Vorlesung aus dem Sommersemester 2011

Höhere Algebra

Priv.-Doz. Dr. Peter Schuster

geTEXt von Viktor Kleen & Florian Stecker

Inhaltsverzeichnis

3 Körper

3.2 Zerfällungskörper

Definition. Ein Körper k heißt *vollkommen* oder *perfekt*, wenn jedes nichtkonstante $f \in k[X] \setminus k$ separabel ist.

Bemerkung. Ein Körper k ist genau dann vollkommen, wenn für jedes $g \in k[X] \setminus k$ aus $g' = 0$ folgt, dass g reduzibel ist.

Bemerkung. Ist k algebraisch abgeschlossen oder $\mathrm{char}(k) = 0$, so ist k vollkommen.

Satz. *Für jeden Körper k mit $\mathrm{char}(k) = p > 0$ sind äquivalent:*

i) k ist vollkommen.
ii) Der Frobeniushomomorphismus $F_k \colon k \to k, x \mapsto x^p$ ist surjektiv.
iii) $\forall g \in k[X](g' = 0 \Rightarrow \exists h \in k[X].\ g = h^p)$

Beweis.

i $\Rightarrow$ ii Es sei $a \in k$ und $f = X^p - a \in k[X]$. Man nehme ein normiertes, irreduzibles $g \in k[X]$ mit $g \mid f$, sowie eine Körpererweiterung $K \supseteq k$ mit $g = \prod_{i=1}^{r}(X - b_i)$ in $K[X]$. Wegen $f(b_1) = \cdots = f(b_r) = 0$, d.h. $b_1^p = \cdots = b_r^p = a$, ist $b_1 = \cdots = b_r$, denn F_K ist injektiv. Da f separabel ist, gilt $r = 1$, d.h. $g = X - b_1$, also $b_1 \in k$.

ii $\Rightarrow$ iii Es sei $g \in k[X]$ mit $g' = 0$. Schreibe $g = \sum_{i=1}^{n} c_i X^i$, also $\sum_{i=1}^{n} i c_i X^{i-1} = 0$, d.h. $ic_i = 0$ für $1 \le i \le n$. Also ist $c_i = 0$ für alle i mit $p \nmid i$. Es folgt $g = \sum_{jp \le n} c_{jp} X^{jp}$ und mit $c_{jp} = d_{jp}^p$ nach Voraussetzung ist $g = \left(\sum_{jp \le n} d_{jp} X^j\right)^p$, mit $d_{jp} \in k$ für $jp \le n$.

iii $\Rightarrow$ i Mit Bemerkung. □

Korollar 1. *Jeder endliche Körper ist vollkommen.*

Korollar 2. *Jeder Primkörper ist vollkommen.*

Korollar 3. *Es sei k ein beliebiger Körper. Ein $f \in k[X] \setminus k$ ist schon dann separabel, wenn alle Koeffizienten von f im Primkörper k_0 von k liegen.*

Beweis. Nach Korollar 2 ist $f \in k_0[X]$ separabel, also nach einer früheren Bemerkung auch in jedem Oberkörper von k_0. □

Beispiel. Ist $\mathrm{char}(k) = p > 0$, so ist $K = k(t)$, d.h. $K = Q(R)$ mit $R = k[t]$, ein unvollkommener Körper, denn $f = X^p - t$ ist irreduzibel in $R[X]$ nach Eisenstein mit dem Primelement $t \in R$, also auch irreduzibel in $K[X]$. Ferner ist $f' = pX^{p-1} = 0$, also f inseparabel. Alternativ ist t in K keine p-te Potenz, denn $t = (\frac{u}{v})^p$ mit $u, v \in R \setminus \{0\}$ ist unmöglich: $tv^p = u^p$ impliziert $1 + p\deg(v) = p\deg(u)$, also $p \mid 1$.

Beispiel. $L = \bigcup_{n \ge 0} \mathbb{F}_{p^{2^n}}$ ist unendlich und vollkommen mit $\mathrm{char}(L) = p$. $[\mathbb{F}_p \to \mathbb{F}_{p^2} \to \cdots \to L]$

3.3 Einheitswurzeln

Erinnerung. Für $n \geq 1$ ist $\varphi(n)$ gleich

i) der Anzahl der Erzeugenden von $\mathbb{Z}/\langle n\rangle$.
ii) Der Ordnung von $(\mathbb{Z}/(n))^\times$.
iii) der Anzahl der zu n teilerfremden $m \in \{1, \dots, n\}$.

Insbesondere gilt für jede Primzahl p und $k \geq 1$:

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

Bemerkung. Es gilt $\sum_{d|n} \varphi(d) = n$ für $n \geq 1$.

Beweis. Es sei $G = \mathbb{Z}/\langle n\rangle$, $P_d = \{x \in G\colon x^d = e\}$ und $Q_d = \{x \in G\colon \operatorname{ord}(x) = d\}$. Wegen $G = P_n = \bigcup_{d|n} Q_d$ ist $n = |G| = \sum_{d|n} |Q_d|$. Für die einzige Untergruppe H_d von G der Ordnung d ist $Q_d = \{x \in H_d\colon \langle x\rangle = H_d\}$, also $|Q_d| = \varphi(d)$. □

Hieraus folgt übrigens wieder $\varphi(p^k) = p^k - p^{k-1}$, denn

$$p^k = \sum_{l=0}^{k-1} \varphi(p^l) + \varphi(k) = p^{k-1} + \varphi(p^k).$$

Bemerkung. Es seien $m, n \geq 1$ teilerfremd. Dann ist $(mn) = (m) \cap (n)$, da $d = 1$ ein ggT von m, n ist, ist $v = mn$ ein kgV von m, n, denn allgemein gilt $dv = mn$. Der Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}/(m) \times \mathbb{Z}/(n), z \mapsto (z + (m), z + (n))$ hat Kern $(m) \cap (n)$, induziert also einen injektiven Ringhomomorphismus $\mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$, der sogar bijektiv ist, also einen Gruppenisomorphismus $(\mathbb{Z}/(mn))^\times \to (\mathbb{Z}/(m))^\times \times (\mathbb{Z}/(n))^\times$ induziert, woraus $\varphi(mn) = \varphi(m)\varphi(n)$ folgt. Es folgt also

$$\frac{\varphi(n)}{n} = \prod_{\substack{p|n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right).$$

Definition. Es sei k ein Körper und $n \geq 1$. Man nennt

— den Zerfällungskörper k_n von $f = X^n - 1$ über k den n-ten *Kreisteilungskörper* von k und
— die Untergruppe $E_n(k) = \{a \in k_n\colon a^n = 1\}$ von $k_n^\times$ die Gruppe der n-ten *Einheitswurzeln*.

Beispiel. Zum Beispiel ist $E_n(\mathbb{Q}) = \left\{e^{\frac{2\pi i}{n}k}\colon 1 \leq k \leq n\right\}$. Als endliche Untergruppe von $k_n^\times$ ist $E_n(k)$ zyklisch. Im Fall $\operatorname{char}(k) \mid n$, d.h. $\operatorname{char}(k) = p > 0$, $n = p^l m$ mit $p \nmid m$, ist $f = (X^m - 1)^{p^l}$, also $k_n = k_m$ und $E_n(k) = E_m(k)$. Von nun an nehmen wir also an, dass $\operatorname{char}(k) \nmid n$ ist, was $\operatorname{char}(k) = 0$ einschließt. Insbesondere sind $f = X^n - 1$ und $f' = nX^{n-1}$ teilerfremd. Es folgt, dass f separabel, also k_n galoissch über k ist, und $|E_n(k)| = |\{a \in k_n\colon f(a) = 0\}| = \deg(f) = n$.

Definition. Ein Erzeuger von $E_n(k)$ heißt *primitive Einheitswurzel* von k. Die Menge $P_n(k)$ der primitiven n-ten Einheitswurzeln von k hat $\varphi(n)$ Elemente.

Beispiel. Zum Beispiel ist $e^{\frac{2\pi i}{n}} \in P_n(\mathbb{Q})$, $P_1(k) = E_1(k) = \{1\}$, $P_n(k) = E_n(k) \setminus \{1\}$ für Primzahlen n und $P_4(\mathbb{Q}) = \{\pm i\}$.

Für jedes $\xi \in P_n(k)$ ist $\mathbb{Z}/(n) \to E_n(k), \overline{z} \mapsto \xi^z$ ein Gruppenisomorphismus, speziell ist $P_n(k) = \{\xi^z \colon 1 \leq z \leq n \text{ mit } z, n \text{ teilerfremd}\}$. Ferner ist $k_n = k(\xi)$ und für jedes $\sigma \in \mathrm{Gal}(k_n/k)$ ist $\sigma(\xi) \in P_n(k)$, also $\sigma(\xi) = \xi^z$ mit $1 \leq z \leq n$ und z, n teilerfremd; ist auch $\sigma(\xi) = \xi^{z'}$, so ist $\xi^{z-z'} = 1$, d.h. $z - z' \in (n)$, womit $\omega \colon \mathrm{Gal}(k_n/k) \to (\mathbb{Z}/(n))^\times, \sigma \mapsto \overline{z}$ mit $\sigma(\xi) = \xi^z$ wohldefiniert ist. ω ist sogar ein Gruppenmonomorphismus, speziell ist $[k_n \colon k] \mid \varphi(n)$.

Definition. Man nennt

$$\Phi_n(k) = \prod_{\xi \in P_n(k)} (X - \xi)$$

das n-te *Kreisteilungspolynom* von k. Es ist normiert und hat Grad $\varphi(n)$.

Beispiel.

1) $\Phi_1(k) = X - 1$, da $P_1(k) = \{1\} = E_1(k)$.

2) $\Phi_2(k) = X + 1$, da $P_2(k) = \{-1\}$.

3) Für jedes $\xi \in P_3(k)$ ist $P_3(k) = \{\xi, \xi^2\}$ und $\xi + \xi^2 = -1$ $[(\xi - 1)(\xi^2 + \xi + 1) = 0$ und $\xi \neq 1]$, also $\Psi_3(k) = (X - \xi)(X - \xi^2) = X^2 - (\xi + \xi^2)X + 1 = X^2 + X + 1$.

4) Für jedes $\xi \in P_4(k)$ ist $P_4(k) = \{\xi, \xi^3\}$ und $\xi^2 = -1$, also $\Phi_4(k) = (X - \xi)(X - \xi^3) = X^2 - (\xi + \xi^3)X + 1 = X^2 + 1$.

Bemerkung. Für $n \geq 1$ ist $X^n - 1 = \prod_{d \mid n} \Phi_d(k)$.

Beweis. Wegen $\{a \in E_n(k) \colon \mathrm{ord}(a) = d\} = P_d(k)$ ist $E_n(k) = \bigcup_{d \mid n} P_d(k)$ (disjunkt), also

$$X^n - 1 = \prod_{a \in E_n(k)} (X - a) = \prod_{d \mid n} \prod_{\xi \in P_d(k)} (X - \xi) = \prod_{d \mid n} \Phi_d(k) \qquad \square$$

Folgerung. Für jede Primzahl p ist $\Phi_p(k) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

Beweis. $\Phi_1(k) \cdot \Phi_p(k) = X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$. $\square$

Beispiel.

5) Aus

$$X^6 - 1 = \underbrace{\underbrace{\Phi_1(k)}_{(X-1)} \underbrace{\Phi_2(k)}_{(X+1)} \underbrace{\Phi_3(k)}_{(X^2+X+1)}}_{X^4+X^3-X-1} \Phi_6(k)$$

folgt $\Phi_6(k) = X^2 - X + 1$.

6) Aus $X^8-1=(X-1)(X+1)(X^2+1)\Phi_8(k)=(X^4-1)\Phi_8(k)$ folgt $\Phi_8(k)=X^4+1$.

Lemma. *Es seien $R\subseteq A$ Integritätsringe. Gibt es zu $h\in A[X]$ ein normiertes $f\in R[X]$ mit $fh\in R[X]$, so ist $h\in R[X]$.*

Beweis. In $R[X]$ hat man $fh=fq+r$ mit $\deg(r)<\deg(f)$, also $f(h-q)=r$ und damit $r=0$, d.h. $fh=fq$, also $h=q$ und damit $h\in R[X]$. □

Folgerung. Für $n\geq 1$ ist $\Phi_n(k)\in R[X]$ mit $R=\{m\cdot 1_k\colon m\in\mathbb{Z}\}$ der Primring von k.

Beweis. Induktion über n mit Lemma: $R[X]\ni X^n-1=\underbrace{\prod_{\substack{d\mid n\\ d<n}}\Phi_d(k)}_{f}\cdot\underbrace{\Phi_n(k)}_{h}$, $A=k_n$. □

Von nun an schreiben wir Φ_n anstelle von $\Phi_n(\mathbb{Q})$. Nach Folgerung ist $\Phi_n\in\mathbb{Z}[X]$, weshalb wir Φ_n auch als Element $\dot{\Phi}_n$ von $k[X]$ auffassen können, worin k ein beliebiger Körper mit $\mathrm{char}(k)\nmid n$ wie oben. Auch: $P_n\equiv P_n(\mathbb{Q})$.

Bemerkung. Für $n\geq 1$ ist $\dot{\Phi}_n=\Phi_n(k)$.

Beweis. Induktion über n: $\prod_{\substack{d\mid n\\ d<n}}\dot{\Phi}_d\cdot\dot{\Phi}_n=X^n-1=\prod_{\substack{d\mid n\\ d<n}}\Phi_d(k)\cdot\Phi_n(k)$. □

Satz (Dedekind)**.** *Für $n\geq 1$ ist $\Phi_n\in\mathbb{Z}[X]$ irreduzibel.*

Beweis. Man nehme $f\in\mathbb{Z}[X]$ irreduzibel und normiert mit $f\mid\Phi_n$. Wir werden zeigen, dass $f=\Phi_n$. Dazu wähle $\xi\in P_n$ mit $f(\xi)=0$, wovon f das Minimalpolynom über $\mathbb{Q}$ ist, und $g\in\mathbb{Z}[X]$ mit $fg=X^n-1$. Für $\ell\geq 1$ ist $\xi^\ell\in E_n(\mathbb{Q})$, d.h. $(\xi^\ell)^n-1=0$, also $f(\xi^\ell)=0$ oder $g(\xi^\ell)=0$. Behauptung: $f(\xi^m)=0$, falls m,n teilerfremd sind. Beweis dazu: zunächst im Fall $m=p$ Primzahl, also $p\nmid n$. Wäre $g(\xi^p)=0$, d.h. $h(\xi)=0$ für $h=g(X^p)\in\mathbb{Z}[X]$, so folgte $f\mid h$ in $\mathbb{Q}[X]$, sogar $fh_1=h$ in $\mathbb{Z}[X]$ nach Lemma, also $\overline{f}\,\overline{h_1}=\overline{h}=\overline{g}^p$ (!) in $\mathbb{F}_p[X]$ (Frobeniushomomorphismus, kleiner Satz von Fermat). Für einen irreduziblen Teiler u von $\overline{f}$ in $\mathbb{F}_p[X]$ wäre also $u\mid\overline{h}$, d.h. $u\mid\overline{g}$, also $u^2\mid\overline{f}\,\overline{g}=X^n-1$, was unmöglich ist, da X^n-1 wegen $p\nmid n$ in $\mathbb{F}_p[X]$ separabel. Noch zu (!): Mit $g=\sum_{i=0}^r c_iX^i$ ist $h=\sum c_iX^{pi}$, also $\overline{h}=\sum\overline{c_i}^pX^{pi}=(\sum\overline{c_i}X^i)^p=\overline{g}^p$. Im allgemeinen Fall schreibe $m=p_1\cdots p_t$ mit Primzahlen p_i. Wegen m,n teilerfremd gilt $p_i\nmid n$ für alle i. Es folgt $f(\xi^{p_1})=0$, also $f(\xi^{p_1p_2})=0$ usw. bis $f(\xi^m)=0$. Nach dieser Behauptung sind alle Elemente von P_n Nullstellen von f, weshalb $\deg(f)\geq|P_n|=\varphi(n)=\deg(\Phi_n)$, also $f=\Phi_n$. □

Korollar 1. *Für jedes $\xi\in P_n(\mathbb{Q})$ ist Φ_n das Minimalpolynom von ξ über $\mathbb{Q}$.*

Korollar 2. $[\mathbb{Q}_n:\mathbb{Q}]=\varphi(n)$, *sogar* $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})\cong(\mathbb{Z}/(n))^\times$.

Beweis. Für jedes $\xi\in P_n(\mathbb{Q})$ ist $\mathbb{Q}_n=\mathbb{Q}(\xi)$ galoissch über $\mathbb{Q}$ von Grad $\deg(\Phi_n)=\varphi(n)$. Insbesondere ist der Gruppenmonomorphismus $w\colon\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})\to(\mathbb{Z}/(n))^\times$ sogar ein Isomorphismus. □

Beispiel. Φ_n kann über $k \neq \mathbb{Q}$ reduzibel sein:

$$\begin{aligned}\Phi_{12} = X^4 - X^2 + 1 &= (X^2 + \sqrt{3}X + 1)(X^2 - \sqrt{3}X + 1) \quad \text{über } \mathbb{Q}(\sqrt{3}) \\ &= (X^2 + 5X + 1)(X^2 - 5X + 1) \quad \text{über } \mathbb{F}_{11} \\ &= (X-2)(X-6)(X-7)(X-11) \quad \text{über } \mathbb{F}_{13}\end{aligned}$$

Nun sei k wieder ein beliebiger Körper mit $ch(k) \nmid n$.

Bemerkung. Jeder irreduzible Teiler von $\Phi_n(k)$ in $k[X]$ hat Grad $[k_n : k]$.

