17. Der algebraische Abschluss

Def. Ein Körper K ist <u>algebraisch abgeschlossen</u>, wenn jedes nicht-konst. Polynom $f \in K[X]$ eine Nullstelle in K besitzt.

Bsp. $\mathbb{C}$ ist alg. abg.; endl. Körper sind nie alg. abg.; $\mathbb{Q}$ nicht alg. abg.

Lemma 17.1 Die folgenden Aussagen sind äquivalent:

(a) K ist alg. abgeschlossen.

(b) Jedes nicht-konst. Polynom $f \in K[X]$ zerfällt über K in Linearfaktoren.

(c) Jedes irred. Polynom $f \in K[X]$ hat Grad 1.

(d) Ist $L : K$ eine alg. Erweiterung, so ist $L = K$.

Beweis: (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) ist klar.

(c) $\Rightarrow$ (d): Sei $L : K$ alg., $a \in L$ (also a alg. über K), und sei $f \in K[X]$ das Min.-Polynom von a über K. Mit (c) gilt $\operatorname{grad}(f) = 1$, d.h. $f = (X - b)$ mit $b \in K$, und weil $f(a) = 0$ gilt $a = b$, also $a \in K$. Weil a beliebig war gilt somit $L = K$.

(d) $\Rightarrow$ (a) Sei $f \in K[X]$ mit $\operatorname{grad}(f) \geq 1$. Dann ex. mit Satz 14.6 eine einfache Erweiterung $K(a)$ von K mit $f(a) = 0$. Mit (d) ist $K(a) = K$, d.h. $a \in K$ und f besitzt eine Nullstelle in K.

⊣

Proposition 17.2 Ist $L : K$ alg. und zerfällt jedes Polynom $f \in K[X]$ über L in Linearfaktoren, so ist L alg. abg.; d.h. auch jedes Polynom $\tilde{f} \in L[X]$ zerfällt über L in Linearfaktoren.

Beweis: Sei $f \in L[X]$ irred. über L und sei a eine Nullstelle von f in einem Zerfällungskörper von f. Dann ist a alg. über L und somit auch über K ($L:K$ ist alg.). Sei $g \in K[X]$ das Min.-Poly. von a über K. Nach dem Euklidischen Alg. ex. Polynome $q, r \in L[X]$ mit $g = q \cdot f + r$ und $\text{grad}(r) < \text{grad}(f)$ oder $r = 0$. An a ausgewertet sehen wir, dass $r(a) = 0$ (weil $f(a) = 0$), woraus folgt $f \mid g$. Weil nach Voraussetzung $g \in K[X]$ über L in Linearfaktoren zerfällt, zerfällt auch das irred. Polynom $f \in L[X]$ in Linearfaktoren, d.h. $\text{grad}(f) = 1$ und L ist mit (c) alg. abg. ⊣

Def. Sei K ein Körper. Ein Erweiterungskörper L von K heißt <u>algebraischer Abschluss</u> von K, wenn $L:K$ alg. ist und jedes Polynom $f \in K[X]$ über L in Linearfaktoren zerfällt.

Bem. Ist L ein alg. von K, so enthält L alle Zerfällungskörper von Polynomen $f \in K[X]$.

Bsp. $\mathbb{C}$ ist ein alg. Abschluss von $\mathbb{R}$, aber nicht von $\mathbb{Q}$.

Satz 17.3 Jeder Körper K besitzt einen alg. Abschluss; dieser ist bis auf Isomorphie eindeutig.

Wir beweisen diesen Satz mit Primidealtheorem (PIT) welches aus dem Auswahlaxiom (AC) folgt, aber schwächer ist als AC.

Der Beweis ist wie folgt aufgebaut:

0. Formulierung von PIT, Ultrafiltertheorem (UFT), PIT für Ringe (PITR),
1. UFT $\Leftrightarrow$ PITR (damit auch PIT $\Leftrightarrow$ PITR) und PIT $\Leftrightarrow$ UFT
2. PITR $\Rightarrow$ jeder Körper besitzt einen alg. Abschluss
3. PITR $\Rightarrow$ der alg. Abschluss ist bis auf Isomorphie eindeutig

