow Q', i$ inj. Ringhom.
$\downarrow \quad \quad \quad \nearrow$ $Q \quad \quad \quad \exists! \varphi: \varphi \circ i = i$		$\exists! \varphi: Q \hookrightarrow Q', \varphi$ inj. Ringhom.

18.5. Def: L heißt Körpererweiterung von K : $L|K : \Leftrightarrow L, K$ Körper, $K \subseteq L$.
(K heißt Teilkörper von L) spricht " L über K "

18.6. Def: $[L:K] := \dim_K L$ (Dim. von L als K -VR)
heißt (Körper-) Grad von $L|K$

vgl.: $m, n \in \mathbb{Z}$
 $m | n$ "teilt"
 $\Leftrightarrow m \mathbb{Z} \subseteq n \mathbb{Z}$ "über"
↑

L heißt endliche Erweiterung von $K : \Leftrightarrow [L:K]$ endl. $\left(\begin{array}{c} L \\ | \\ K \end{array} \right)$

18.7. Bsp: $\mathbb{C}|\mathbb{R}$, $[\mathbb{C}:\mathbb{R}] = 2$. $\left(\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array} \right)$

18.8. Satz: $E|L$ und $L|K$ endl. $\Rightarrow E|K$ endl. und $[E:K] = [E:L] \cdot [L:K]$.
(Multiplikativität des Körpergrads)

Bew.: Sei $x_1, \dots, x_m$ L -Basis von E

$y_1, \dots, y_n$ K -Basis von L .

Dann: $x_i y_j$ bilden K -Basis von E ,

denn: erst: Sei $z \in E$, $z = \sum_{i=1}^m w_i x_i$, $w_i \in L$

$$w_i = \sum_{j=1}^n a_{ij} y_j, \quad 1 \leq i \leq m \Rightarrow z = \sum_{i,j} a_{ij} x_i y_j$$

lin. unabh.: Sei $\sum_{i,j} a_{ij} x_i y_j = 0$, die $a_{ij} \in K$

$$\Rightarrow 0 = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} y_j \right) x_i \quad \Rightarrow \forall i: \sum_{j=1}^n a_{ij} y_j = 0 \Rightarrow \forall i,j: a_{ij} = 0.$$

□

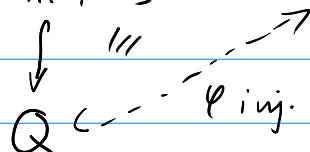
18.9. Def: Sei $L|K$, $x_1, \dots, x_n \in L$. Dann:

$K(x_1, \dots, x_n) := \bigcap \{K'; K \subseteq K' \subseteq L, K' \text{ Körper}, x_1, \dots, x_n \in K'\}$
↑ heißt der von $x_1, \dots, x_n$ über K erzeugte Körper.

spricht: " K adjungiert x_1 bis x_n " $\rightarrow$ Körper-Adjunktion

18.10. Lemma: $K(x_1, \dots, x_n)$ ist der Quotientenkörper von $K[x_1, \dots, x_n]$, d.h. $K(x_1, \dots, x_n) = \text{Quot}(K[x_1, \dots, x_n])$,
d.h. $\forall z \in K(x_1, \dots, x_n) (\Leftrightarrow) \exists u, v \in K[x_1, \dots, x_n] : (v \neq 0 \wedge z = \frac{u}{v})$,
 $= \left\{ \sum a_i x_1^{i_1} \dots x_n^{i_n}, \dots \right\}$

Bew.: $K[x_1, \dots, x_n] \hookrightarrow K(x_1, \dots, x_n)$



Sei Q der Quot. Körper von $K[x_1, \dots, x_n]$

Univ. Eig. von Quot. Körpern

$\Rightarrow \exists \varphi: Q \hookrightarrow K(x_1, \dots, x_n)$.

Nun enthält Q sicher $x_1, \dots, x_n$ sowie K , d.h. $K(x_1, \dots, x_n) \subseteq Q$.