Beweis. Ist f ein solcher, noch dazu normiert, so ist $f(\xi) = 0$ für ein $\xi \in P_n(k)$, wovon f das Minimalpolynom über k ist, also $\deg(f) = [k(\xi) : k] = [k_n : k]$ wie gewünscht. □

Folgerung. Es sind äquivalent:

i) $\Phi_n(k) \in k[X]$ ist irreduzibel.
ii) $[k_n : k] = \varphi(n)$.
iii) $\mathrm{Gal}(k_n/k) \cong (\mathbb{Z}/(n))^\times$

Beispiel (von Kreisteilungskörpern in char $= p$)**.** Für $k = \mathbb{F}_p$ und $m \geq 1$ ist $\mathbb{F}_{p^m}$ der Zerfällungskörper von $X^{p^m} - X$, d.h. derjenige von $X \cdot (X^n - 1)$ mit $n = p^m - 1$, also $\mathbb{F}_{p^m} = k_n$.

Definition. Eine Galoiserweiterung K/k heißt *zyklisch / abelsch / ...*, wenn $\mathrm{Gal}(K/k)$ eine zyklische / abelsche / ... Gruppe ist.

Bemerkung. Für jeden Zwischenkörper L von K/k gilt: K/k zyklisch/abelsch $\Longrightarrow K/L$ und L/k zyklisch/abelsch.

Beweis. Hauptsatz der Galoistheorie: $G = \mathrm{Gal}(K/k)$ abelsch (sogar zyklisch) $\Longrightarrow H := \mathrm{Gal}(L/k) \lhd G$ und H, G/H abelsch (sogar zyklisch). □

Beispiel.

1) Ist k endlich und K/k eine endliche Körpererweiterung so ist K/k zyklisch. [K ist galoissch über dem Primkörper k_0, also auch über k und $\mathrm{Gal}(K/k) = \langle F^\ell \rangle$ mit $|k| = p^\ell$, d.h. $k = \mathbb{F}_{p^\ell}$, wobei $F\colon K \to K, x \mapsto x^p$, $\mathrm{char}(k) = p$.]

2) Für $\mathrm{char}(k) \nmid n$ ist k_n/k abelsch. [$\mathrm{Gal}(k_n/k) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, für $\xi \in P_n(k)$: $\sigma \mapsto \overline{z}$ mit $\sigma(\xi) = \xi^z$.] Nach Bemerkung ist L/k abelsch für jeden Zwischenkörper L von k_n/k. Im Fall $k = \mathbb{Q}$ gilt sogar folgende Umkehrung: Zu jeder abelschen Erweiterung $K/\mathbb{Q}$ gibt es ein $n \geq 1$ mit $K \subseteq \mathbb{Q}_n$ (Satz von Kronecker-Weber).

3) Für $0 \neq \mathrm{char}(k) \nmid n$ ist k_n/k zyklisch. Für $k = \mathbb{Q}$ hingegen gilt: $\mathbb{Q}_n/\mathbb{Q}$ ist abelsch mit $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, aber $\mathbb{Q}_n/\mathbb{Q}$ ist nicht zyklisch für $n \in \{8, 12, 15, 16, 20, 21, \dots\}$ [Übung].

Definition. Sei K ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(K)$. Analog zur *Spur* $T\colon K \to K, x \mapsto \sum_{\sigma \in G} \sigma(x)$ von G in K nennt man $N\colon K \to K, x \to \prod_{\sigma \in G} \sigma(x)$ die *Norm* von G in K.

Bemerkung. Für $x, y \in K$ und $\rho \in G$ gilt:

a) $T(x+y) = T(x) + T(y)$, $T(\rho(x)) = T(x)$.
b) $N(x \cdot y) = N(x) \cdot N(y)$, $N(\rho(x)) = N(x)$.

Lemma (Hilberts Theorem 90)**.** *Für K, G wie oben gilt: Ist $G = \langle\sigma\rangle$ zyklisch, so gilt für jedes $a \in K$:*

1) $T(a) = 0 \iff \exists b \in K(a = b - \sigma(b))$
2) $N(a) = 1 \iff \exists b \in K^\times(a = b/\sigma(b))$

In 1) und 2) gilt „$\Leftarrow$“ auch ohne die Voraussetzung, dass G zyklisch ist.

Beweis. Jeweils nur „$\Rightarrow$“. O.B.d.A. $n := \mathrm{ord}(\sigma) > 1$.

1) Wegen $T(K) = \mathrm{Fix}_K(G)$ gibt es $c \in K$ mit $T(c) = 1$. Für $y_i = \sum_{j=0}^{i} \sigma^j(a)$ $(i \geq 0)$ ist $\sigma(y_i) = y_{i+1} - a$. Für $b = \sum_{i=0}^{n-1} y_i\sigma^i(c)$ folgt $\sigma(b) = \sum_{i=0}^{n-1}(y_{i+1} - a)\sigma^{i+1}(c)$, also
$$b - \sigma(b) = \underbrace{y_0}_{a}\underbrace{\sigma^0(c)}_{c} - y_n\underbrace{\sigma^n(c)}_{c} + a\underbrace{\sum_{i=0}^{n-1}\sigma^{i+1}(c)}_{T(\sigma(c))=T(c)=1} = a \text{ wegen } y_n = a + T(a) = a.$$

2) Mit $N(a) = 1$ ist $a \neq 0$. Für $y_i = \prod_{j=0}^{i}\sigma^j(a)$, speziell $y_0 = a$ folgt $\sum_{i=0}^{n-1} y_i\sigma^i \neq 0$ (Lemma von Dedekind). Deshalb gibt es ein $c \in K$ mit $b := \sum_{i=0}^{n-1} y_i\sigma^i(c) \neq 0$. Wegen $a\sigma(y_i) = y_{i+1}$ ist $a\sigma(b) = \sum_{i=0}^{n-1} y_{i+1}\sigma^{i+1}(c) = b - y_0\sigma^0(c) + y_n\sigma^n(c) = b - ac + ac = b$ wegen $y_n = a \cdot N(a) = a$, d.h. $a = b/\sigma(b)$. □

Definition. Es sei k ein Körper. Ein *reines Polynom* über k hat die Form $f = X^n - a$ mit $n \geq 1$, $a \in k$. Nun sei $\mathrm{char}(k) \nmid n$ und $a \neq 0$. Dann ist f separabel in $k[X]$, also der Zerfällungskörper K von f galoissch über k, und f hat n verschiedene Nullstellen in K, die n-ten *Wurzeln* $b_1, \ldots, b_n$ von a.

Es gilt $k_n \subseteq K$ mit $E_n(k) = \{b_1 b_i^{-1} : 1 \leq i \leq n\}$ und $\{b_1, \ldots, b_n\} = \{\xi b_{i_0} : \xi \in E_n(k)\}$ für irgendein $i_0 \in \{1, \ldots, n\}$, also $K = k_n(b_{i_0})$ für jedes $i_0 \in \{1, \ldots, n\}$. Neben k_n/k sind auch K/k und K/k_n galoissch als Zerfällungskörper des separablen Polynoms f über k bzw. k_n.

Bemerkung. Für jeden Körper k sind äquivalent:

i) $k \cap P_n(k) \neq \varnothing$
ii) $E_n(k) \subseteq k$
iii) $k = k_n$

Satz. *Sei k ein Körper, $n \geq 1$, $\mathrm{char}(k) \nmid n$ und k enthalte eine primitive n-te Einheitswurzel ξ.*

a) Ist $a \in k$ und K der Zerfällungskörper von $f = X^n - a$ über k, so ist K/k zyklisch mit $[K : k] \mid n$. Genau dann ist $[K : k] = n$, wenn f in $k[X]$ irreduzibel ist.
b) Ist K/k zyklisch mit $[K : k] = n$, so gibt es ein $b \in K$ mit $b^n \in k$ und $k(b) = K$. Für $a = b^n$ ist $f = X^n - a$ das Minimalpolynom von b über k und K der Zerfällungskörper von f über k.

Beweis.

a) O.B.d.A. sei $a \neq 0$. Nehme $b \in K$ mit $b^n = a$. Nun ist $\mathrm{Gal}(K/k) \to E_n(k), \sigma \mapsto \sigma(b)/b$ ein Gruppenhomomorphismus. [$k = k_n \Rightarrow \sigma(b)/b \in k \Rightarrow \pi(\sigma(b)/b) = \sigma(b)/b$, d.h. $\pi\sigma(b) = \pi(b)\sigma(b)/b \Rightarrow \pi\sigma(b)/b = (\pi(b)/b) \cdot (\sigma(b)/b)$ für $\pi, \sigma \in \mathrm{Gal}(K/k)$], der sogar injektiv ist [$k = k_n \Rightarrow K = k(b)$, also $\sigma(b)/b = 1 \Rightarrow \sigma(b) = b \Rightarrow \sigma = \mathrm{id}_K$]. Mit $E_n(k)$ zyklisch der Ordnung n folgt K/k zyklisch, $[K : k] \mid n$. Für das Minimalpolynom g von b über k gilt $[K : k] = \deg(g)$ und $g \mid f$, also $[K : k] = n \Leftrightarrow \deg(g) = n \Leftrightarrow g = f \Leftrightarrow f$ irreduzibel.

b) Es sei $G = \mathrm{Gal}(K/k)$. Nehme $\sigma \in G$ mit $G = \langle\sigma\rangle$. Wegen $N(\xi^{-1}) = (\xi^{-1})^n = 1$ gibt es nach Lemma (Hilbert 90) ein $b \in K^\times$ mit $\xi^{-1} = b/\sigma(b)$, d.h. $\sigma(b) = b\xi$. Aus $\sigma(b^n) = \sigma(b)^n = b^n\xi^n = b^n$ folgt $b^n \in \mathrm{Fix}_K(G) = k$, d.h. $f = X^n - a \in k[X]$ mit $a = b^n$ und $f(b) = 0$. Die Bahn $\{b, \sigma(b), \ldots, \sigma^{n-1}(b)\} = \{b, b\xi, \ldots, b\xi^{n-1}\}$ hat Länge n, also ist $[k(b) : k] = n$, speziell ist f das Minimalpolynom von b über k, und $K = k(b)$ ist der Zerfällungskörper von f über $k = k_n$. □

Beispiel. (dafür, dass $k = k_n$ unverzichtbar ist)

zu a: $k = \mathbb{Q}$, $n = 15$, $a = 1 \Rightarrow K = \mathbb{Q}_{15}$ ist nicht zyklisch über $\mathbb{Q}$ und $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(15) = 8 \nmid 15 = n$.

zu b: $k = \mathbb{F}_p$, $K = \mathbb{F}_{p^n} \Rightarrow K/k$ zyklisch, $[K : k] = n$. Ist zudem $n \geq 2$ mit n, $p^n - 1$ teilerfremd (z.B. $n = 2 = p$), so gibt es kein $b \in K$ mit $b^n \in k$ und $K = k(b)$, denn: Für ein solches $b \neq 0$ wäre bereits $b \in k$ [mit $1 = un + v(p^n - 1)$ wäre $b = \underbrace{(b^n)^u}_{\in k} \cdot \underbrace{(b^{p^n-1})^v}_{1} \in k$.]

Satz. *Es sei k ein Körper der Primzahlcharakteristik p.*

a) Ist $a \in k$ und K der Zerfällungskörper von $f = X^p - X - a$ über k, so gilt:
   i) Hat f eine Nullstelle in k, so ist $k = K$.
   ii) Hat f keine Nullstelle in k, so ist f in $k[X]$ irreduzibel und K/k zyklisch von Grad p.

b) Ist K/k zyklisch vom Grad p, so gibt es ein $b \in K$ mit $b^p - b \in k$ und $k(b) = K$. Für $a = b^p - b$ ist $f = X^p - X - a$ das Minimalpolynom von b über k und K der Zerfällungskörper von f über k.

Beweis.

a) Nehme $b \in K$ mit $f(b) = 0$. Dafür sind $b, b+1, b+2, \ldots, b+(p-1)$ die p verschiedenen Nullstellen von f [$f(b+i) = (b+i)^p - (b+i) - a = b^p - b - a + i^p - i = f(b) = 0$, kleiner Satz von Fermat]. Also ist f separabel und $K = k(b)$ ist galoissch über k. Im Fall i) ist $b \in k$, also $K = k$. Im Fall ii) ist $b \notin k = \mathrm{Fix}_K(G)$ mit $G = \mathrm{Gal}(K/k)$, also $\sigma(b) \neq b$ für ein $\sigma \in G$. Mit $\sigma(b) = b + m$ für ein $m \in \{1, \ldots, p-1\}$ ist $\sigma^\ell(b) = b + \ell m$ für $\ell \geq 0$. Damit ist $|\{\mathrm{id} = \sigma^0, \sigma^1, \ldots, \sigma^{p-1}\}| = p$, denn aus $\sigma^i = \sigma^j$ mit $0 \leq i, j \leq p-1$, speziell $\sigma^i(b) = \sigma^j(b)$ folgt $im = jm$ in K, also $i = j$ wegen $m \neq 0$ in $\mathbb{F}_p \subseteq K$. Es ergibt sich $p \leq |G| = [K : k] = [k(b) : b] \leq p$, insbesondere ist f das Minimalpolynom von b über k.

b) Wieder sei $G = \mathrm{Gal}(K/k)$. Nach Voraussetzung ist $G = \langle\sigma\rangle$. Wegen $T(-1) = p \cdot (-1) = 0$ gibt es nach Lemma (Hilbert 90) ein $b \in K$ mit $-1 = b - \sigma(b)$, d.h. $\sigma(b) = b+1$. Aus $\sigma(b^p - b) = \sigma(b)^p - \sigma(b) = (b+1)^p - (b+1) = b^p + 1 - b - 1 = b^p - b$ folgt $b^p - b \in \mathrm{Fix}_K(G) = k$. Wegen $\sigma(b) \neq b$ ist $b \notin k$, d.h. $k \subsetneq k(b) \subseteq K$, also $k(b) = K$. Speziell ist $[k(b) : k] = p$, also f das Minimalpolynom von b über k wegen $f(b) = 0$. Speziell $[k(b) : k] = p$, also f das Minimalpolynom von b über k wegen $f(b) = 0$ und damit $f = \prod_{i=0}^{p-1}((X - (b + i))$, also K Zerfällungskörper von f. □

3.4 Radikalerweiterungen

Für Grad 1,2,3,4 kann man die Nullstellen eines Polynoms aus den Koeffizienten gewinnen, und zwar durch Wurzelziehen und rationale Operationen.

Für Grad 3 wurde dies von S. dal Ferro und N. Fontana schon 1515 entdeckt, allerdings erst von G. Cardano um 1545 an die breite Öffentlichkeit gebraucht. Die Lösungsformel für Grad 4 fand L. Ferrari im Jahre 1540. Aber geht dies auch für Grad 5 und größer? Leibniz stellte 1680 erstmals die Frage, ob prinzipielle Hindernisse gäbe, die dies verhinderten. Abel lieferte dann 1826 einen ersten einwandfreien Unmöglichkeitsbeweis, allerdings ohne die von ihm verwendeten gruppentheoretischen Methoden explizit auszuführen. Dies tat schließlich Galois († 1832) mit der nach ihm benannten „Galoistheorie“.

Definition. Eine Körpererweiterung $k \subseteq K$ heißt *Radikalerweiterung*, wenn es Zwischenkörper $k = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_m = K$ gibt derart, dass für jedes $i \in \{1, \ldots, m\}$ ein $a_i \in L_i$ und ein $n_i \geq 1$ existieren mit $a_i^{n_i} \in L_{i-1}$ und $L_i = L_{i-1}(a_i)$. Die $n_1, \ldots, n_m$ heißen *Exponenten.*

Bemerkung.

a) Sind $k \subseteq L$ und $L \subseteq K$ Radikalerweiterungen, so auch $k \subseteq L$.

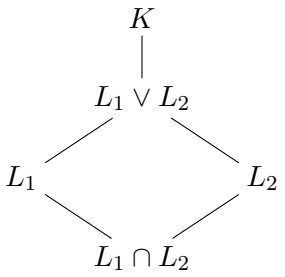
b) Jede Radikalerweiterung ist endlich.

Satz. *Ist $k \subseteq K$ eine Radikalerweiterung und k vollkommen, so gibt es eine Erweiterung $K \subseteq K'$ derart, dass $k \subseteq K'$ eine galoissche Radikalerweiterung ist.*

Beweis. Induktion nach $[K : k]$. Im Fall $k \subsetneq K$ gibt es nach Voraussetzung einen Zwischenkörper L von $k \subseteq K$ mit $L \subsetneq K$, so dass $k \subseteq L$ eine Radikalerweiterung ist und $L(a) = K$ mit $a^n \in L$. Wegen $[L : k] < [K : k]$ gibt es nach Induktion eine Erweiterung $L \subseteq L'$, so dass $k \subseteq L'$ eine galoissche Radikalerweiterung ist. Mit $G' = \mathrm{Gal}(L'/k)$ sei $g = \prod_{\sigma \in G'}(X^n - \sigma(a^n)) \in L'[X]$. Der Zerfällungskörper K' von g über L' ist wie verlangt, denn: Mit $g = \prod_{j=1}^{r}(X - b_j)$ in $K'[X]$ ist $b_j^n = \sigma(a^n)$ für ein $\sigma \in G'$, also $b_j^n \in L'$ $(1 \leq j \leq r)$, sowie $K' = L'(b_1, \ldots, b_r)$, also K' Radikalerweiterung von L' , nach Bemerkung auch von k. Wegen $g(a) = 0$ ist $a \in K'$und damit $K = L(a) \subseteq L'(a) \subseteq K'$. Noch zu zeigen: K'/k ist galoissch. Wegen ${}^{\pi}g = g$ für alle $\pi \in G'$ und $\mathrm{Fix}_{L'}(G') = k$ ist $g \in k[X]$. Nun ist L' Zerfällungskörper eines $f \in k[X] \setminus k$, also K' Zerfällungskörper von $fg \in k[X]$ und damit K'/k galoissch. □

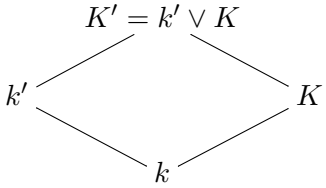
Zusatz. Man kann erreichen, dass $k \subseteq K'$ dieselben Exponenten hat wie $k \subseteq K$, indem man $a \in \{a_1, \ldots, a_m\}$ wählt, denn dann ist in $L' \subseteq L'(b_1) \subseteq L'(b_1, b_2) \subseteq \cdots \subseteq L'(b_1, \ldots, b_r) = K'$ sogar $b_j^n \in L$.