Beweis von Satz 17.3

0. Definitionen Sei S eine nicht-leere Menge.

- $\mathcal{F} \subseteq \mathcal{P}(S)$ ist ein Filter falls gilt:
  - $S \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$
  - $x \in \mathcal{F} \wedge y \in \mathcal{F} \Rightarrow x \cap y \in \mathcal{F}$
  - $x \in \mathcal{F} \vee y \in \mathcal{F} \Rightarrow x \cup y \in \mathcal{F}$
- $\mathcal{I} \subseteq \mathcal{P}(S)$ ist ein Ideal falls gilt: $\{x^c : x \in \mathcal{I}\}$ ist ein Filter, wobei $x^c := S \setminus x$.
- Für $x, y \subseteq S$ sei $x + y := (x \setminus y) \cup (y \setminus x)$ und $x \cdot y := x \cap y$. Dann ist $\mathcal{R} = (\mathcal{P}(S), 0_{\mathcal{R}}, 1_{\mathcal{R}}, +, \cdot)$ mit $0_{\mathcal{R}} := \emptyset$ und $1_{\mathcal{R}} := S$ ein kommutativer Ring (und Ideale $\mathcal{I} \subseteq \mathcal{P}(S)$ sind Ideale in $\mathcal{R}$).
- $\mathcal{U} \subseteq \mathcal{P}(S)$ ist ein Ultrafilter falls $\mathcal{U}$ ein Filter ist und für alle $x \subseteq S$ gilt $x \in \mathcal{U} \vee x^c \in \mathcal{U}$ ($\mathcal{U}$ ist ein max. Filter).
- $\mathcal{I} \subseteq \mathcal{P}(S)$ ist ein Primideal (im Ring $\mathcal{R}$) falls $\{x^c : x \in \mathcal{I}\}$ ein Ultrafilter ist. [siehe Serie 11, Aufgabe 60]
- Primidealtheorem (PIT): Jedes Ideal $\mathcal{I} \subseteq \mathcal{P}(S)$ lässt sich zu einem Primideal erweitern.
- Ultrafiltertheorem (UFT): Jeder Filter $\mathcal{F} \subseteq \mathcal{P}(S)$ lässt sich zu einem Ultrafilter erweitern.
- Primidealtheorem für Ringe (PITR): Jedes echte Ideal in einem Ring lässt sich zu einem Primideal erweitern.

Erste Implikationen:

- PIT $\Leftrightarrow$ UFT (folgt direkt aus den Definitionen)
- AC $\Rightarrow$ UFT (kann mit dem Teichmüller-Prinzip TP gezeigt werden, wobei TP $\Leftrightarrow$ AC) [siehe Grundstrukturen 2024, Serie 6, Aufg. 23]

Es gilt UFT $\not\Rightarrow$ AC: Es gibt Modelle $V \models ZF$ mit $V \models$ UFT aber $V \not\models$ AC.

1. LFT $\Leftrightarrow$ PITR

($\Leftarrow$) Weil $\mathcal{R} = (\mathcal{P}(S), 0_{\mathcal{R}}, 1_{\mathcal{R}}, +, \cdot)$ ein Ring ist haben wir

PITR $\Rightarrow$ PIT und mit PIT $\Leftrightarrow$ LFT gilt PITR $\Rightarrow$ LFT

($\Rightarrow$) • Sei $R=(R,0,1,+,\cdot)$ ein komm. Ring und $I \subsetneq R$ ein echtes Ideal in R.

• Sei $\mathcal{B}$ eine Menge von partiellen Funktionen g von R nach $\{0,1\}$ wobei $\mathrm{dom}(g)$ eine endl. Teilmenge von R ist.

Wir sagen $\mathcal{B}$ ist eine "binary mess" auf R falls gilt:

- Für jede endl. Teilmenge $E \subseteq R$, d.h. $E \in \mathrm{fin}(R)$, ex. eine Funktion $g \in \mathcal{B}$ mit $\mathrm{dom}(g) = E$.
- Für jedes $g \in \mathcal{B}$ und jede endl. Teilmenge $E \subseteq R$ ist $g|_E \in \mathcal{B}$.

Ist $f: R \to \{0,1\}$ eine Funktion und $\mathcal{B}$ eine binary mess auf R, so ist f <u>konsistent mit $\mathcal{B}$</u> falls für jedes $E \in \mathrm{fin}(R)$ gilt: $f|_E \in \mathcal{B}$.