Ings.: $Q = K(x_1, \dots, x_n)$. $\square$

Bsp.: $\mathbb{Q}[\sqrt{2}] = \left\{ \sum_{i=0}^n a_i (\sqrt{2})^i; n \in \mathbb{N}_0, a_i \in \mathbb{Q} \right\} = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$

$$(\sqrt{2})^2 = 2 \in \mathbb{Q}, (\sqrt{2})^3 = 2\sqrt{2} \in \sqrt{2} \cdot \mathbb{Q}$$

$$(\sqrt{2})^4 \in \mathbb{Q}, (\sqrt{2})^5 \in \sqrt{2} \cdot \mathbb{Q} \dots$$

$$\mathbb{Q}(\sqrt{2}) = \underset{18.10}{\text{Quot}} \mathbb{Q}[\sqrt{2}] = \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}}; a, b, c, d \in \mathbb{Q}, c+d\sqrt{2} \neq 0 \right\}$$

$$\text{Wegen } \frac{1}{c+d\sqrt{2}} = \frac{c-d\sqrt{2}}{(c+d\sqrt{2})(c-d\sqrt{2})} = \frac{c-d\sqrt{2}}{c^2-d^2} = \underbrace{\left(\frac{c}{c^2-d^2}\right)}_{a'} + \underbrace{\left(\frac{-d}{c^2-d^2}\right)}_{b'} \sqrt{2}$$

$$\text{folgt } \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{2}].$$

$\nearrow \mathbb{Q}(\sqrt{2})$ ist einfach über $\mathbb{Q}$

18.11. Def.: $L|K$ einfache Erw. von $K : (\Leftrightarrow) \exists x \in L : L = K(x)$

Dann: x primitives El. für $L|K$

$\nearrow$ Kurz: x a.g. | K

18.12. Def.: $L|K$. Dann heißt $x \in L$ algebraisch über K : $(\Leftrightarrow)$

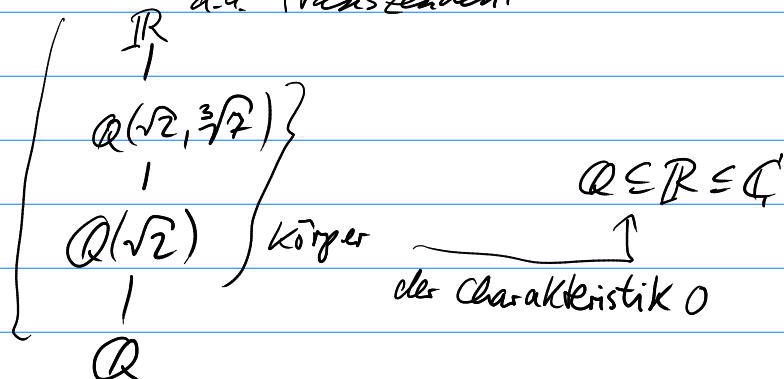
$$\exists f \in K[T] : (f \neq 0 \wedge f(x) = 0)$$

Dann: x Wurzel von f (bzw. Nullstelle von f)

Bsp. $\sqrt{2}$ ist Wurzel von $T^2 - 2$, also: $\sqrt{2}$ ist alg. über $\mathbb{Q}$

18.13. Bsp: $\mathbb{R} \mid \mathbb{Q}$. $\mathbb{R} \ni x = \sqrt[5]{7}$ ist alg. $\mid \mathbb{Q}$, da Wurzel von $T^5 - 7 \in \mathbb{Q}[T]$
 "Kurz: $\sqrt[5]{7}$ ist algebraisch ($\mid \mathbb{Q}$)"

$\pi \in \mathbb{R}$ ist nicht algebraisch über $\mathbb{Q}$ [Lindemann, Jahr 1882]
 d.h. transzendent



18.14. Bsp: Jedes $x \in \mathbb{R}$ ist alg. $\mid \mathbb{R}$, da Wurzel von $T - x \in \mathbb{R}[T]$.
 " K " K " K "

18.15. Satz: Das normierte $f \in K[T]$ (d.h. $\neq 0$, höchst. Koeff. = 1)
 von minimalem Grad mit $f(x) = 0$ ist änd. best. und irreduzibel.

Bew.: Eind.: $f_1 - f_2$ hat strikt kleineren Grad, $(f_1 - f_2)(x) = 0 \Rightarrow f_1 - f_2 = 0$.