Satz (Verschiebungssatz für Galoiserweiterungen)**.** *Es seien L_1, L_2 Unterkörper eines Körpers K. Für das* Kompositum $L_1 \vee L_2 := L_1(L_2) = L_2(L_1)$ *von L_1 und L_2 gilt: Ist $L_1/(L_1 \cap L_2)$ galoissch, so ist $(L_1 \vee L_2)/L_2$ galoissch mit* $\mathrm{Gal}(L_1/(L_1 \cap L_2)) \cong \mathrm{Gal}((L_1 \vee L_2)/L_2)$.



Beweis. Es sei $k = L_1 \cap L_2$. O.B.d.A. sei $L_1 \vee L_2 = K$. Als Galoiserweiterung ist L_1 Zerfällungskörper eines separablen $f \in k[X]$, welches auch in $L_2[X]$ separabel ist mit Zerfällungskörper K. $[f = \prod_{i=1}^{s}(X - a_i), k(a_1, \ldots, a_s) = L_1 \Rightarrow L_2(a_1, \ldots, a_s) = L_2(L_1) = K]$, also ist K/L_2 galoissch. Für $\sigma \in \mathrm{Gal}(K/L_2)$ ist $\sigma(a_i) \in \{a_1, \ldots, a_s\}$, d.h. $\sigma(L_1) \subseteq L_1$ (Dimensionsargument), also $\sigma(L_1) = L_1$, weshalb $\varphi\colon \mathrm{Gal}(K/L_2) \to \mathrm{Gal}(L_1/k), \sigma \mapsto \sigma|_{L_1}$ definiert ist. Klar ist, dass φ ein Gruppenmonomorphismus ist. Noch zu zeigen: φ ist surjektiv, d.h. für $H = \mathrm{Im}(\varphi)$ ist $H = \mathrm{Gal}(L_1/k)$, d.h. $\mathrm{Fix}_{L_1}(H) = k$ (Hauptsatz). Nur „$\subseteq$“: zu $x \in L_1 \setminus k$, also $x \in L_1 \setminus L_2$ gibt es ein $\sigma \in \mathrm{Gal}(K/L_2)$ mit $\sigma(x) \neq x$, also $\varphi(x) \neq x$ mit $\varphi(\sigma) \in H$, weshalb $x \in L_1 \setminus \mathrm{Fix}_{L_1}(H)$, so ist $(L_1 \vee L_2)/L_2$ galoissch mit $\mathrm{Gal}(L_1/(L_1 \cap L_2)) \cong \mathrm{Gal}((L_1 \vee L_2)/L_2)$. □

Korollar 1.



In obigem Diagramm sei $K' = k' \vee K$ (aber nicht unbedingt $k = k' \cap K$). Ist K/k galoissch, so ist K/k' galoissch und $\mathrm{Gal}(K'/k')$ *ist isomorph zu einer Untergruppe von* $\mathrm{Gal}(K/k)$.

Beweis. Auch $K'/(k' \cap K)$ ist galoissch, und $\mathrm{Gal}(K/(k' \cap K))$ ist Untergruppe von $\mathrm{Gal}(K/k)$. Satz mit $L_1 = K$, $L_2 = k'$. □

Erinnerung. Sei G eine Gruppe und H eine Untergruppe von G. Dann gilt

- G abelsch $\Longrightarrow$ G auflösbar.
- G auflösbar $\Longrightarrow$ H auflösbar.
- G auflösbar $\wedge$ $H \lhd G \Longrightarrow$ G/H auflösbar.

— $H, G/H$ auflösbar $\wedge$ $H \lhd G \Longrightarrow G$ auflösbar.

Korollar 2. *Es sei k ein Körper, $n \geq 1$, $\mathrm{char}(k) \nmid n$. Ist $k \subseteq K$ eine Galoiserweiterung, so ist $k_n \subseteq K_n$ eine Galoiserweiterung, und es gilt: $G = \mathrm{Gal}(K/k)$ ist genau dann auflösbar, wenn $G_n = \mathrm{Gal}(K_n/k_n)$ es ist.*

Beweis. Wegen $K_n = k_n \vee K$ is K_n/k_n galoissch nach Korollar 1, sowie G_n isomorphi zu einer Untergruppe von G, woraus „$\Rightarrow$“ folgt. „$\Leftarrow$“: Sogar K_n/k_n ist galoissch, denn K ist Zerfällungskörper eines separablen $f \in k[X]$ nach Voraussetzung, also K_n Zerfällungskörper des separablen Polynoms $f \cdot (X^n - 1) \in k[X]$. Wegen k_n/k galoissch ist (Hauptsatz) $G_n \lhd \mathrm{Gal}(K_n/k)$ mit abelschem Faktor $\mathrm{Gal}(K_n/k)/G_n \cong \mathrm{Gal}(k_n/k)$. Ist also G_n auflösbar, so auch $\mathrm{Gal}(K_n/k)$. Wegen K/k galoissch ist (Hauptsatz) $\mathrm{Gal}(K_n/K) \lhd \mathrm{Gal}(K_n/k)$ mit $\mathrm{Gal}(K_n/k)/\mathrm{Gal}(K_n/K) \cong G$ und mit $\mathrm{Gal}(K_n/k)$ ist auch G auflösbar. □

Satz (Kriterium von Galois)**.** *Es sei $k \subseteq K$ eine Galoiserweiterung, $G = \mathrm{Gal}(K/k)$, $\mathrm{char}(k) = 0$. Genau dann ist G auflösbar, wenn K einen Oberkörper E hat, sodass $k \subseteq E$ eine Radikalerweiterung ist.*

Beweis. „$\Rightarrow$“: Induktion nach $|G|$: Im Fall $|G| > 1$ gibt es $H \lhd G$ mit $[G : H] = p$ eine Primzahl. Nach Korollar 2 für $n = p$ ist K_p/k_p galoissch und $G_p = \mathrm{Gal}(K_p/k_p)$ auflösbar, sowie isomorph zu einer Untergruppe von G nach Korollar 1.

Ist $|G_p| < |G|$, so gibt es zu $k_p \subseteq K_p$ nach Induktion eine Erweiterung $K_p \subseteq E$, sodass $k_p \subseteq E$ eine Radikalerweiterung ist, weshalb auch $k \subseteq E$ eine Radikalerweiterung ist, da ja $k \subseteq k_p$ eine Radikalerweiterung ist.

Ist $|G_p| = |G|$, d.h. $G_p \cong G$, so gilt für das Bild H_p von H in G_p, dass $L = \mathrm{Fix}_{K_p}(H_p)$ galoissch über k_p vom Grad $[G_p : H_p] = p$ ist, also $L = k_p(a)$ mit $a^p \in k_p$ (Satz über die $X^n - a$). Speziell ist $k_p \subsetneq L$ eine Radikalerweiterung. Nach Induktion gibt es yu $L \subseteq K_p$ eine Erweiterung $K_p \subseteq E$, sodass $L \subseteq E$ und damit auch $k \subseteq E$ eine Radikalerweiterung ist [da $k \subseteq k_p$ und $k_p \subseteq L$, also auch $k \subseteq L$ eine Radikalerweiterung ist].

„$\Leftarrow$“: Es gibt eine Erweiterung $E \subseteq E'$, sodass $k \subseteq E'$ eine *galoissche* Radikalerweiterung ist. Ist $\mathrm{Gal}(E'/k)$ auflösbar, so auch $\mathrm{Gal}(E'/k)/\mathrm{Gal}(E'/K) \cong G$, weshalb wir $K = E = E'$ annehmen können, d.h. dass $k \subseteq K$ eine galoissche *Radikal*erweiterung ist, oder auch $k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = K$ mit $L_{i-1}(a_i) = L_i$ und $a_i^{n_i} \in L_{i-1}$ $(1 \leq i \leq m)$. Nun Induktoin über m: Nach Korollar 2 für $n = n_1$ reicht es yu yeigen, dass $G_n = \mathrm{Gal}(K_n/k_n)$ auflösbar ist. Für $L = k_n(a_1)$ ist $k_n \subseteq L \subseteq k_n(a_1, a_2) \subseteq \cdots \subseteq k_n(a_1, \ldots, a_m) = K_n$, also nach Induktion (für $L \subseteq K_n$): $H_n = \mathrm{Gal}(K_n/L)$ ist auflösbar und L als Zerfällungskörper von $X^n - a_1^n \in k_n[X]$ zyklisch über k_n (Satz über die $X^n - a$), speziell $H_n \lhd G_n$ mit $G_n/H_n \cong \mathrm{Gal}(L/k_n)$ zyklisch, also G_n auflösbar. □

Bemerkung. Für „$\Rightarrow$“ reicht $\mathrm{char}(k) \nmid |G|$ anstelle von $\mathrm{char}(k) = 0$ mit dem selben Beweis [$\mathrm{char}(k) \nmid p$, $\mathrm{char}(k) \nmid |G_p|$].

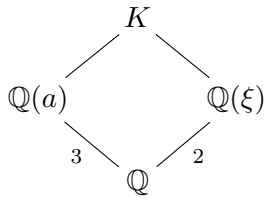
Bemerkung. Ist K/k galoissch und $\mathrm{Gal}(K/k)$ eine p-Gruppe mit $\mathrm{char}(k) \nmid p$, so gibt es eine Erweiterung $K \subseteq E$, sodass $k \subseteq E$ eine Radikalerweiterung ist.

Definition. Sei k ein Körper und K der Zerfällungskörper von $f \in k[X] \setminus k$. Man nennt $G = \mathrm{Gal}(K/k)$ die *Galoisgruppe* $\mathrm{Gal}(f/k)$ von f über k.

Beispiel. Es ist $\mathrm{Gal}(X^n - 1/k) = \mathrm{Gal}(k_n/k)$ für $\mathrm{char}(k) \nmid n$ isomorph zu einer Untergruppe von $(\mathbb{Z}/(n))^\times$, speziell $\mathrm{Gal}(X^n - 1/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$.

Sind $a_1, \ldots, a_m \in K$ die m verschiedenen Nullstellen von f, so operiert G auf $N = \{a_1, \ldots, a_m\}$ vermöge $G \times N \to N, (\sigma, a) \mapsto \sigma(a)$, d.h. man hat den Gruppenhomomorphismus $\gamma\colon G \to S_m$ mit $\gamma(\sigma)(i) = j$ genau dann, wenn $\sigma(a_i) = a_j$ $(1 \leq i, j \leq m)$. Diese Operation ist *treu*, d.h. γ ist injektiv, mit anderen Worten: Aus $\sigma(a) = a$ für alle $a \in N$ folgt $\sigma = \mathrm{id}$. Insbesondere ist $[K : k] = |\mathrm{Gal}(f/k)| = |G|$ ein Teiler von $m! = |S_m|$. Ist f irreduzibel, d.h. f bis auf Normierung Minimalpolynom jedes $a \in N$, so ist die Operation transitiv, d.h. $\forall a, b \in N \exists \sigma \in G(\sigma(a) = b)$.

Beispiel. Für jede Primzahl p und $f = X^3 - p \in \mathbb{Q}[X]$ ist $N = \{a, a\xi, a\xi^2\}$ für $a = \sqrt[3]{p}$, $\xi \in P_3(\mathbb{Q})$, sowie $K = \mathbb{Q}(a, \xi)$ mit $[K : \mathbb{Q}] = 6$, d.h. $|\mathrm{Gal}(f/\mathbb{Q})| = 6$ und damit $\mathrm{Gal}(f/\mathbb{Q}) \cong_\gamma S_3$, insbesondere ist die Galoiserweiterung K/k nicht abelsch.



Definition. Man nennt $f \in k[X] \setminus k$ *durch Radikale auflösbar*, wenn es eine Radikalerweiterung $k \subseteq E$ gibt, sodass f in $E[X]$ in Linearfaktoren zerfällt. Speziell kann man erreichen, dass $k \subseteq K \subseteq E$ ist für den Zerfällungskörper K von f über k.

Satz. *Es sei k ein Körper mit $\mathrm{char}(k) = 0$. Genau dann ist $f \in k[X] \setminus k$ durch Radikale auflösbar, wenn $\mathrm{Gal}(f/k)$ eine auflösbare Gruppe ist.*

Beweis. Folgt sofort.

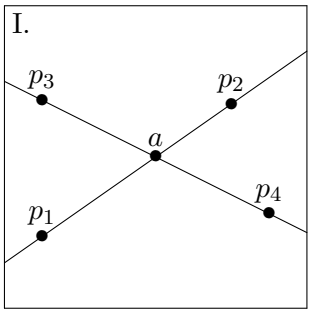
Korollar. *Für einen Körper k mit $\mathrm{char}(k) = 0$ ist jedes $f \in k[X] \setminus k$ mit $\deg(f) \leq 4$ durch Radikale auflösbar.*

Beweis. $\mathrm{Gal}(f/k)$ ist via γ isomorph zu einer Untergruppe von S_m mit $m \leq 4$. □

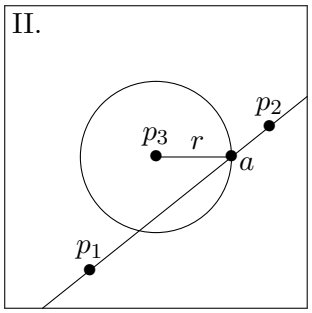
Man kann zeigen (evtl. später): Zu jedem $n \geq 1$ gibt es eine Galoiserweiterung $\mathbb{Q} \subseteq K$ mit $\mathrm{Gal}(K/\mathbb{Q}) \cong S_n$, d.h. $\mathrm{Gal}(f/\mathbb{Q}) \cong S_n$ für jedes $f \in \mathbb{Q}[X]$, dessen Zerfällungskörper gleich K ist. Für $n \geq 5$ ist f also nicht durch Radikale auflösbar.

3.5 Konstruktionen mit Zirkel und Lineal

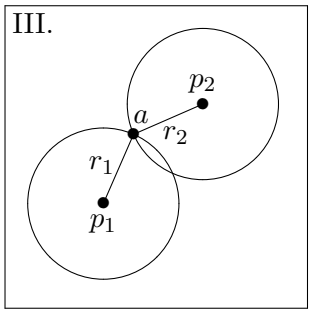
Es sei $M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Man sagt, dass a aus M durch einen *elementaren Konstruktionsschritt* entsteht, wenn



$p_1, p_2, p_3, p_4 \in M$



$r = |p_4 - p_5|$
$p_1, p_2, p_3, p_4, p_5 \in M$



$r_1 = |p_4 - p_3|, r_2 = |p_5 - p_6|$
$p_1, p_2, p_3, p_4, p_5, p_6 \in M$

Es sei $\mathscr{E}(M)$ die Menge aller $a \in \mathbb{C}$, die aus M durch einen elementaren Konstruktionsschritt entstehen.

Erinnerung. $z\overline{z} = |z|^2$ für ein $z \in \mathbb{C}$, speziell $z \in L = \overline{L} \Rightarrow |z|^2 \in L$ mit $\overline{L} = \{\overline{z} \colon z \in L\}$.

Lemma. *Es sei L ein Unterkörper von $\mathbb{C}$ mit $L = \overline{L}$, d.h. $\forall z \in \mathbb{C}(z \in L \Rightarrow \overline{z} \in L)$. Ist $a \in \mathscr{E}(M)$ für ein $M \subseteq L$, so gibt es ein $b \in \mathbb{C}$ mit $a \in L(b)$ und $b^2 \in L$.*

Beweis.

I. Hier ist $b = 1$ möglich, denn: aus $a = p_1 + u(p_2 - p_1)$, $a = p_3 + v(p_4 - p3)$ mit $u, v \in \mathbb{R}$ folgt

$$\begin{pmatrix} p_2 - p_1 & p_3 - p_4 \\ \overline{p_2} - \overline{p_1} & \overline{p_3} - \overline{p_4} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p_3 - p_1 \\ \overline{p_3} - \overline{p_1} \end{pmatrix}$$

worin die Matrix Determinante $\neq 0$ hat [sonst wäre $z = \overline{z}$ für $z = (p_2 - p_1)(\overline{p_3} - \overline{p_4})$, d.h. $z \in \mathbb{R}$, also die beiden Geraden parallel, denn: $z = x\overline{y} \Rightarrow zy = x|y|^2$], also $u, v \in L$, also $a \in L$.

II. Aus $a = p_1 + u(p_2 - p_1)$ mit $u \in \mathbb{R}$ und $|a - p_3| = r$ folgt, dass

$$(\underbrace{u(p_2 - p_1) + p_1 - p_3}_{a - p_3})(\underbrace{u(\overline{p_2} - \overline{p_1}) + \overline{p_1} - \overline{p_3}}_{\overline{a} - \overline{p_3}}) = |a - p_3|^2 = r^2 = |p_4 - p_5|^2 \in L$$

d.h. $(ux + y)(u\overline{x} + \overline{y}) = u^2|x|^2 + u(x\overline{y} + \overline{x}y) + |y|^2 \in L$ mit $x, y \in L$, also $u^2 + 2uq \in L$ für ein $q \in L$ (nämlich $q = (x\overline{y} + \overline{x}y)/(2|x|^2)$), weshalb $b = u + q$ wie verlangt, denn $b^2 = u^2 + 2uq + q^2 \in L$ sowie $a \in L(b)$ wegen $u = b - q \in L(b)$.