<u>zum Beweis:</u> Auf R (mit $I \subsetneq R$) definieren wir zuerst eine binary mess $\mathcal{B}$ und zeigen dann mit LFT, dass es eine Funktion $f: R \to \{0,1\}$ gibt die konsistent ist mit $\mathcal{B}$ und dass $\underbrace{f^{-1}(0)}_{=\{s \in R : f(s)=0\}} \subseteq R$ ein Primideal in R ist welches I enthält.

• Sei $\mathcal{B}$ die Menge aller partieller Funktionen $g: R \to 2$ mit $\mathrm{dom}(g) \in \mathrm{fin}(R)$ für die gilt:

(1) $a \in I \cap \mathrm{dom}(g) \Rightarrow g(a) = 0$

(2) $a, b, a-b \in \mathrm{dom}(g) \wedge g(a) = g(b) = 0 \Rightarrow g(a-b) = 0$

(3) Für $s \in R$ und $a, s \cdot a \in \mathrm{dom}(g)$ gilt: $g(a) = 0 \Rightarrow g(s \cdot a) = 0$

(4) $1 \in \mathrm{dom}(g) \Rightarrow g(1) = 1$

(5) $a, b, a \cdot b \in \mathrm{dom}(g) \wedge g(a) = g(b) = 1 \Rightarrow g(a \cdot b) = 1$

Dann ist $\mathcal{B}$ eine binary mess:

- Sei $E \subseteq fun(R)$. Wir zeigen, dass $\{g \in \mathcal{B} : dom(g) = E\} \neq \emptyset$ wie folgt:
  - Ist $E \cap I = \emptyset$, so sei $g_1(x) = 1$ für alle $x \in E$.
  - Ist $1 \notin E$, so sei $g_0(x) = 0$ für alle $x \in E$.

  Dann erfüllen g_1, g_0 die Bed. (1)-(5) und $g_1, g_0 \in \mathcal{B}$ mit $dom(g_1) = dom(g_0) = E$.

  Sei $E = \{a_1, \dots, a_k, 1, x_1, \dots, x_n\}$ mit $a_i \in I$ und $x_j \in R \setminus (I \cup \{1\})$, $k \geq 1$, $n \geq 0$

  und sei X die Familie aller Teilmengen $X \subseteq \{x_1, \dots, x_n\}$ für die ein Ideal $\mathfrak{J} \subseteq R$ ex. mit

  $$\{a_1, \dots, a_k\} \cup X \subseteq \mathfrak{J} \subsetneq R.$$

  Dann ist X endl. und nicht leer ($\emptyset \in X$ weil I Ideal in R).

  Somit gibt es (mind.) ein $X_E \in X$ mit max. Kardinalität und ein Ideal $\mathfrak{J}_E \subsetneq R$ mit $\{a_1, \dots, a_k\} \cup X_E \subseteq \mathfrak{J}_E \subsetneq R$; sei $X_E = \{x_1, \dots, x_r\}$.

  [Hier brauchen wir AC nicht, denn wir müssen nur zeigen, dass $\{g \in \mathcal{B} : dom(g) = E\} \neq \emptyset$.]

  Wir definieren nun $g : E \to 2$ durch

  $$g(a) := \begin{cases} 0 & \text{falls } a \in \mathfrak{J}_E \cap E = \{a_1, \dots, a_k, x_1, \dots, x_r\}, \\ 1 & \text{falls } a \in E \setminus \mathfrak{J}_E = \{1, x_{r+1}, \dots, x_n\}. \end{cases}$$

  Dann erfüllt g die Bed. (1)-(5):
  - (1) & (4) folgt aus Def.
  - (2): $a, b, a-b \in E \wedge g(a) = g(b) = 0$, so gilt $a, b \in \mathfrak{J}_E$. Damit ist auch $a - b \in \mathfrak{J}_E$, insbes. $a - b \in \mathfrak{J}_E \cap E$, also $g(a-b) = 0$.
  - (3) $s \in R$; $a, s \cdot a \in E$, und $g(a) = 0$, dann ist $a \in \mathfrak{J}_E \cap E$, und somit auch $s \cdot a \in \mathfrak{J}_E \cap E$, d.h. $g(s \cdot a) = 0$.
  - (5) $x, y, x \cdot y \in E$ mit $g(x) = g(y) = 1$. Wäre $g(x \cdot y) = 0$, dann wäre $x \cdot y \in \mathfrak{J}_E$ mit $x, y \notin \mathfrak{J}_E$. Weil X_E max. war, muss