Irred.: Sei $f = g \cdot h$ mit $g, h \in K[T]$. Dann $0 = f(x) = g(x) \cdot h(x)$,
 $\exists g(x) = 0$. Also: $\deg(g) = \deg(f) \Rightarrow h \in K^\times$ (da f normiert). $\square$

18.16. Def.: f (wie in 18.15) heißt Minimalpolynom von x über K ,
Grad von x über K := $\deg(f)$,
 Kurz: $f = \text{Mipo}_K(x)$, $\deg(x)$:= $\deg(f) = \deg \text{Mipo}_K(x)$.

18.17. Satz: Sei $L \mid K$, $x \in L$ alg. $\mid K$, $f \in K[T]$ das Mipo von $x \mid K$.

Dann: (i) $K(x) = K[x] \cong K[T] / (f)$ ↑ "über"
 vermöge $g(x) \mapsto g + (f)$

(ii) $[K(x) : K] = \deg(f) =: n$,
 und $1, x, x^2, \dots, x^{n-1}$ ist K -Basis von $K(x)$.

(iii) Ist $g \in K[T]$ irred., normiert mit $g(x) = 0 \Rightarrow g = f$.

-5-

$$T \xrightarrow{\varphi} X$$

Bew.: (i): $K[T] \xrightarrow{\varphi} K[X] \subseteq L$

$$\downarrow \quad \quad \quad \cong \quad \quad \quad \varphi : g + (f) \mapsto g(x)$$

$$K[T]/\ker \varphi$$

Es ist $\ker \varphi = (f)$, denn: $\ker \varphi = (g) \Rightarrow f = g \cdot h \Rightarrow h \in K^* \Rightarrow (g) = (f)$.

Da f irred., ist (f) maximales Ideal.

«Sonst: $(f) \subsetneq (g) \subsetneq K[T] \Rightarrow f = g \cdot h \nmid$
 $\Rightarrow K[X] \cong K[T]/(f)$ ist Körper, also $K(X) = K[X]$.
 «Kor.: $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ »

(ii): $[K(X):K] = [K[T]/(f):K] = \deg(f) = n$
 und $1, x, x^2, \dots, x^{n-1}$ K -Basis von $K(X)$ nach A14.12.

(iii): $g(x) = 0 \Rightarrow (g) \subseteq (f) \rightarrow$
 g irred. $\Rightarrow (g) = (f) \Rightarrow f = g \cdot h, h \in K^* \rightarrow$ $\square$

18.18. Bsp.: Sei $m \in \mathbb{Z}$ kein Quadrat, $x := \sqrt{m} \notin \mathbb{Q}$
 Nun $T^2 - m \in \mathbb{Q}[T]$ irred. «Eisensteinpl_m»
 $\Rightarrow T^2 - m$ ist Mipo von x | $\mathbb{Q}$
 somit: $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2, \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m}; a, b \in \mathbb{Q}\}$
 Körper

18.19. Bsp.: Sei p prim, $k \geq 1, x := \sqrt[k]{p} \in \mathbb{R}, \mathbb{Q}(x) | \mathbb{Q}$.
 Dann $T^k - p$ irred. «Eisenstein», also Mipo von x | $\mathbb{Q}$.
 somit: $[\mathbb{Q}(x) : \mathbb{Q}] = k, \mathbb{Q}(x) = \{a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1}; a_i \in \mathbb{Q}\}$

18.20. Lemma: Sei $L | K$. Für $x \in L$ sind äquiv.: (i) x alg. | K , (ii) $K(x) | K$ endl.
 Bew.: (i) $\Rightarrow$ (ii) nach 18.17, da $[K(x) : K] = \text{Grad von } x | K$.
 (ii) $\Rightarrow$ (i): Sei $n := [K(x) : K]$. Dann sind $1, x, \dots, x^n$ K -lin. abh.,
 d.h. $\exists a_0, \dots, a_n \in K$, nicht alle $a_i = 0$: $a_0 + a_1 x + \dots + a_n x^n = 0 \Rightarrow x$ Wurzel von $\sum a_i T^i = 0$.

18.21. Def: $L | K$ heißt alg.: $\Leftrightarrow \forall x \in L : x$ alg. | K . $\square$