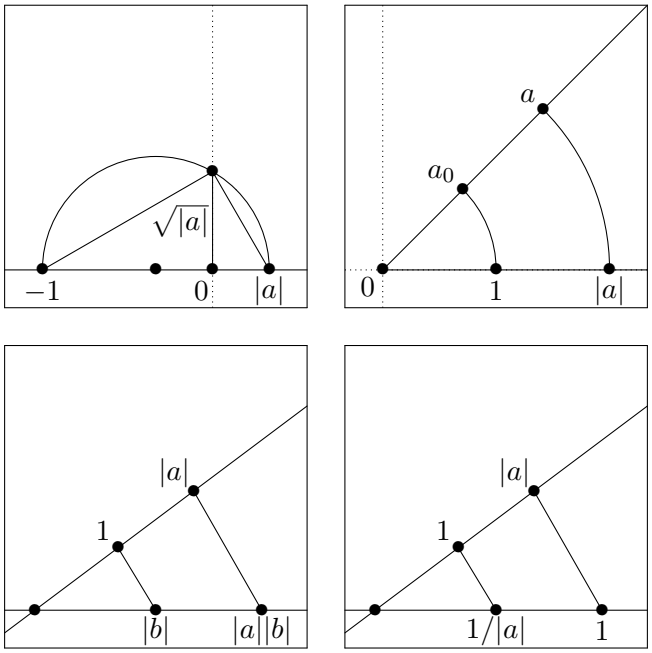
III. Aus $L \ni (a - p_\nu)(\overline{a} - \overline{p_\nu}) = |a - p_\nu|^2 = r_\nu^2$ $(*)$ für $\nu = 1, 2$ folgt $L \ni r_1^2 - r_2^2 = a(\overline{p_2} - \overline{p_1}) + \overline{a}(p_2 - p_1) + |p_1|^2 - |p_2|^2$, d.h. $a(\overline{p_2} - \overline{p_1}) + \overline{a}(p_2 - p_1) \in L$, also $\overline{a} = aq_1 + q_2$ mit $q_1, q_2 \in L$. Durch Einsetzen in $(*)$ erhält man $a^2 + 2aq \in L$ für ein $q \in L$, also $b = a + q$ wie verlangt. □

Definition. Ein $a \in \mathbb{C}$ heißt (mit Zirkel und Lineal) *konstruierbar*, wenn es $a_1, \ldots, a_n \in \mathbb{C}$ gibt mit $a_n = a$ und $a_1 \in \mathscr{E}(0,1)$, $a_2 \in \mathscr{E}(0,1,a_1)$, $\ldots$, $a_n \in \mathscr{E}(0,1,a_1,\ldots,a_{n-1})$.

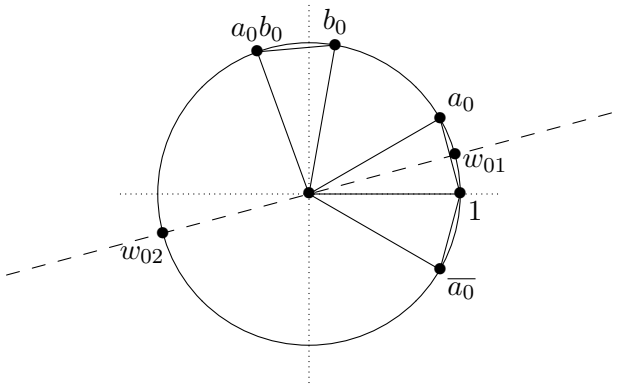
Bemerkung. Alle $a \in \mathbb{Z}$ sind konstruierbar, sogar alle $a \in \mathbb{Z}[i]$, d.h. alle *ganzzahligen ebenen Gitterpunkte*.

Lemma. *Die Menge* $\mathbb{K} = \{a \in \mathbb{C} \colon a \text{ konstruierbar}\}$ *ist ein Unterkörper von* $\mathbb{C}$*, der* quadratisch abgeschlossen *ist, d.h.* $\forall z \in \mathbb{C}(z^2 \in \mathbb{K} \Rightarrow z \in \mathbb{K})$.

Beweis. Klar: $0, 1 \in \mathbb{K}$. Nun seien $a, b \in \mathbb{K}$. Neben $-a, a+b \in \mathbb{K}$ gilt $|a|, |b| \in \mathbb{K}$, sowie $a_0, b_0 \in \mathbb{K}$ mit $a = |a|a_0$, $b = |b|b_0$. Es folgt $|a| \cdot |b| \in \mathbb{K}$ und $1/|a| \in \mathbb{K}$ für $a \neq 0$ (Strahlensatz), sowie $\sqrt{|a|} \in \mathbb{K}$ (Höhensatz):



Ferner gilt $a_0 \cdot b_0$, $\overline{a_0} \in \mathbb{K}$ und $w_{0\nu} \in \mathbb{K}$ für $w_{0\nu}^2 = a_0$ $(\nu = 0, 1)$:



Es ergibt sich $a \cdot b = \underbrace{|a| \cdot |b|}_{\in \mathbb{K} \cap \mathbb{R}} \cdot a_0 \cdot b_0 \in \mathbb{K}$ (!), $1/a = 1/|a| \cdot \overline{a_0} \in \mathbb{K}$, $w_\nu = \sqrt{|a|} \cdot w_{0\nu} \in \mathbb{K}$ $(\nu = 1, 2)$ mit $w_\nu^2 = a$. □

Satz. *Für jedes $a \in \mathbb{C}$ sind äquivalent:*

i) $a \in \mathbb{K}$

ii) Es gibt eine Folge $L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m$ von Unterkörpern von $\mathbb{C}$, so dass $\mathbb{Q} = L_0$, $[L_\nu : L_{\nu-1}] = 2$ $(1 \leq \nu \leq m)$, $a \in L_m$.

iii) a ist algebraisch über $\mathbb{Q}$ und für das Minimalpolynom f von a über $\mathbb{Q}$ ist $\mathrm{Gal}(f/\mathbb{Q})$ eine 2-Gruppe, d.h. (siehe unten) $|\mathrm{Gal}(f/\mathbb{Q})| = 2^\ell$ $(\ell \geq 0)$.

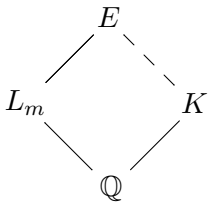
iv) Es gibt einen Zwischenkörper K von $\mathbb{Q} \subseteq \mathbb{C}$, so dass $K/\mathbb{Q}$ galoissch, $[K : \mathbb{Q}]$ eine Zweierpotenz und $a \subseteq K$ ist.

Beweis.

i $\Rightarrow$ ii Es seien $a_1, \ldots, a_n \in \mathbb{C}$ mit $a_1 \in \mathscr{E}(0,1)$, $a_2 \in \mathscr{E}(0,1,a_1)$, $\ldots$ und $a_n = a$. Wegen $0, 1 \in \mathbb{Q}$ und $\mathbb{Q} = \overline{\mathbb{Q}}$ gibt es (vorvoriges Lemma) ein $b_0 \in \mathbb{C}$ mit $b_0^2 \in \mathbb{Q}$ und $a_1 \in \mathbb{Q}(b_0) =: L_1$, dafür muss nicht $L_1 = \overline{L_1}$ sein! Für $b_1 = \overline{b_0}$ ist aber $b_1^2 = \overline{b_0^2} \in L_1$, sogar $b_1^2 \in \mathbb{Q}$, und $a \in L_1(b_1) =: L_2$, sowie $L_2 = \overline{L_2}$. Ebenso gibt es ein $b_2 \in \mathbb{C}$ mit $b_2^2 \in L_2$ und $a_2 \in L_2(b_2) =: L_3$. Für $b_3 = \overline{b_2}$ ist $b_3^2 = \overline{b_2^2} \in L_3$, sogar $b_3^2 \in L_2$, und $a_2 \in L_3(b_3) =: L_4$, $L_4 = \overline{L_4}$, usw. bis zu $a = a_n \in L_{2n-1}$. In $\mathbb{Q} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{2n-1}$ ist $[L_i : L_{i-1}] \leq 2$.

ii $\Rightarrow$ i Wir zeigen $L_i \subseteq \mathbb{K}$ durch Induktion nach i. Fall $i = 0$: $L_0 = \mathbb{Q} \subseteq \mathbb{K}$. Fall $i > 0$: Nehme $b \in \mathbb{C}$ mit $L_{i-1}(b) = L_i$. Nach Induktion reicht es zu zeigen, dass $b \in \mathbb{K}$ ist (hier verwendet: $\mathbb{K}$ ist ein Körper, Lemma). Dazu sei $X^2 + rX + s$ das Minimalpolynom von L_{i-1}, wofür gilt: $(b + \frac{r}{2})^2 = \frac{r^2}{4} - s \in L_{i-1} \subseteq \mathbb{K} \Rightarrow b + \frac{r}{2} \in \mathbb{K}$ (nach Lemma), d.h. $b \in \mathbb{K}$. (nach Induktion ist $r \in \mathbb{K}$).

ii $\Rightarrow$ iii Gerade gesehen: $\mathbb{Q} \subseteq L_m$ ist Radikalerweiterung, für die alle Exponenten 2 sind. Nach Lemma früher gibt es eine Erweiterung $L_m \subseteq E$, so dass $\mathbb{Q} \subseteq E$ eine galoissche Radikalerweiterung mit denselben Exponenten ist. Speziell ist $\mathrm{Gal}(E/\mathbb{Q})$ eine 2-Gruppe, also auch die Faktorgruppe $\mathrm{Gal}(f/\mathbb{Q})$, denn für den Zerfällungskörper K von f über $\mathbb{Q}$ kann man $K \subseteq E$ erreichen [$f(a) = 0, a \in L_m \subseteq E$, $\mathbb{Q} \subseteq E$ galoissch, f irreduzibel. $\Rightarrow$ f zerfällt in $E[X]$ in Linearfaktoren].



iii $\Rightarrow$ iv Klar mit K wie oben.

iv $\Rightarrow$ ii Nach dem Satz von Wielandt (folgt sofort!) hat man Untergruppen $\{\mathrm{id}\} = H_m \subseteq H_{m-1} \subseteq \cdots \subseteq H_1 \subseteq H_0 = G$ von $G = \mathrm{Gal}(K/\mathbb{Q})$ mit $|H_i| = 2^{m-i}$ $(0 \leq i \leq m)$. Für $L_i = \mathrm{Fix}_K(H_i)$ folgt $\mathbb{Q} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = K$ und nach Artin $[K : L_i] = |H_i| = 2^{m-i}$, also $[K : L_{m-1}] = 2$, $[L_{m-1} : L_{m-2}] = 2$, etc. $\square$

Korollar 1. *Für jedes $a \in \mathbb{K}$ ist $\mathbb{Q}(a)$ eine algebraische Erweiterung von $\mathbb{Q}$, so dass $[\mathbb{Q}(a) : \mathbb{Q}]$ eine Potenz von 2 ist.*

Beweis. Für den Zerfällungskörper K des Minimalpolynoms von a über $\mathbb{Q}$ ist o.E. $\mathbb{Q}(a) \subseteq K$. □

Korollar 2 (Unmöglichkeit der Quadratur des Kreises)**.** *Es gibt kein Quadrat mit konstruierbarer Seitenlänge, das den Flächeninhalt des Einheitskreises hat, d.h. $\nexists a \in \mathbb{K}(a^2 = \pi)$.*

Beweis. Korollar 1: Mit a wäre auch $a^2 = \pi$ algebraisch über $\mathbb{Q}$, aber π ist nach Lindemann 1882 nicht algebraisch, d.h. *transzendent.* □

Korollar 3 (Unmöglichkeit der Würfelverdopplung)**.** *Es gibt keinen Würfel mit konstruierbarer Kantenlänge, dessen Rauminhalt das Doppelte des Einheitswürfels ist, d.h. $\nexists a \in \mathbb{K}(a^3 = 2)$.*

Beweis. Für jedes $a \in \mathbb{C}$ mit $a^3 = 2$ ist $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, Korollar 1. □

Korollar 4. *Genau dann ist das regelmäßige n-Eck mit Zirkel und Linear konstruierbar, d.h. $e^{2\pi i/n} \in \mathbb{K}$, wenn $\varphi(n) = 2^n$. Dies ist zum Beispiel der Fall für $n \in \{3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \dots\}$.*

Beweis. Φ_n ist das Minimalpolynom von $e^{2\pi i/n}$ über $\mathbb{Q}$, und $\mathrm{Gal}(\Phi_n/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ hat Ordnung $\varphi(n)$. □

Bemerkung. Wegen $\varphi(p^\ell) = p^\ell - p^{\ell-1} = p^\ell(p-1)$ ist $\varphi(2^\ell)$ eine Potenz von 2 für $\ell \geq 0$. Für $n = 2^\ell \cdot p_1^{m_1} \cdots p_r^{m_r}$ mit r verschiedenen Primzahlen $p_i \geq 3$ und $m_i \geq 1$ ist $\varphi(n)$ genau dann Potenz von 2, wenn alle $\varphi(p_i^{m_i})$ es sind, d.h. wenn alle $m_i = 1$ und alle $p_i = 2^{n_i} + 1$ sind. Bisher kennt man nur fünf dieser *Fermatschen Primzahlen*: $p \in \{3, 5, 17, 257, 65537\}$.

Korollar 5. *Nicht jeder Winkel lässt sich mit Zirkel und Lineal dreiteilen, z.B. geht das nicht für $60°$.*

Beweis. Sonst wäre das regelmäßige 18-Eck konstruierbar, aber $\varphi(18) = 6$. □

4 Sylow-Untergruppen

Satz (Wielandt)**.** *Es sei G eine endliche Gruppe, $|G| = n$, und $d \geq 1$ mit $d \mid n$. Ist $d = p^\ell$ für eine Primzahl p, so hat G eine Untergruppe U mit $|U| = d$.*

Beweis. G operiert auf $V = \{A \subseteq G \colon |A| = d\}$ durch $G \times V \to V, (x, A) \mapsto xA$, und für $A \in V$ ist $|S(A)| \leq d$ [für beliebiges $a \in A$ ist $S(A) \to A, x \mapsto xa$ definiert und injektiv]. Unser Ziel ist nun ein $A_0 \in V$ mit $|S(A_0)| = d$, denn dafür ist $U = S(A_0)$ wie verlangt. Zunächst zeigen wir: $p \nmid \binom{n-1}{d-1}$. Dazu sei $i = p^{\ell_i} m_i$ für $1 \leq i \leq d-1$ mit $\ell_i \geq 0$ und $p \nmid m_i$. Dafür ist $\ell_i < \ell$ und

$$\frac{n-i}{d-i} = \frac{p^\ell n' - p^{\ell_i} m_i}{p^\ell - p^{\ell_i} m_i} = \frac{p r_i - m_i}{p s_i - m_i}$$

mit $r_i, s_i \geq 1$, also

$$\binom{n-1}{d-1} = \prod_{i=1}^{d-1} \frac{n-i}{d-i} = \prod_{i=1}^{d-1} \frac{pr_i - m_i}{ps_i - m_i} = \frac{pr+t}{ps+t}$$

mit $r, s \in \mathbb{Z}$, $t = \prod_{i=1}^{d-1}(-m_i)$. Aus $p \mid \binom{n-1}{d-1}$ folgte $pu(ps+t) = pr+t$ mit $u \geq 1$, also $p \mid t$, d.h. $p \mid m_i$ für ein i, was wir ausgeschlossen haben. Also $p \nmid \binom{n-1}{d-1}$. Wir beschließen den Beweis wie folgt: Für $n/d = p^{\ell'}m$ mit $\ell' \geq 0$, $p \nmid m$ ist $|V| = \binom{n}{d} = \frac{n}{d}\binom{n-1}{d-1} = p^{\ell'}m\binom{n-1}{d-1}$, also $p^{\ell'+1} \nmid |V|$. Wegen $V = \bigsqcup_{A \in V} B(A)$ gibt es ein $A_0 \in V$ mit $p^{\ell'+1} \nmid |B(A_0)|$, also: $d = p^\ell$ teilt $|S(A_0)|$ wegen $|S(A_0)| \cdot |B(A_0)| = n = p^{\ell+\ell'}m$. □

Beispiel. $d = p^\ell$ ist unerlässlich: Für $n \geq 5$ hat A_n keine Untergruppe U mit $[A_n : U] = 2$, d.h. $|U| = |A_n|/2 = \frac{n!}{4}$, obzwar $\frac{n!}{4} \mid |A_n|$.

Satz (Cauchy)**.** *Sei G eine endliche Gruppe. Ist p eine Primzahl mit $p \mid |G|$, so hat G ein Element der Ordnung p.*

Beweis. Spezialfall des Satzes von Wielandt.

Bemerkung. Für jede endliche Gruppe G und jede Primzahl p sind äquivalent:

i) $|G|$ ist eine Potenz von p.
ii) Für alle $x \in G$ ist $\operatorname{ord}(x)$ eine Potenz von p. In diesem Fall heißt G (endliche) p-Gruppe.

Beweis. Nur ii) ⇒ i): Zu jedem Primteiler von $|G|$ gibt es ein $x \in G$ mit $\operatorname{ord}(x) = q$, weshalb $p = q$ sein muss. □

Lemma. *Für jede endliche p-Gruppe gilt: $|G| \neq 1 \Rightarrow |Z(G)| \neq 1$*

Korollar. *Ist G eine endliche p-Gruppe, so hat G zu jedem $d \geq 1$ mit $d \mid |G|$ einen Normalteiler der Ordnung d.*

Beweis. Induktion nach $n = |G|$. Nur für $d, n > 1$. Nach Lemma ist $Z(G) \neq 1$, speziell ist $|Z(G)| > 1$ ein Vielfaches von p, also hat $Z(G)$ eine Untergruppe U mit $|U| = p$. Nun ist $U \lhd G$ und $[G : U] = n/p$, also (Induktion) hat G/U einen Normalteiler H/U mit $[H : U] = d/p$, wofür $H \lhd G$ mit $|H| = d$ gilt. □

Anwendung. Zu jeder Primzahl p gibt es bis auf Isomorphie genau zwei Gruppen der Ordnung p^2, nämlich $\mathbb{Z}/\langle p^2\rangle$ und $(\mathbb{Z}/\langle p\rangle)^2 = \mathbb{Z}/\langle p\rangle \times \mathbb{Z}/\langle p\rangle$.