gelten $(\mathfrak{J}_E \cup \{x\}) = (\mathfrak{J}_E \cup \{y\}) = R$. D.h. es ex. $a, b \in \mathfrak{J}_E$ und $r, s \in R$, sodass $1 = a + r \cdot x = b + s \cdot y$. Damit ist

$$1 = 1 \cdot 1 = (a + r \cdot x) \cdot (b + s \cdot y) = \underbrace{a \cdot b}_{\in \mathfrak{J}_E} + \underbrace{asy}_{\in \mathfrak{J}_E} + \underbrace{brx}_{\in \mathfrak{J}_E} + \underbrace{rsxy}_{\in \mathfrak{J}_E \text{ (weil } g(x,y)=0)}$$

Somit ist $1 \in \mathfrak{J}_E$ und $\mathfrak{J}_E = R$ ↯ zu $\mathfrak{J}_E \subsetneq R$

- Wir haben nun für jedes $E \in fin(R)$ ein $g \in \mathcal{B}$ mit $dom(g) = E$ konstruiert, und weil sich die Eigenschaften (1) - (5) auf Teilmengen von $dom(g)$ vererben, ist $\mathcal{B}$ eine binary mess.

Wir konstruieren nun mit dem UFT eine zu $\mathcal{B}$ konsistente Funktion $f: R \to 2$:

- Sei $E \in fin(R)$ und sei $X_E := \{h \in {}^R2 : h|_E \in \mathcal{B}\}$.
  Sei weiter $\mathcal{F} := \{X \subseteq {}^R2 : \exists E_1, \dots, E_n \in fin(R)\,(\underbrace{X_{E_1} \cap \dots \cap X_{E_n}}_{= X_{E_1 \cup \dots \cup E_n}} \subseteq X)\}$.
  Dann ist $\mathcal{F}$ ein Filter über ${}^R2$ und mit dem UFT lässt sich $\mathcal{F} \subseteq \mathcal{P}({}^R2)$ zu einem Ultrafilter $\mathcal{U} \subseteq \mathcal{P}({}^R2)$ erweitern. Weil $\mathcal{U}$ ein Ultrafilter ist, gilt für jedes $x \in R$,
  entweder $\{h \in {}^R2 : h(x) = 0\} \in \mathcal{U}$ oder $\{h \in {}^R2 : h(x) = 1\} \in \mathcal{U}$,
  und wir definieren die Funktion $f: R \to 2$ sodass für alle $x \in R$ gilt: $X_{\{x\}} := \{h \in {}^R2 : h(x) = f(x)\} \in \mathcal{U}$
  Für jede endl. Menge $E = \{x_1, \dots, x_n\} \subseteq R$ gilt nun
  $\bigcap_{1 \le i \le n} X_{\{x_i\}} \in \mathcal{U}$, und somit ist $f|_E \in \mathcal{B}$,
  d.h. f ist konsistent mit $\mathcal{B}$.

Es bleibt zu zeigen, dass $p := f^{-1}(0)$ ein Primideal in R ist welches I erweitert.

- $p \subseteq R$ ist ein Ideal:
  Seien $a, b \in p$ und sei $E := \{a, b, a-b\}$. Weil $g = f|_E$ in $\mathcal{P}$ ist, folgt mit (2), $g(a) = g(b) = 0 \Rightarrow g(a-b) = 0$, d.h. $a-b \in p$. Ist $r \in R$ und $F := \{a, r \cdot a\}$, so folgt mit (3) analog $r \cdot a \in p$.
- p ist Primideal:
  Seien $a, b \in R$ mit $a \cdot b \in p$. Dann folgt aus (5), dass $a \in p$ oder $b \in p$.

$p \subseteq R$ ist also ein Primideal, welches I erweitert.