Definition. Nun sei G eine Gruppe und p eine Primzahl. Die *p-Komponente* $G_p = \{x \in G\colon \operatorname{ord}(x) \text{ ist Potenz von } p\}$ ist (!) die Vereinigung aller p-Untergruppen von G. Ist G_p eine Untergruppe von G, z.B. wenn (!) G abelsch ist, so ist G_p die *größte p-Untergruppe* von G. Eine bezüglich $\subseteq$ maximale p-Untergruppe von G heißt *p-Sylow-Untergruppe*, hier kurz p-SU, von G.

Bemerkung. Mit dem Lemma von Zorn hat jedes G eine p-Sylow-Untergruppe. Ohne das Lemma von Zorn gilt dies zumindest für $|G| < \infty$, denn dann hat G nur endlich viele p-Untergruppen.

Beispiel.

1) Ist $p \nmid |G|$, so ist $G_p = \{e\}$ die einzige p-Sylow-Untergruppe von G.
2) Ist $|G| = p^\ell m$ mit $\ell \geq 0$ und $p \nmid m$, so ist jede Untergruppe U mit $|U| \geq p^\ell$ eine p-Sylow-Untergruppe von G, denn ist H eine p-Untergruppe mit $U \subseteq H$, so ist $|H| = p^k$ mit $|U| \mid |H| \mid |G|$, also $\ell \leq k \leq \ell$, d.h. $k = \ell$, also $|U| = |H|$ und damit $U = H$. Inbesondere ($m = 1$): Ist G eine endliche p-Gruppe, so ist $G_p = G$ die größte p-Untergruppe und damit die einzige p-Sylow-Untergruppe.
3) Jede Konjugierte xPx^{-1} einer p-Sylow-Untergruppe P mit $x \in G$ ist wieder eine p-Sylow-Untergruppe von G, denn $|xPx^{-1}| = |P|$, also ist xPx^{-1} eine p-Untergruppe, und ist H eine p-Untergruppe mit $xPx^{-1} \subseteq H$, so ist $x^{-1}Hx$ eine p-Untergruppe mit $P \subseteq x^{-1}Hx$, also $P = x^{-1}Hx$, d.h. $xPx^{-1} = H$.

Satz (Sylow)**.** *Es sei G eine endliche Gruppe der Ordnung $|G| = n$, und p eine Primzahl mit $n = p^\ell m$ für $\ell \geq 0$ und $p \nmid m$.*

a) Jede p-Sylow-Untergruppe von G hat Ordnung p^ℓ.
b) Je zwei p-Sylow-Untergruppen von G sind zueinander konjugiert.
c) Für die Anzahl s_p der p-Sylow-Untergruppen von G gilt $s_p \mid m$ und $s_p \equiv 1 \bmod p$.

Beweis. Nehme (Wielandt) eine Untergruppe H von G mit $|H| = p^\ell$. Auf $G/H = V$ operiert jede Untergruppe U von G vermöge $U \times V \to V, (u, xH) \mapsto uxH$. Wegen $p \nmid m = [G : H] = |V|$ und $V = \bigsqcup_{x \in G} B(xH)$ gibt es ein $x \in G$ mit $p \nmid |B(xH)| = [U : S(xH)]$. Ist U eine p-Gruppe, so ist $|B(xH)|$ eine Potenz von p, also 1, d.h. xH ist ein Fixpunkt, d.h. $uxH = xH$ für alle $u \in U$ und damit $U \subseteq xHx^{-1}$ [zu $u \in U$ gibt es ein $h \in H$ mit $uxh = xe = x$, also $u = xh^{-1}x^{-1} \in xHx^{-1}$]. Ist U sogar eine p-Sylow-Untergruppe, so folgt $U = xHx^{-1}$, speziell $|U| = p^\ell$. Es ergeben sich damit a) und b). Für c) sei $\mathcal{P} = \{P_0, \ldots, P_{s_p - 1}\}$ mit $H = P_0$ die Menge der p-Sylow-Untergruppen von G, $|\mathcal{P}| = s_p$. Nach b) ist $\mathcal{P} = \{xHx^{-1} \colon x \in G\}$, also $s_p = [G : N_G(H)]$ und damit $s_p \mid [G : H] = m$. Weiters hat die Operation $H \times \mathcal{P} \to \mathcal{P}, (h, P) \mapsto hPh^{-1}$ nur $H = P_0$ als Fixpunkt [H ist einer, und aus $hPh^{-1} = P$ folgt $H \subseteq N_G(P)$, also sind P, H p-Sylow-Untergruppeon von $N_G(P)$ und damit $H = yPy^{-1}$ mit $y \in N_G(P)$ nach b) für $N_G(P)$ statt G, weshalb $H = P$ wegen $P \lhd N_G(P)$]. Mit $\mathcal{P} = \bigsqcup_{P \in \mathcal{P}} B(P) = \{P_0\} \sqcup \bigsqcup_{i > 0} B(P_i)$ und $1 < |B(P_i)| = [H : S(P_i)] \mid |H| = p^\ell$ für $i > 0$ ergibt sich $s_p = |\mathcal{P}| = 1 + p^{\ell_1} + \cdots + p^{\ell_{s_p - 1}}$ mit $\ell_i \geq 1$ für $i > 0$, also $s_p \equiv 1 \bmod p$. □

Zusatz. $s_p - 1$ ist eine Summe positiver Potenzen von p.

Bemerkung. Mit Hilfe der Beispiele 2 und 3 ergibt sich unter den Voraussetzungen des Satzes: Die p-Sylow-Untergruppen von G sind genau die Untergruppen der Ordnung p^ℓ. Durch Konjugation operiert G transitiv auf ihren p-Sylow-Untergruppen. Genau dann gibt es nur eine p-Sylow-Untergruppe, wenn $P \lhd G$ für eine (und damit) alle p-Sylow-Untergruppen P von G.

Anwendung. Es sei G eine endliche Gruppe mit $|G| = pq$ für Primzahlen $p \neq q$. Es gilt $\mathbb{Z}/\langle p\rangle \times \mathbb{Z}/\langle q\rangle \cong \mathbb{Z}/\langle pq\rangle$ [chinesischer Restsatz. Ringhomomorphismen sind Gruppenhomomorphismen]. Nun sei $p < q$. Nehme eine p-Sylow-Untergruppe P und eine q-Sylow-Untergruppe Q von G. Neben $P \cong \mathbb{Z}/\langle p\rangle$, $Q \cong \mathbb{Z}/\langle q\rangle$ ist $Q \lhd G$, denn $s_q \in \{1, p\} \cap \{1, 1+q, 1+2q, \dots\} = \{1\}$ wegen $p < q < 1+q$. Wegen $P \cap Q = \{e\}$ ist $\mu\colon P \times Q \to G, (x, y) \mapsto xy$ injektiv. $[xy = x_1y_1 \Rightarrow x_1^{-1}x = y_1^{-1}y \in P \cap Q = \{e\} \Rightarrow x_1 = x \wedge y_1 = y]$, also sogar bijektiv $[|P \times Q| = pq = |G|]$. Ist $P \not\lhd G$, so ist $1 < s_p \in \{1, q\} \cap \{1, 1+p, 1+2q, \dots\}$, d.h. $s_p = q$ und $s_p = 1 + ip$, also $p \mid q-1$ (z.B. für $p = 2$, $q = 3$). Ist $P \lhd G$, d.h. $s_p = 1$, so ist μ auch ein Homomorphismus, also ein Isomorphismus $[(xy)(x_1y_1) = (xx_1)(yy_1)$ wegen $yx_1y^{-1}x_1^{-1} \in P \cap Q = \{e\}$, d.h. $yx_1 = x_1y]$.

Es ergibt sich: Sind $p < q$ Primzahlen mit $p \nmid q-1$, so ist jede Gruppe der Ordnung pq zyklisch, d.h. isomorph zu $\mathbb{Z}/\langle pq\rangle$ und hat genau eine p-Sylow-Untergruppe sowie genau eine q-Sylow-Untergruppe.

5 Schiefkörper und zentral einfache Algebren

Definition. Ein Schiefkörper D ist ein Ring (im allgemeinen nicht kommutativ), in dem jedes Element $x \in D \setminus \{0\}$ ein multiplikatives Inverses hat.

Beispiel.

— Ein Körper ist ein Schiefkörper.

— Weitere Beispiele ergeben sich aus den *Quaternionenalgebren*: Sei F ein Körper mit $\operatorname{char} F \neq 2$ und $a, b \in F \setminus \{0\}$. Die Quaternionenalgebra $(\frac{a,b}{F})$ zum Paar (a, b) ist definiert als 4-dimensionaler F-Vektorraum $A = F.1 \oplus F.i \oplus F.j \oplus F.(ij)$ mit folgender Multiplikation: 1 operiert als 1, $i^2 = a$, $j^2 = b$, $ij = -ji$, linear fortgesetzt:

$$\begin{aligned}&(u.1 + v.i + w.j + x.(ij)) \cdot (u_1.1 + v_1.i + w_1.j + x_1.(ij)) = \\ &= (uu_1 + vv_1a + ww_1b - xx_1ab).1 + (uv_1 + vu_1 - wx_1b + xw_1b).i \\ &+ (uw_1 + wu_1 + vx_1a - xv_1a).j + (ux_1 + vw_1 - wv_1 + xu_1).(ij)\end{aligned}$$

Definition. Ein Ring R heißt *F-Algebra* mit einem Körper oder kommutativen Ring F, wenn es einen Ringhomomorphismus $i\colon F \to R$ gibt mit $\operatorname{Im} I \subseteq Z(R)$. Nach dieser Definition ist $A = (\frac{a,b}{F})$ eine F-Algebra mit $i\colon F \to A, \lambda \mapsto \lambda 1$.

Frage. Wann ist $(\frac{a,b}{F})$ ein Schiefkörper?

Zur Antwort dieser Frage benutzen wir, dass $(\frac{a,b}{F})$ eine Involution besitzt:

$$u.1 + x.i + y.j + z.(ij) \mapsto u.1 - x.i - y.j - z.(ij)$$

Es gilt $\overline{\alpha \cdot \beta} = \overline{\beta} \cdot \overline{\alpha}$ für alle $\alpha, \beta \in (\frac{a,b}{F})$ und $\overline{\overline{\alpha}} = \alpha$ für alle $\alpha \in (\frac{a,b}{F})$. Dann ist $q\colon (\frac{a,b}{F}) \to F$, $\alpha \mapsto \alpha \cdot \overline{\alpha}$ eine quadratische Form auf dem F-Vektorraum $(\frac{a,b}{F})$.

Erinnerung. Eine Abbildung $q\colon V \to F$ auf einem F-Vektorraum V heißt *quadratische Form*, wenn gilt

— $q(\lambda v) = \lambda^2 q(v)$

— $b_q(v,w) := q(v+w) - q(v) - q(w)$ ist eine symmetrische Bilinearform.

Lemma. *$\left(\frac{a,b}{F}\right)$ ist ein Schiefkörper genau dann, wenn $q = q_{\left(\frac{a,b}{F}\right)}$ nur die triviale Nullstelle hat, d.h. $q(\alpha) = 0 \Leftrightarrow \alpha = 0$.*

Beweis. Wenn $\left(\frac{a,b}{F}\right)$ ein Schiefkörper ist, so gilt $\alpha \cdot \beta \neq 0$ für alle α, β aus $\left(\frac{a,b}{F}\right) \setminus \{0\}$, also ist insbesondere $q(\alpha) = \alpha\overline{\alpha} \neq 0$ für $\alpha \neq 0$. „$\Leftarrow$“: Sei $\alpha \neq 0$, so ist $q(\alpha) \neq 0$, also $1 = \alpha(\frac{1}{q(\alpha)}\overline{\alpha})$, also $\alpha^{-1} = \frac{1}{q(\alpha)}\overline{\alpha}$. □

Folgerung. Ist F algebraisch abgeschlossen, so hat jede quadratische Form $q\colon V \to F$ mit $\dim V \geq 2$ eine nichttriviale Nullstelle, also ist $\left(\frac{a,b}{F}\right)$ nie ein Schiefkörper, wenn F algebraisch abgeschlossen ist. Allgemeiner: Ist F algebraisch abgeschlossen, D eine F-Algebra, die ein Schiefkörper ist, und $\dim_F D < \infty$, so ist $F = D$.

Beweis. Sei $D \supseteq F$ eine F-Algebra und ein Schiefkörper, F algebraisch abgeschlossen und $\dim_F D < \infty$. Sei $x \in D$, dann ist $F[x] = \{\sum_{i=0}^{n} a_i x^i \colon a_i \in F\}$ ein kommutativer (!) Unterkörper von D, denn: Offenbar ist $F[x]$ ein kommutativer Ring, da $F \subseteq Z(D)$. Jedes Element aus $F[x]$ ist invertierbar. Wenn $y \in F[x]$, so auch $1, y, y^2, y^3, \ldots$ und diese müssen linear abhängig sein, d.h. es existiert eine Gleichung der Form

$$a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n = 0$$

wobei nicht alle $a_i = 0$ sind. Sei $i_0 = \min\{i \colon a_i \neq 0\}$, dann $i_0 \leq n-1$, denn $a_n y^n = 0$ ist unmöglich für $a_n \neq 0$, $y \neq 0$. Also $0 = y^{i_0}(a_{i_0} + a_{i_0+1}y + \cdots + a_n y^{n-i_0}) \Rightarrow 0 = a_{i_0} + a_{i_0-1}y + \cdots + a_n y^{n-i_0} \Rightarrow y \cdot \frac{1}{a_{i_0}}(a_{i_0+1} + \cdots + a_n y^{n-i_0-1}) = 1$. Weil $F[x] \supseteq F$ eine endliche, also algebraische Körpererweiterung ist und F algebraisch abgeschlossen, gilt $F[x] = F$ für alle $x \in D$, also $F = D$. □

Lemma. *Ist D ein Schiefkörper, so ist $Z(D)$ ein Körper.*

Beweis. $Z(D)$ ist ein Ring und kommutativ. $1, 0 \in Z(D)$. $x, y \in Z(D) \Rightarrow \forall d \in D\colon (x+y)d = xd + yd = dx + dy = d(x+y) \Rightarrow (x+y) \in Z(D)$ und $xyd = xdy = dxy \Rightarrow xy \in Z(D)$. Ist $0 \neq x \in Z(D)$, so ist $x^{-1} \in D$, da D ein Schiefkörper ist und für $d \in D$ gilt: $x^{-1}d = x^{-1}d(xx^{-1}) = x^{-1}xdx^{-1} = dx^{-1}$, also $x^{-1} \in Z(D)$. □

Satz. *Endliche Schiefkörper sind Körper, d.h. kommutativ.*

Beweis. Sei D ein endlicher Schiefkörper. Dann ist nach Lemma $F = Z(D)$ ein endlicher Körper. Sei $p = \operatorname{char} F > 0$ und $|F| = q = p^\ell$ für ein $\ell \geq 1$. D ist ein F-Vektorraum. Sei $n = \dim_F D \geq 1$. Dann hat D genau q^n Elemente. Ist $n = 1$, so ist $D = F$ und wir sind fertig. Nehmen wir also an, dass $n \geq 1$. Wir definieren eine Äquivalenzrelation auf $D^\times = D \setminus \{0\}$:

$$x \sim \tilde{x} \iff \exists y \in D^\times \colon yxy^{-1} = \tilde{x}$$

Die Äquivalenzklassen sind also die Bahnen der inneren Automorphismen der multiplikativen Gruppe $D^\times$. Sei $C(x) = \{\tilde{x} \in D^\times : \tilde{x} \sim x\}$ die Äquivalenzklasse von x. Es ist $C(x) = \{x\} \Leftrightarrow x \in F^\times = Z(D)^\times$. Seien $x_1, \ldots, x_s$ Repräsentanten der Äquivalenzklassen $C(x)$ mit $|C(x)| \geq 2$. Dann hat man eine disjunkte Vereinigung : $D^\times = F^\times \sqcup \bigsqcup_{i=1}^{s} C(x_i)$. Behauptung: Für alle $x \in D^\times$ ist $N(x) = \{y \in D^\times : yxy^{-1} = x\} \cup \{0\}$ ein Schiefkörper. Beweis: $0, 1 \in N(x)$. Ist $y \neq 0$ in $N(x)$, so gilt $yxy^{-1} = x \Leftrightarrow x = y^{-1}xy$, also $y^{-1} \in N(x)$. Sind $y, z \in N(x)$, so benutzen wir, dass $yxy^{-1} = x \Leftrightarrow yx = xy$, und damit $(y \dot{+} z)x = x(y \dot{+} z)$, also $y + z$ und $y \cdot z \in N(x)$. $N(x)$ ist ein Unter-F-Vektorraum von D, da $F \subseteq N(x)$ und D ist ein $N(x)$-Vektorraum und daher: $\dim_F N(x) = \delta(x)$ teilt n, denn $n = \dim_F D = \dim_{N(x)} D \cdot [N(x) : F]$ und $[N(x) : F] = \dim_F N(x)$. Also $|N(x)| = q^{\delta(x)}$ und $D^\times / N(x)^\times \cong C(x), y \mapsto yxy^{-1}$ (als Menge). Also

$$|C(x)| = \frac{q^n - 1}{q^{\delta(x)} - 1} \Rightarrow q^n - 1 = |D^\times| = q - 1 + \sum_{i=1}^{s} \frac{q^n - 1}{q^{\delta(x_i)} - 1} \qquad (**)$$

Sei nun $\Phi_n(T) = \prod_{\xi \in P_n}(T - \xi) \in \mathbb{Z}[T]$ das n-te Kreisteilungspolynom. Da $\delta(x_i) \mid n$ gilt: $\Phi_n(T)$ teilt $(T^n - 1)/(T^{\delta(x_i)} - 1)$ in $\mathbb{Z}[T]$. Also gilt nach $(**)$:

$$\Phi_n(q) \text{ teilt } \sum_{i=1}^{s} \frac{q^n - 1}{q^{\delta(x_i)} - 1} \text{ und } q^n - 1 \Longrightarrow \Phi_n(q) \mid q - 1$$

Dies ist aber unmöglich, da für eine n-te Einheitswurzel $\xi \neq 1$ gilt $|\xi - q| \gneq |1 - q| = q - 1$. □

Bemerkung. Dieser Satz geht auf Wedderburn (1882-1948) zurück, einem Schotten, studiert in Edinbourgh (bei Frobenius), Professor in Princeton, Doktorvater von Nathan Jacobson (1910 - 1999).

Erinnerung. Man muss Links- und Rechtsmoduln unterscheiden. Es existieren in nichtkommutativen Ringen:

— Linksideale I: $\forall x, y \in I, \lambda \in R$: $x + y, \lambda x \in I$.

— Rechtsideale I: $\forall x, y \in I, \lambda \in R$: $x + y, x\lambda \in I$.

— Zweiseitige Ideale (oder einfach Ideale) I: $\forall x, y \in I, \lambda \in R$: $x + y, \lambda x, x\lambda \in I$.

Beispiel. Sei F ein Körper, V ein F-Vektorraum, $f \in \mathrm{End}_F(V)$, $\lambda \in F$ und $v \in V$. Mit $vf := f(v)$ wird V dann zu einem $\mathrm{End}_F(V)$-Rechtsmodul, wobei die Linearität $f(\lambda v) = \lambda f(v)$ der Assoziativität $(\lambda v)f = \lambda(vf)$ im $\mathrm{End}_F(V)$-Modul entspricht.

Definition. Sei R ein Ring, A eine F-Algebra, F ein Körper.

(i) Ein R-Modul $M \neq (0)$ (links oder rechts) heißt *einfach*, wenn (0) und (M) die einzigen R-Untermoduln von M sind.

(ii) Der Ring $R \neq (0)$ heißt *einfach*, wenn (0) und R die einzigen zweiseitigen Ideale sind.

(iii) Die F-Algebra A heißt *zentral einfach*, wenn gilt
   (a) $\dim_F(A) < \infty$

(b) A ist einfach (als Ring)
(c) $F \to A, \lambda \mapsto \lambda 1$ ist ein Isomorphismus $F \to Z(A) = \{x \in A \colon \forall a \in A \colon ax = xa\}$

Definition. Sind A, B F-Algebren, so heißt eine F-lineare Abbildung $\alpha \colon A \to B$, die gleichzeitig ein Ringhomomorphismus ist, ein *F-Algebra-Homomorphismus.* α heißt *F-Algebra-Isomorphismus*, wenn α bijektiv ist.

Lemma 1 (Schur)**.** *Sei R ein Ring, M ein einfacher R-Modul, dann ist* $\mathrm{End}_R(M)$ *ein Schiefkörper.*

Beweis. Wir müssen zeigen, dass jedes $\alpha \neq 0$ aus $\mathrm{End}_R(M)$ bijektiv ist (wie in Linearer Algebra zeigt man, dass α^{-1} R-linear ist, wenn α dies ist). Sei $\alpha \colon M \to M$ R-linear, $\alpha \neq 0$. Dann $\operatorname{Ker} \alpha \neq M$, also $\operatorname{Ker} \alpha = (0)$, da $\operatorname{Ker} \alpha$ ein R-Untermodul und M ein einfacher R-Modul ist. Also ist α injektiv. Desweiteren ist $\operatorname{Im} \alpha \neq (0)$, also $\operatorname{Im} \alpha = M$, da M einfach und $\operatorname{Im} \alpha$ ein R-Untermodul ist. Somit ist α auch surjektiv. □

Lemma 2. *Ist $M \cong M_1 \oplus M_2$ für R-Moduln M, M_1, M_2, so ist*

$$\mathrm{End}_R(M) \cong \begin{pmatrix} \mathrm{End}_R(M_1) & \mathrm{Hom}_R(M_2, M_1) \\ \mathrm{Hom}_R(M_1, M_2) & \mathrm{End}_R(M_2) \end{pmatrix} = \left\{ \begin{pmatrix} f & g \\ h & i \end{pmatrix} : \begin{array}{c} f \in \mathrm{End}_R(M_1) \\ g \in \mathrm{Hom}_R(M_2, M_1) \\ h \in \mathrm{Hom}_R(M_1, M_2) \\ i \in \mathrm{End}_R(M_2) \end{array} \right\}$$

Insbesondere: Ist $M \cong \underbrace{N \oplus \cdots \oplus N}_{\nu \text{ mal}}$ und $A = \mathrm{End}_R(N)$, so ist $\mathrm{End}_R(M) \cong M_\nu(A)$.

Beweis. Sei $\alpha \colon M \to M_1 \oplus M_2$ der R-Modul-Isomorphismus. Dann gibt $f \mapsto \alpha \circ f \circ \alpha^{-1}$ einen Isomorphismus $\mathrm{Hom}_R(M, M) \to \mathrm{Hom}_R(M_1 \oplus M_2, M_1 \oplus M_2)$. Sei o.E. $M = M_1 \oplus M_2$. Seien $p_i \colon M \to M_i$ und $j_i \colon M_i \to M$ die zugehörigen Projektionen und Injektionen, dann ist $p_i \circ j_i = \mathrm{id}_{M_i}$, $j_1 \circ p_1 + j_2 \circ p_2 = \mathrm{id}_M$, $p_1 \circ j_2 = 0 = p_2 \circ j_1$. □

Bemerkung. Ist F ein Körper, so ist $\mathrm{End}_F(F) \cong F$ über den Isomorphismus $F \to \mathrm{End}_F(F), \lambda \mapsto \ell_\lambda$ mit $\ell_\lambda \colon y \mapsto \lambda y$.

Satz. *Ist A eine zentral einfache F-Algebra, so existiert ein Schiefkörper D, der eine zentral einfache F-Algebra ist (so ein D nennt man auch F-Divisionsalgebra) mit $A \cong M_\ell(D)$ als F-Algebra für ein $\ell \in \mathbb{N}$.*

Beweis. Sei A eine zentral einfache F-Algebra. Da A endlich dimensional ist, existiert ein minimales Rechtsideal I von A, d.h. ein Rechtsideal I, welches ein einfacher A-Rechtsmodul ist. $AI = \{\sum x_i y_i \colon x_i \in A, y_i \in I\}$ ist ein zweiseitiges Ideal und $\neq (0)$, da $1 \in A$. Weil A einfach ist, muss dann $AI = A$ gelten. Insbesondere existieren dann $y_1, \ldots, y_\ell \in I$ mit $1 \in \sum_{i=1}^{\ell} Ay_i$. Wir wählen dieses ℓ minimal. Dann gilt:

(i) $\alpha_i \colon I \to x_i I, \lambda \mapsto x_i \lambda$ ist ein Isomorphismus von A-Rechtsmoduln.
(ii) $\sum_{i=1}^{\ell} x_i I$ ist eine direkte Summe, also $A = \bigoplus_{i=1}^{\ell} x_i I$.

Beweis für (i) und (ii):

(i) Wäre $x_i I = 0$, so $1 \in \sum_{j=1, j\neq i}^{\ell} x_j I$ im Widerspruch zur Minimalität von ℓ. Also $\alpha_i \neq 0$, also $\operatorname{Ker} \alpha_i \neq I$, und damit $\operatorname{Ker} \alpha_i = 0$, da I ein einfacher A-Rechtsmodul ist, also ist α_i injektiv. Weil α_i auch surjektiv ist, ist α_i ein Isomorphismus.

(ii) Wegen $1 \in \sum_{i=1}^{\ell} x_i I$ existieren $y_1, \ldots, y_\ell \in I$ mit $1 = \sum_{i=1}^{\ell} x_i y_i$, also gilt für alle $a \in A$, dass $a = 1a = \sum_{i=1}^{\ell} x_i y_i a \in \sum_{i=1}^{\ell} x_i I$, also $A = \sum_{i=1}^{\ell} x_i I$. Die Summe ist direkt, d.h. $\forall s \in \{1, \ldots, \ell\}$ gilt $x_s I \cap \sum_{i=1, i\neq s}^{\ell} x_i I = (0)$. Angenommen es existiert $1 \leq s \leq \ell$ mit $x_s I \cap \sum_{i=1, i\neq s}^{\ell} x_i I = N \neq (0)$. N ist dann ein A-Untermodul von $x_s I$. Nach (i) ist $x_s I$ einfach. Also $N = x_s I$, da $N \neq (0)$, also $x_s I \subseteq \sum_{i=1, i\neq s}^{\ell} x_i I$. Daraus folgt $1 \in \sum_{i=1, i\neq s}^{\ell} x_i I$, was wieder der Minimalität von ℓ widerspricht.

Also

$$A \cong \bigoplus_{i=1}^{\ell} x_i I \cong \underbrace{I \oplus \cdots \oplus I}_{\ell \text{ mal}}, \sum_{i=1}^{\ell} x_i \lambda_i \leftarrow\!\shortmid (\lambda_1, \ldots, \lambda_\ell)$$

und damit $\operatorname{End}_A(A) \cong \operatorname{End}_A(I^\ell) \cong M_\ell(\operatorname{End}_A(I)) = M_\ell(D)$ mit $D = \operatorname{End}_A(I)$ Schiefkörper nach Schurs Lemma. Daraus folgt der Satz, da $D \to M_\ell(D), \lambda \mapsto \lambda I$ einen Isomorphismus $Z(D) \cong Z(M_\ell(D))$ gibt (Übung) und $A \to \operatorname{End}_A(A), a \mapsto \{\ell_a \colon x \mapsto a.x\}$ ein Ringhomomorphismus $\neq 0$ ist,und injektiv, da aus $\ell_a = 0$ folgt, dass $0 = \ell_a(1) = a.1 = a$, sowie surjektiv, weil für alle $f \in \operatorname{End}_A(A)$ gilt $f(a) = f(1.a) = f(1).a = \ell_{f(1)}(a)$. □

Bemerkung.

— Der Satz geht wiederum auf Wedderburn zurück. Verallgemeinert wurde er von Emil Artin (1898-1962).

— Das D und somit aus Dimensionsgründen ℓ sind eindeutig bis auf Isomorphie.

— $M_\ell(D)$ ist einfach für alle Schiefkörper D und zentral einfach über $Z(D)$, wenn D von endlicher Dimension über $Z(D)$ ist.

6 Algebraisch abgeschlossene Körper

Bemerkung. Folgende Aussagen sind äquivalent für einen Körper k.

i) k ist algebraisch abgeschlossen, d.h. jedes $f \in k[X] \setminus k$ zerfällt in $k[X]$ in Linearfaktoren, d.h. $f = c \prod_{i=1}^{n} (X - b_i)$ mit $c, b_1, \ldots, b_n \in k$.

ii) Jedes $f \in k[X] \setminus k$ hat in k mindestens eine Nullstelle.

iii) Für jedes $f \in k[X]$ gilt: f irreduzibel $\Rightarrow \deg(f) = 1$.

iv) Für jeden Oberkörper K von k gilt: Ist $k \subseteq K$ algebraisch, dann $k = K$.

Beweis. Übung. In i) kann man $f \neq 0$ statt $f \notin k$ verlangen. In ii) kann man f als irreduzibel voraussetzen. In iv) kann man $k \subseteq K$ als endlich voraussetzen.

Satz (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Beweis nach Artin. Es reicht zu zeigen: $(*)$ Für jede Körpererweiterung $\mathbb{C} \subseteq K$ gilt: Ist $\mathbb{R} \subseteq K$ galoissch, so ist $\mathbb{C} = K$. Aus $(*)$ folgt nämlich die Behauptung des Satzes: Zu $f \in \mathbb{C}[X] \setminus \mathbb{C}$ nehme den Zerfällungskörper L über $\mathbb{C}$. Da $\mathbb{R} \subseteq \mathbb{C} \subseteq L$ beide endlich (und separabel) sind, gibt es eine Erweiterung $L \subseteq K$ mit $\mathbb{R} \subseteq K$ galoissch. Nach $(*)$ is $\mathbb{C} = K$, also auch $\mathbb{C} = L$, d.h. f zerfällt in $\mathbb{C}[X]$ in Linearfaktoren. Bleibt also zu zeigen, dass $(*)$ gilt. Dazu wähle eine 2-Sylowuntergruppe H von $G = \mathrm{Gal}(K/\mathbb{R})$. Da $L = \mathrm{Fix}_K(H)$ endlich (und separabel) über $\mathbb{R}$ ist, gibt es $a \in L$ mit $\mathbb{R}(a) = L$ (Satz vom primitiven Element). Für das Minimalpolynom f von a über $\mathbb{R}$ ist $\deg(f) = [\mathbb{R}(a) : \mathbb{R}] = [L : \mathbb{R}] = [G : H]$ ungerade nach Sylow, weshalb f eine Nullstelle in $\mathbb{R}$ hat (Zwischenwertsatz). Es folgt $\deg(f) = 1$, d.h. $G = H$, also ist G eine 2-Gruppe. Wäre $\mathbb{C} \subsetneq K$, so wäre $G' := \mathrm{Gal}(K/\mathbb{C}) = \{e\}$, hätte also nach dem Satz von Wielandt eine Untergruppe H' mit $[G' : H'] = 2$. (Hier: Wielandt für $d = 2^\ell$, $|G^i| = 2^{\ell+1}$. Beachte, dass G' als Untergruppe von G eine 2-Gruppe ist.) Für $L' = \mathrm{Fix}_K(H')$ wäre dann $[L' : \mathbb{C}] = 2$, also $L' = \mathbb{C}(b)$ für ein beliebiges $b \in L' \setminus \mathbb{C}$. Für das Minimalpolynom g von b über $\mathbb{C}$ wäre $\deg(g) = 2$, also (!) zerfiele g in $\mathbb{C}[X]$ in Linearfaktoren, was unmöglich ist. Noch zu (!): Für $g = X^2 + wX + z$ mit $w, z = \mathbb{C}$ ist $g = (X + w/2)^2 - (w^2/4 - z)$. Es gibt $c \in \mathbb{C}$ mit $c^2 = w^2/4 - z$, wofür $g = (X + w/2 + c)(X + w/2 - c)$. □

Korollar 6. *Für jedes $f \in \mathbb{R}[X]$ gilt: f irreduzibel $\Longrightarrow \deg(f) \in \{1, 2\}$.*

Beweis. Nach dem Satz gibt es ein $a \in \mathbb{C}$ mit $f(a) = 0$, wovon f das Minimalpolynom über $\mathbb{R}$ ist, also $\deg(f) = [\mathbb{R}(a) : \mathbb{R}]$. Betrachte die Fälle $a \in \mathbb{R}$, $a \notin \mathbb{R}$. □

Erinnerung. Ist $k \subseteq K$ eine Körpererweiterung, so ist der ganze Abschluss $\overline{k} = \{a \in K : a \text{ ganz über } k\}$ ein Unterkörper von K und $\overline{k}$ ist in K ganz abgeschlossen, d.h. ist $a \in K$ ganz über $\overline{k}$, so ist bereits $a \in \overline{k}$. Ferner: $\overline{k} = \{a \in K : a \text{ algebraisch über } k\}$.

Korollar 7. *Der Körper $\mathbb{A} = \{a \in \mathbb{C} : a \text{ algebraisch über } \mathbb{Q}\}$ der algebraischen Zahlen ist algebraisch abgeschlossen.*

Beweis. Zu $f \in \mathbb{A}[X] \setminus \mathbb{A} \subseteq \mathbb{C}[X] \setminus \mathbb{C}$ gibt es nach Satz ein $a \in \mathbb{C}$ mit $f(a) = 0$. Speziell ist $a \in \mathbb{C}$ ganz über $\mathbb{A}$, also $a \in \mathbb{A}$ wie oben. □

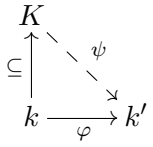
Definition. Ist $k \subseteq K$ eine algebraische Körpererweiterung, und ist K algebraisch abgeschlossen, so heißt K ein *algebraischer Abschuss* von k. Ein solches K ist durch k bis auf Isomorphie eindeutig bestimmt (s.u.!)

Beispiel.

a) Der algebraische Abschluss von $\mathbb{R}$ ist $\mathbb{C}$.

b) Der algebraische Abschluss von $\mathbb{Q}$ ist $\mathbb{A}$.