⊣ 1. Schritt

2. PITR $\Rightarrow$ jeder Körper besitzt einen alg. Abschluss

Sei K ein Körper. Für jedes normierte Polynom $u \in K[X]$ mit $\text{grad}(p) = m \geq 2$ seien $Z_u^{(1)}, \ldots, Z_u^{(m)}$ paarweise verschiedene Unbestimmte, versch. für jedes u; sei Z die Menge aller $Z_u^{(k)}$ für $u \in K[X]$, $\text{grad}(u) = m_u \geq 2$ und $1 \leq k \leq m_u$, und sei $K[Z]$ der Polynomring in den Unbestimmten $X_u^{(k)} \in Z$. Weiter sei $I \subseteq K[Z]$ das Ideal, welches für $u \in K[X]$ mit $u = a_0 + a_1 X + \ldots + a_{m-1} X^{m-1} + X^m$ von den Elementen

$$e_u^{(m-1)} := a_{m-1} + \sum_{i=1}^{m} Z_u^{(i)}, \quad e_u^{(m-2)} := a_{m-2} - \sum_{1 \leq i < j \leq m} Z_u^{(i)} \cdot Z_u^{(j)}, \ldots$$

$$\ldots, e_u^{(0)} := a_0 - (-1)^m \cdot (X_u^{(1)} \cdot \ldots \cdot X_u^{(m)})$$ erzeugt wird.

Bemerkung: Für alle normierten Polynome $u \in K[X]$ mit $\text{grad}(u) = m \geq 2$ gilt über $K[Z]/I$:

$$u = \prod_{i=1}^{m} (X - Z_u^{(i)})$$

[ausmultiplizieren und Gleichheiten in I benutzen]

Somit zerfällt jedes $u \in K[X]$ in $K[Z]/I$ in Linearfaktoren.

Beh. 1 I ist ein echtes Ideal in $K[Z]$.

Bew: Wir führen die Annahme $I = K[Z]$ zu einem Widerspruch.

- Ist $I = K[Z]$, so ist $1 \in I$ und wir finden endl. viele Erzeugende $e_{u_i}^{(k)}$ und endl. viele $\alpha_{i,k} \in K$ sodass
$$\sum_{i=1}^{N} \sum_{k=0}^{\deg(u_i)-1} \alpha_{i,k} \cdot e_{u_i}^{(k)} = 1 \quad (\text{für } N \in \mathbb{N}) \quad (*)$$
- Mit Kor. 15.1 ex. eine Körpererweiterung L von K in der jedes Polynom u_i (für $1 \leq i \leq N$) in Linearfaktoren zerfällt. Für jedes u_i mit $\operatorname{grad}(u_i) = m_i$ gilt:
$$u_i = \prod_{k=1}^{m_i - 1} (X - \xi_{u_i}^{(k)}) \quad \text{für } \xi_{u_i}^{(k)} \in L.$$
Durch ausmultiplizieren sehen wir, dass für jedes $e_{u_i}^{(k)} \in K[Z_{u_i}^{(1)}, \dots, Z_{u_i}^{(m_i)}]$ gilt $e_{u_i}^{(k)}(\xi_{u_i}^{(1)}, \dots, \xi_{u_i}^{(m_i)}) = 0$,
D.h. die Summe $(*)$ ist gleich 0.

Beh. 1

Mit PIT bzw. PITR können wir I zu einem Primideal $p \subseteq R$ erweitern. D.h. $K[Z]/p$ ist ein Integritätsring, der in seinen Quotientenkörper $Q := \operatorname{Quot}(K[Z]/p)$ eingebettet werden kann. Wir haben also: $K \hookrightarrow K[Z] \twoheadrightarrow K[Z]/p \hookrightarrow Q$.

Beh. 2 Jedes Polynom $u \in K[X]$ zerfällt über Q in Linearfaktoren.

Bew. u zerfällt über $K[Z]/I$ in Linearfaktoren, also auch über $K[Z]/p$ und somit auch über Q.

Beh. 2

Beh. 3 Die Körpererweiterung $Q : K$ ist algebraisch. [Übung]

Somit ist Q ein alg. Abschluss von K.

2. Schritt

wie im Beweis von PIT $\Rightarrow$ PITR, bzw. UFT $\Rightarrow$ PITR.

Für die Eindeutigkeit (bis auf Isom.) nehmen wir zwei alg. Abschlüsse L und L' von K und konstruieren mit UFT eine Funktion $f : L \to L'$ mit $f|_K = \mathrm{id}$, welche die Nullstellen von $u \in K[X]$ in L auf die Nullst. in L' abbildet.