Satz (ZL). *Es seien k, k' Körper. Ist $\varphi : k \to k'$ ein Ringhomomorphismus, und ist k' algebraisch abgeschlossen, so gibt es zu jeder algebraischen Erweiterung $k \subseteq K$ einen Ringhomomorphismus $\psi : K \to k'$ mit $\psi|_k = \varphi$, d.h. folgendes Diagramm kommutiert:*



Beweis. Schon gezeigt für $k \subseteq K$ endlich (+). Im allgemeinen Fall sei Ω die Menge aller (L, f), worin L ein Zwischenkörper von $k \subseteq K$ und $f\colon L \to k'$ ein Ringhomomorphismus mit $f|_k = \varphi$ ist. Wegen $(k, \varphi) \in \Omega$ ist $\Omega \neq \varnothing$. Durch

$$(L_1, f_1) \leq (L_2, f_2) :\Longleftrightarrow L_1 \subseteq L_2 \wedge f_1 = f_2|_{L_1}$$

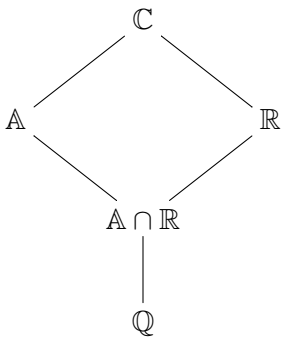
wird Ω induktiv geordnet, denn: Ist $T = \{(L_i, f_i)\colon i \in I\}$ eine Kette in Ω, so ist $L := \bigcup_{i\in I} L_i$ ein Zwischenkörper von $k \subseteq K$, und durch $f(x) := f_i(x)$ für $x \in L_i$ wird ein Ringhomomorphismus $f\colon L \to k'$ mit $f|_k = \varphi$ definiert. [Ist $x \in L_i \cap L_j$, etwa $(L_i, f_i) \leq (L_j, f_j)$, so ist $f_i(x) = f_j(x)$] Also: $(L, f) \in \Omega$ und (L, f) ist eine obere Schranke von T. Nach Zorn hat Ω ein maximales Element (M, ψ), für welches $M = K$ ist, denn: für $x \in K$ ist $M \subseteq M(x)$ endlich [da x sogar algebraisch über k ist nach Voraussetzung], also gibt es nach (+) einen Ringhomomorphismus $g\colon M(x) \to k'$ mit $g|_M = \psi$, d.h. $(M, \psi) \leq (M(x), g) \in \Omega$, also $(M, \psi) = (M(x), g)$ [da (M, ψ) ein maximales Element von Ω ist], speziell $M = M(x)$, d.h. $x \in M$ wie gewünscht. □

Korollar 1. *Jede algebraische Erweiterung K des Körpers k lässt sich in den algebraischen Abschluss k' von k einbetten, d.h. es gibt einen Ringhomomorphismus $\psi\colon K \to k'$ mit $\psi(x) = x$ für alle $x \in k$.*

Korollar 2. *Je zwei algebraische Abschlüsse E_1, E_2 eines Körpers k sind über k isomorph, d.h. es gibt einen Isomorphismus $\psi\colon E_1 \to E_2$ mit $\psi(x) = x$ für alle $x \in k$.*

Beweis. Da E_1/k algebraisch und E_2 algebraisch abgeschlossen ist, gibt es nach Satz einen Ringhomomorphismus $\psi\colon E_1 \to E_2$ mit $\psi(x) = x$ für alle $x \in k$. Nun ist ψ injektiv. Also $E_1 \cong_\psi \operatorname{Im}(\psi)$. Da E_1 algebraisch abgeschlossen ist, ist auch $\operatorname{Im}(\psi)$ algebraisch abgeschlossen. Da E_2/k algebraisch ist, ist $E_2/\operatorname{Im}(\psi)$ algebraisch, also $E_2 = \operatorname{Im}(\psi)$, d.h. ψ surjektiv. □

Wieder sei $\mathbb{A}$ der Körper der algebraischen Zahlen. Er ist ein Zwischenkörper von $\mathbb{Q} \subseteq \mathbb{C}$, genauer ist $\mathbb{A}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Ferner umfasst $\mathbb{A}$ den Körper $\mathbb{K}$ der mit Zirkel und Lineal konstruierbaren Zahlen $a \in \mathbb{C}$, denn geht $a \in \mathbb{C}$ durch einen elementaren Konstruktionsschritt aus $M \subseteq \mathbb{A}$ hervor, so ist $a \in \mathbb{A}$ [nach einem Lemma für $L = \mathbb{A}$ gibt es $b \in \mathbb{C}$ mit $a \in \mathbb{A}(b)$ und $b^2 \in \mathbb{A}$, d.h. $b \in \mathbb{A}$].



Für jedes $z \in \mathbb{A}$ sind auch $\overline{a}$, $\operatorname{Re}(z)$, $\operatorname{Im}(z)$ und $|z|$ algebraisch über $\mathbb{Q}$. Für den Körper $\mathbb{A} \cap \mathbb{R}$ der *reell-algebraischen Zahlen* gilt $\mathbb{A} = (\mathbb{A} \cap \mathbb{R})(i)$, denn für $z \in \mathbb{A}$ is $z = x + iy \in$

$(\mathbb{A} \cap \mathbb{R})(i)$ mit $x = \mathrm{Re}(z)$ und $y = \mathrm{Im}(z)$. Speziell ist $\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A}$ eine Galoiserweiterung vom Grad 2 und $\mathbb{A}$ der Zerfällungskörper von $X^2 + 1$ über $\mathbb{A} \cap \mathbb{R}$.

Es sei k ein Körper. Zu jedem $f \in k[X] \setminus k$ gibt es eine endliche Körpererweiterung $k \subseteq K$, so dass f in K eine Nullstelle a hat. Nach Kronecker kann man erreichen, dass f in $K[X]$ in Linearfaktoren zerfällt. Dies beweist man durch Induktion nach $\deg(f)$: Nehme einen irreduziblen Teiler f_0 von f und setze $K = k[X]/(f_0)$; beachte $(f_0) \supseteq (f)$. Alternativ wähle, mit Lemma von Zorn, ein maximales Ideal $M \supseteq (f)$ und setze $K = k[X]/M$. Bei beiden methoden ist K ein Oberkörper von k und $a = \overline{X}$ eine Nullstelle von f in K [man hat $k[X]/(f) \to K$].

Lemma (ZL) (Kleiner Satz von Steinitz)**.** *Zu jedem Körper k gibt es eine algebraische Erweiterung $k \subseteq K$, so dass jedes $f \in k[X] \setminus k$ eine Nullstelle in K hat.*

Beweis. Es sei $F = k[X] \setminus k$ und $R = k[X_f \colon f \in F]$, d.h. R ist der Polynomring über k in den (unendlich vielen) Unbestimmten X_f, $f \in F$, d.h. R besteht aus den k-Linearkombinationen der Monome von der Art $X_{f_1}^{l_1} \dots X_{f_m}^{l_m}$ mit $m \geq 1$, $f_i \in F$, $l_i \geq 0$. Ferner entstehe $f(X_f) \in R$ aus $f \in F$, indem man X durch X_f ersetzt, d.h. mit $f = \sum_{i=0}^{n} c_i X^i \in F$ ist $f(X_f) = \sum_{i=0}^{n} c_i X_f^i \in R$ (alle $x_i \in k$). Für das von $f(X_f)$ mit $f \in F$ erzeugte Ideal $I = (f(X_f) \colon f \in F)$ gilt $I \subsetneq R$, denn sonst wäre $1_R \in I$, d.h. $1_R = \sum_{j=1}^{m} r_j f_j(X_{f_j})$ $(*)$ für $r_j \in R$ und $f_j \in F$. Nach Kronekcer gäbe es dazu eine endliche Körpererweiterung $k \subseteq L$ und $a_1, \dots, a_m \in L$ mit $f_j(a_j) = 0$ für alle $1 \leq j \leq m$. Durch Anwenden des k-linearen Ringhomomorphismus $\varphi \colon R \to L$ mit

$$\varphi(X_f) = \begin{cases} a_j & \text{falls } f = f_j \\ 0 & \text{sonst} \end{cases}$$

für $f \in F$ auf $(*)$ erhielte man für $s_j \in L$

$$1_L = \sum_{j=1}^{m} s_j f_j(a_j) = 0_L,$$

was unmöglich ist. Nach Zorn liegt also I in einem maximalen Ideal M von R, wofür $K = R/M$ ein Oberkörper von k ist. Für jedes $f \in F$ ist $f(X_f) \in I \subseteq M$, also $\overline{X_f}$ Nullstelle von f in K; speziell ist $\overline{X_f}$ algebraisch über k. Es folgt, dass $K = k(\overline{X_f} \colon f \in F)$ algebraisch über k ist. □

Satz (ZL) (Steinitz)**.** *Jeder Körper k hat einen algebraischen Abschluss K.*

Beweis. Nach Lemma kann man k sukzessive zu Körpern $k = k_0 \subseteq k_2 \subseteq \dots$ erweitern, so dass für jedes $n \geq 0$, $k_n \subseteq k_{n+1}$ algebraisch ist und jedes $f \in k_n[X] \setminus k_n$ eine Nullstelle in k_{n+1} hat. Nun ist $K = \bigcup_{i=0}^{\infty} k_i$ ein Oberkörper von k; jedes $a \in K$ liegt in einem k_n, ist also algebraisch über k, weshalb K algebraisch über k ist. Jedes $f \in K[X] \setminus K$ liegt in einem $k_n[X] \setminus k_n$, hat also eine Nullstelle in $k_{n+1} \subseteq K$, d.h. K ist algebraisch abgeschlossen. □

Beispiel. Für den algebraischen Abschluss K von $k = \mathbb{F}_p$ hat man $\mathbb{F}_{p^n} \hookrightarrow K$ für $n \geq 1$. Für jedes $a \in K$ ist $k(a)$ endlich über k, also $k(a)$ ein endlicher Körper der Charakteristik p, d.h. $k(a) \simeq \mathbb{F}_{p^n}$ für $n = [k(a) : k]$. In diesem Sinne ist

$$K = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$$

7 Varietäten

7.1 Algebraische Mengen

Definition. Es sei k ein Körper und $n \geq 1$. Wir setzen $R_n = k[X_1, \ldots, X_n]$. Für $S \subseteq R_n$ heißt $V(S) = \{p \in k^n \colon \forall f \in S \colon f(p) = 0\}$ die *Nullstellenmenge* oder die *Varietät* von S. Ein $A \subseteq k^n$ heißt algebraische Menge, wenn $A = V(S)$ ist für ein $S \subseteq R_n$. Für $f \in R_n \setminus k$ nennt man $V(f) = V(\{f\})$ eine *Hyperfläche* in k^n. Im Fall $n = 2$ sind die Hyperflächen die *ebenen algebraischen Kurven.*

Beispiel. Ebene algebraische Kurven für $k = \mathbb{R}$:

Definition. Für $A \subseteq k^n$ heißt $I(A) = \{f \in R_n \colon \forall p \in A \colon f(p) = 0\}$ das *Verschwindungsideal* von A (es ist ein Ideal!), sowie $k[A] = R_n/I(A)$ der *Koordinatenring* von A.

Einschub. Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale eines kommutativen Rings R. Neben $\mathfrak{a} \cap \mathfrak{b}$ ist $\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=1}^{m} f_i g_i \colon m \geq 1, \forall i \colon f_i \in \mathfrak{a}, g_i \in \mathfrak{b}\}$ ein Ideal von R mit $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Das *Radikal* $\sqrt{\mathfrak{a}} = \{f \in R \colon \exists m \geq 1 \colon f^m \in \mathfrak{a}\}$ ist ein Ideal von R. Man nennt $\mathfrak{b}$ ein *Radikalideal*, wenn $\mathfrak{b} = \sqrt{\mathfrak{b}}$. Damit ist $\sqrt{\mathfrak{a}}$ das kleinste Radikalideal von R, welches $\mathfrak{a}$ umfasst, d.h. es gilt $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ und $\sqrt{\mathfrak{a}} = \sqrt{\sqrt{\mathfrak{a}}}$, und für $\mathfrak{b} = \sqrt{\mathfrak{b}}$ gilt $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \sqrt{\mathfrak{a}} \subseteq \mathfrak{b}$. Allgemein gilt $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$. Jedes Primideal ist ein Radikalideal, und mit dem Zornschen Lemma gilt $\sqrt{\mathfrak{a}} = \bigcap\{\mathfrak{p} \subseteq R \colon \mathfrak{p} \text{ Primideal}, \mathfrak{a} \subseteq \mathfrak{p}\}$ (Übung, eventuell später).

Lemma (Eigenschaften von V und I)**.**

0) $S \subseteq T \Rightarrow V(S) \supseteq V(T)$; $A \subseteq B \Rightarrow I(A) \supseteq I(B)$
1) a) $V(\varnothing) = V(0) = k^n$; $V(R_n) = V(1) = \varnothing$
b) $V(\bigcup_{\lambda \in \Lambda} S_\lambda) = \bigcap_{\lambda \in \Lambda} V(S_\lambda)$
c) Für $p = (t_1, \ldots, t_n) \in k^n$ *ist* $\{p\} = V(X_1 - t_1, \ldots, X_n - t_n)$.
2) a) Für $\mathfrak{a} = (S)$ *ist* $V(\mathfrak{a}) = V(S)$.
b) Für Ideale $\mathfrak{a}, \mathfrak{b}$ *von* R_n *ist* $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.
c) Für jedes Ideal $\mathfrak{a}$ *von* R_n *ist* $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.
3) Jede algebraische Menge $A \subseteq k^n$ *ist Durchschnitt endlich vieler Hyperflächen. Man weiß: Es genügen* n *Hyperflächen. (Eisenbud-Evans 1973, Storch 1972).*
4) a) $S \subseteq IV(S)$, $V(S) = VIV(S)$ *für* $S \subseteq R_n$.
b) $A \subseteq VI(A), I(A) = IVI(A)$ *für* $A \subseteq k^n$.
5) a) $I(\varnothing) = R_n$
b) $I(\bigcup_{\lambda \in \Lambda} A_\lambda) = \bigcap_{\lambda \in \Lambda}(A_\lambda)$

c) Für $p = (t_1, \ldots, t_n) \in k^n$ ist $I(p) \overset{(*)}{=} (X_1 - t_1, \ldots, X_n - t_n)$, und dies ist ein maximales Ideal von R_n. Insbesondere ist $I(A)$ für jedes $A \subseteq k^n$ Durchschnitt von maximalen Idealen, nämlich $I(A) = I(\bigcup_{p\in A}\{p\}) = \bigcap_{p\in A} I(p)$.

6) $I(k^n) = 0 \iff k$ unendlich.

Insbesondere sind endliche Vereinigungen und beliebige Schnitte von algebraischen Mengen wieder algebraische Mengen. Neben k^n und $\varnothing$ sind alle endlichen Teilmengen von k^n algebraisch. Die algebraischen Mengen in k^n sind also die abgeschlossenen Mengen einer Topologie auf k^n, der Zariski-Topologie. *Für $k = \mathbb{R}$ oder $k = \mathbb{C}$ ist sie gröber als die euklidische Topologie.*

Es gilt $B = VI(B)$ für jedes algebraische Menge B in k^n. Allgemein ist $\overline{A} = VI(A)$ für jedes $A \subseteq k^n$ die kleinste algebraische Menge in k^n, welche A umfasst, mit anderen Worten: $\overline{A}$ ist der Abschluss von A bzgl. der Zariski-Topologie.

Beweis von (2).

a) Wegen $S \subseteq \mathfrak{a}$ ist $V(S) \supseteq V(\mathfrak{a})$, worin „=“ gilt wie folgt: Ist $p \in V(S)$ und $f \in \mathfrak{a}$, d.h. $f = \sum_{i=1}^m g_i h_i$, $m \geq 1$, $g_i \in R_n$, $h_i \in S$, so ist $f(p) = \sum g_i(p)h_i(p) = 0$, also $p \in V(\mathfrak{a})$.

b) Wegen $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cup \mathfrak{b} \subseteq \left\{\begin{smallmatrix}\mathfrak{a}\\ \mathfrak{b}\end{smallmatrix}\right\}$ ist $V(\mathfrak{a}\mathfrak{b}) \supseteq V(\mathfrak{a} \cap \mathfrak{b}) \supseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$, worin „=“ gilt wie folgt: Ist $p \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$, d.h. $p \notin V(\mathfrak{a}) \wedge p \notin V(\mathfrak{b})$, d.h. $f(p) \neq 0$ und $g(p) \neq 0$ für ein $f \in \mathfrak{a}$ und ein $g \in \mathfrak{b}$, so ist $fg(p) = f(p)g(p) \neq 0$ mit $fg \in \mathfrak{a}\mathfrak{b}$, also $p \notin V(\mathfrak{a}\mathfrak{b})$.

c) Wegen $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ gilt $V(\mathfrak{a}) \supseteq V(\sqrt{\mathfrak{a}})$, worin „=“ gilt wie folgt: Ist $p \in V(\mathfrak{a})$ und $f \in \sqrt{\mathfrak{a}}$, etwa $f^m \in \mathfrak{a}$ mit $m \geq 1$, so ist $f(p)^n = f^n(p) = 0$, also $f(p) = 0$. □

Beweis von (3). Für $A = \varnothing$ ist z.B. $A = V(X_1) \cap V(X_1 - 1)$. Für $A = k^n$ ist $A = \bigcap \varnothing$. Für $A \notin \{\varnothing, k^n\}$ ist $A = V(\mathfrak{a})$ mit $\mathfrak{a} \notin \{0, R\}$. Nach Hilberts Basissatz ist R_n noethersch, also $\mathfrak{a} = (f_1, \ldots, f_m)$ mit $m \geq 1$ und $f_i \notin k$ und damit $A = V(\mathfrak{a}) = V(\{f_1, \ldots, f_m\}) = \bigcup_{i=1}^m V(f_i)$. □

Beweis von (4). „$\subseteq$“ ist klar für a) und b). Noch zu „=“: Nur a), b) geht analog: Aus $S \subseteq IV(S)$ folgt $V(S) \supseteq VIV(S)$, worin Gleichheit gilt wegen $A \subseteq VI(A)$ für $A = V(S)$. Da $A \subseteq \overline{A}$, $\overline{A}$ algebraisch ist und $A \subseteq B$, B algebraisch $\Rightarrow I(A) \supseteq I(B) \Rightarrow \overline{A} = VI(A) \subseteq VI(B) = B$, ist $\overline{A}$ tatsächlich der Abschluss von A in der Zariski-Topologie. □

Beweis von (5). nur c) („maximales Ideal“): Der Homomorphismus $R_n \to k, f \mapsto f(p)$ ist surjektiv mit Kern $I(p)$, weshalb $R_n/I(p) \cong k$ ein Körper ist, d.h. $I(p)$ ist ein maximales Ideal von R_n. In $(*)$ ist „$\supseteq$“ klar. Noch zu „$\subseteq$“: Allgemein gilt (!): Zu $f \in R_n$ gibt es $f_1, \ldots, f_n \in R_n$ mit $f = f(p)\ddot{u}\sum_{i=1}^n f_i(X_i - t_i)$. Ist also $f(p) = 0$, so ist $f = \sum_{i=1}^n f : i(X_i - t_i)$ wie verlangt. Noch zu (!): Induktion nach n: $n = 1$: Division mit Rest von $f(p)$ durch $X_1 - t_1$. $n \geq 2$: Division mit Rest von g durch $X_n - t_n$ liefert $f = g + f_n(X_n - t_n)$ mit $\deg_{X_n}(g) = \deg_{X_n}(X_n - t_n) = 1$, d.h. $g \in R_{n-1}$, also (Induktion) $g = g(p') + \sum_{i=1}^{n-1} f_i(X_i - t_i)$ mit $p' = (t_1, \ldots, t_{n-1})$, wofür $g(p') = g(p) = f(p)$. □

Beweis von (6). „$\Rightarrow$“: k endlich $\Rightarrow 0 \neq \prod_{t\in k}(X_1 - t) \in I(k^n)$. „$\Leftarrow$“: Induktion nach n. $n = 1$: $f \in I(k) \Rightarrow f = 0$. $n > 1$: Es sei $f \in I(k^n)$. Für $t \in k$ ist $f_t = f(X, 1, \ldots, X_{n-1}, t) \in I(k^{n-1})$. Nach Induktion ist $f_t = 0$ in R_{n-1}. Damit hat $f \in R_{n-1}[X_n]$ unendlich viele Nullstellen in R_{n-1}, nämlich alle $t \in k$. Es folgt $f = 0$. □

Bemerkung. Jede absteigende Folge $A_0 \supseteq A_1 \supseteq \ldots$ algebraischer Mengen wird stationär.

Beweis. $I(A_0) \subseteq I(A_1) \subseteq \ldots$ ist eine Folge von Idealen im noetherschen Ring R_n. Es gibt also ein $N \geq 0$ mit $I(A_N) = I(A_{N+1}) = \ldots$, wofür $VI(A_N) = VI(A_{N+1}) = \ldots$, d.h. $A_N = A_{N+1} = \ldots$ ist. □

Definition. Eine algebraische Menge A in k^n ist *irreduzibel*, wenn $A \neq \varnothing$ ist und wenn für algebraische Mengen B, C in k^n aus $A = B \cup C$ folgt $A = B$ oder $A = C$.

Lemma. *Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale eines kommutativen Rings R. Für jedes Primideal $\mathfrak{p}$ von R gilt: $\mathfrak{ab} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \vee \mathfrak{b} \subseteq \mathfrak{p}$. Die Voraussetzung $\mathfrak{ab} \subseteq \mathfrak{p}$ ist z.B. dann erfüllt, wenn sogar $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$.*

Beweis. Es sei $\mathfrak{ab} \subseteq \mathfrak{p}$ und $\mathfrak{p}$ ein Primideal. Der Fall $\mathfrak{a} \subseteq \mathfrak{p}$ ist klar. Nehmen wir also an, dass $\mathfrak{a} \not\subseteq \mathfrak{p}$, d.h. es gibt $f \in \mathfrak{a} \setminus \mathfrak{p}$. Dann ist $\mathfrak{b} \subseteq \mathfrak{p}$, denn: Für $g \in \mathfrak{b}$ ist $fg \in \mathfrak{ab} \subseteq \mathfrak{p}$, also $g \in \mathfrak{b}$, da $\mathfrak{p}$ ein Primideal ist. □

Bemerkung. Für jede algebraische Menge A in k^n gilt: A irreduzibel $\Longleftrightarrow$ $I(A)$ ist Primideal von R_n.

Beweis. Es gilt: $A \neq \varnothing \Leftrightarrow I(A) \neq R_n$. „⇒“: Es sei A irreduzibel und $f, g \in R_n$. Ist $fg \in I(A)$, so ist $V(fg) \supseteq VI(A) = A$, also $V(f) \cup V(g) \supseteq A$ und damit $(A \cap V(f)) \cup (A \cap V(g)) = A$. Beide vereinigte Mengen sind algebraisch, also ist nach Voraussetzung etwa $A \cap V(f) = A$, d.h. $V(f) \supseteq A$, d.h. $f \in I(A)$. „⇐“: Es sei $I(A)$ ein Primideal. Ist $A = B \cup C$ mit B, C algebraisch, so ist $I(A) = I(B) \cap I(C)$, mit dem Lemma ist etwa $I(A) = I(B)$, also $A = B$. □

Folgerung. k^n irreduzibel $\Longleftrightarrow$ k unendlich.

Beweis. „⇒“ k endlich $\Rightarrow k^n = \bigcup_{p \in k^n} V(p)$ reduzibel (oder $k^n = V(X_1) \dot\cup \bigcup_{t \in k^\times} V(X_1 - t) \cdots$). „⇐“ k unendlich $\Rightarrow I(k^n) = 0$, also ist $I(k^n)$ ein Primideal im Integritätsring R_n, weshalb k^n nach Bemerkung irreduzibel ist. □

Definition. Eine algebraische Menge B in k^n heißt *irreduzible Komponente* einer algebraischen Menge A in k^n, wenn B maximale irreduzible Teilmenge von A ist, das heißt B irreduzibel, $B \subseteq A$, und für C irreduzibel mit $C \subseteq A$ gilt: $B \subseteq C \Rightarrow B = C$.

Satz (Zerlegung in irreduzible Komponenten)**.** *Es sei A eine algebraische Menge in k^n.*

a) A hat nur endlich viele irreduzible Komponenten.
b) Jede irreduzible Teilmenge von A liegt in einer irreduziblen Komponente von A.
c) A ist die Vereinigung seiner irreduziblen Komponenten.

Beweis. Behauptung: A ist Vereinigung endlich vieler seiner irreduzibler Teilmengen ($\Diamond$). Damit: Ist $A = A_1 \cup \cdots \cup A_m$ mit A_i irreduzibel für $1 \leq i \leq m$ und o.B.d.A. $A_i \not\subseteq A_j$ für $i \neq j$, und ist C irreduzibel, $C \subseteq A$, so ist $C = (C \cap A_1) \cup \cdots \cup (C \cap A_m)$. Also $C = C \cap A_i$, d.h. $C \subseteq A_i$ für ein i. Es folgt: $A_1, \ldots, A_m$ sind genau die irreduziblen

Komponenten von A. Noch zu ($\Diamond$): Träfe die Behauptung nicht zu, so wäre $A \in \Omega$, also $\Omega \neq \varnothing$, für

$$\Omega = \{B \subseteq A\colon B \neq \varnothing,\ B \text{ algebraisch},\ B \text{ nicht } \bigcup \text{ endlich vieler irreduzibler Teilmengen}\}$$

Nach der Bemerkung zu „Eigenschaften von V und I“ hätte Ω ein minimales Element B_0, das nicht irreduzibel ist, also $B_0 = C \cup D$ für algebraische Mengen C, D mit $\varnothing \neq C, D \subsetneq B_0$, wofür $C, D \notin \Omega$ [B_0 ist minimal], also C und D jeweils Vereinigung endlich vieler irreduzibler Teilmengen, woraus folgt, dass $B_0 = C \cup D$ eine Vereinigung endlich vieler irreduzibler Teilmengen ist, was wegen $B_0 \in \Omega$ unmöglich ist. □

Bemerkung. Ersetzt man „algebraisch“ durch „abgeschlossen“, so kann man „irreduzibel“ und „irreduzible Komponente“ völlig analog für einen beliebigen topologischen Raum X an Stelle von k^n mit der Zariski-Topologie definieren.

Definition. Ein topologischer Raum X heißt *noethersch*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

i) Jede absteigende Folge abgeschlossener Teilmengen von X wird stationär.
ii) Jede nichtleere Menge Ω von abgeschlossenen Teilmengen von X hat ein minimales Element, d.h. es gibt $B_0 \in \Omega$, so dass $B \subseteq B_0 \Rightarrow B = B_0$ gilt für alle $B \in \Omega$.
iii) Eine Menge $\mathcal{A}$ von abgeschlossenen Teilmengen von X enthält schon dann alle abgeschlossenen Teilmengen von X, wenn $\mathcal{A}$ *hereditär* ist, d.h. für jede abgeschlossene Teilmenge C von X gilt: Ist $D \in \mathcal{A}$ für jede abgeschlossene Teilmenge D von X mit $D \subsetneq C$, so ist $C \in \mathcal{A}$. (Noethersche Induktion)

Bemerkung. k^n mit der Zariski-Topologie ist ein noetherscher topologischer Raum.

Beweis von ($\Diamond$) für topologische Räume. Es sei $\mathcal{A}$ die Menge aller abgeschlossener Teilmengen von einem topologischen Raum X, die sich als endliche Vereinigung irreduzibler Teilmengen schreben lassen. Zu zeigen: $\mathcal{A}$ ist hereditär. Dazu sei C eine abgeschlossene Teilmenge von X, so dass $D \in \mathcal{A}$ für jede abgeschlossene Teilmenge D von X mit $D \subsetneq C$. Fall C irreduzibel: Dann ist $C \in \mathcal{A}$. Fall C reduzibel, d.h. $C = E \cup F$ mit $E, F \subsetneq C$ und E, F abgeschlossen. Nach Induktion: $E, F \in \mathcal{A}$. Es folgt $C \in \mathcal{A}$. □

7.2 Der Hilbertsche Nullstellensatz

Bemerkung. Ist der Körper k algebraisch abgeschlossen, insbesondere unendlich, so ist $V(f)$ unendlich für jedes $f \in k[X, Y] \backslash k$, denn wir können annehmen, dass $f = \sum_{i=0}^{m} g_i Y^i$, $g_i \in k[X]$, $m \geq 1$, $g_m \neq 0$. Dafür ist $\{t \in k\colon g_m(t) = 0\}$ endlich. Es gibt also unendlich viele $t_0, t_1, \cdots \in k$ mit $g_m(t_j) \neq 0$ für alle $j \geq 0$. Für jedes $j \geq 0$ ist $f_j = \sum_{i=0}^{m} g_i(t_j) Y^i \in k[Y] \setminus k$, also hat f_j eine Nullstelle s_j in k. Für alle $j \geq 0$ ist $(t_j, s_j) \in V(f)$. Die Voraussetzung “algebraisch abgeschlossen” ist notwendig, denn für $k = \mathbb{R}$ ist z.B. $V(X^2 + Y^2 + 1) = \emptyset$ und $V(\sum_{i=1}^{n} (X_i - t_i)^2) = \{p\}$ mit $p = (t_1, \ldots, t_n) \in \mathbb{R}^n$.

Bemerkung. Ein $A \subseteq k$ ist genau dann eine algebraische Menge, wenn A endlich oder $A = k$ ist (dies gilt für alle Körper k). [“dann” ist bekannt. “nur dann”: Mit $A = V(f)$ ist A endlich falls $f \neq 0$ und $A = k$ falls $f = 0$.]

Eine Ringerweiterung $R \subseteq R'$ von kommutativen Ringen heißt *von endlichem Typ*, wenn $R' = R[a_1, \ldots, a_n]$ für gewisse $a_1, \ldots, a_n \in R'$, d.h. es gibt einen surjektiven R-Algebrahomomorphismus $\eta\colon R[X_1, \ldots, X_n] \to R'$, mit anderen Worten es gibt ein Ideal $\mathfrak{a}$ von $R[X_1, \ldots, X_n]$, so dass $R[X_1, \ldots, X_n]/\mathfrak{a} \simeq R'$ als R-Algebren.

Satz (Zariski, körpertheoretische Fassung des Hilbertschen Nullstellensatzes)**.** *Jede Körpererweiterung von endlichem Typ ist endlich.*

Beweis. Es seien $k \subseteq K$ Körper mit $k[a_1, \ldots, a_n] = K$. Es ist zu zeigen, dass alle a_i algebraisch über k sind. Wir führen Induktion nach n. Wir haben $\eta\colon k[X_1, \ldots, X_n] \to K, X_i \mapsto a_i$, η ist surjektiv und $k[X_1, \ldots, X_n]/\operatorname{Ker}(\eta) \simeq K$. Ist $n = 1$, so ist $\operatorname{Ker}(\eta) \neq 0$, da K ein Körper ist, also ist a_1 algebraisch über k. Sei nun $n > 1$. Es sei $R = k[a_1]$, $L = Q(R) = k(a_1)$. Wegen $R \subseteq K$ und K Körper ist $L \subseteq K$. Ferner ist $L[a_2, \ldots, a_n] = K$ wegen $K = R[a_2, \ldots, a_n] \subseteq L[a_2, \ldots, a_n] \subseteq K$. Nach Induktion ist K/L endlich, es bleibt zu zeigen, dass L/k endlich ist (dies geht nicht mit dem Fall $n = 1$, denn R ist ein Körper genau dann, wenn $R = L$ genau dann, wenn a_1 algebraisch über k ist). Nach Induktion sind alle a_i mit $i \geq 2$ algebraisch über L, also gibt es $r \in R \setminus \{0\}$, so dass alle ra_i mit $i \geq 2$ ganz über R sind. Daraus folgt $(*)$: Zu jedem $b \in K$ gibt es $\ell \geq 1$, so dass $r^\ell b$ ganz über R ist. [Da b eine k-Linearkombination von Monomen der Form $a_1^{m_1} \ldots a_n^{m_n}$ ist, is $r^\ell b$ für geeignetes ℓ eine R-Linearkombination von Monomen der Form $(ra_1)^{m_1} \ldots (ra_n)^{m_n}$. Also ist $r^\ell b$ ganz über R.] Wäre a_1 nicht algebraisch über k, so wäre $k[X] \simeq R$, also R faktoriell; es gäbe also ein Primelement p von R mit $p \nmid r$ (Euklid), wozu es nach $(*)$ ein $\ell \geq 1$ gäbe mit $r^\ell \frac{1}{p}$ ganz über R, d.h. $r^\ell \frac{1}{p} \in R$, da R faktoriell ist. Also $p \mid r$, was ausgeschlossen ist. □

Korollar 1. *Ist k algebraisch abgeschlossen, so sind die maximalen ideale von $R_n = k[X_1, \ldots, X_n]$ genau die $I(p) = (X_1 - t_1, \ldots, X_n - t_n)$, $p = (t_1, \ldots, t_n) \in k^n$.*

Beweis. Es sei $\mathfrak{m}$ ein maximales Ideal von R_n. Vermöge des injektiven Ringhomomorphismus $\rho\colon k \hookrightarrow R_n \twoheadrightarrow R_n/\mathfrak{m}$ wird $K = R_n/\mathfrak{m}$ ein Oberkörper von k, und $K = k[\overline{X_1}, \ldots, \overline{X_n}]$ von endlichem Typ über k, also K/k endlich, speziell K/k algebraisch, also ρ bijektiv, da k algebraisch abgeschlossen ist. Für $1 \leq i \leq n$ gibt es insbesondere $t_i \in k$ mit $\rho(t_i) = \overline{X_i}$, d.h. $X_i - t_i \in \mathfrak{m}$. Insgesamt ist $I(p) \subseteq \mathfrak{m}$ mit $p = (t_1, \ldots, t_n)$, also $I(p) = \mathfrak{m}$, da $I(p)$ maximal ist. □

Korollar 2. *Ist k algebraisch abgeschlossen und $A \subseteq k^n$ eine algebraische Menge, so entsprechen die Punkte von A genau den maximalen Idealen von $k[A] = R_n/I(A)$.*

Beweis. Es sei $\operatorname{Max}(k[A])$ die Menge der maximalen Ideale von $k[A]$. Für jedes $p \in A$ ist $I(p) \supseteq I(A)$, also hat man $\pi\colon A \to \operatorname{Max}(k[A]), p \mapsto I(p)/I(A)$. Dieses π ist injektiv, und für k algebraisch abgeschlossen auch surjektiv, denn zu $\mathfrak{M} \in \operatorname{Max}(k[A])$, d.h. $\mathfrak{M} = \mathfrak{m}/I(A)$ mit $\mathfrak{m} \in \operatorname{Max}(R_n)$, gibt es nach Korollar 1 ein $p \in k^n$ mit $\mathfrak{m} = I(p)$. Wegen $I(A) \subseteq \mathfrak{m}$ ist $A \supseteq V(\mathfrak{m})$, also $A \ni p$. Damit ist $\mathfrak{M} = \pi(p)$ wie gewünscht. □

Korollar 3 (Schwache Form des Hilbertschen Nullstellensatzes)**.** *Ist k algebraisch abgeschlossen, so gilt für jedes Ideal $\mathfrak{a}$ von R_n: aus $\mathfrak{a} \subsetneq R_n$ folgt $V(\mathfrak{a}) \neq \emptyset$.*

Beweis. Man nehme ein maximales Ideal $\mathfrak{m}$ von R_n mit $\mathfrak{a} \subseteq \mathfrak{m}$ (möglich für $\mathfrak{a} \subsetneq R_n$, da R_n noethersch ist). Nach Korollar 1 ist $\mathfrak{m} = I(p)$ für ein $p \in k^n$, wofür $V(A) \supseteq V(\mathfrak{m}) = VI(\mathfrak{m}) \ni p$. □

Bemerkung. Für jede Teilmenge $A \subseteq k^n$ ist $I(A)$ ein Radikalideal.

Beweis. Sei $f \in \sqrt{I(A)}$, d.h. $f^\ell \in I(A)$ für ein ℓ, d.h. $0 = f^\ell(p) = f(p)^\ell$ für alle $p \in A$, also $f(p) = 0$ für alle $p \in A$. □

Nachtrag (zum Beweis des Satzes von Zariski)**.**

1) Für jede Körper k hat $k[X]$ unendlich viele paarweise nicht assoziierte irreduzible Polynome: Für k unendlich nehme $X - t$ mit $t \in k$. Für k endlich wissen wir $\forall n \geq 1 \exists f \in k[X]$: f irreduzibel und $\deg(f) = n$. Insbesondere gilt: Ist $R \cong k[X]$ und $r \in R$, so gibt es ein $p \in R$ mit $p \nmid r$ und p prim.

2) Es sei R ein Integritätsring, $L = Q(R)$, $L \subseteq K$ eine Körpererweiterung. Sind $a_2, \ldots, a_n$ algebraishc über L, so gibt es ein $r \in R \setminus \{0\}$ derart, dass ra_i ganz über R ist für alle i. In der Tat sind die a_i ganz über L, d.h. $a_i^{m_i} = f_i(a_i)$, $m_i \geq 1$, $f_i \in L[X]$, $\deg(f_i) < m_i$. Analoges gilt mit $m = \max\{m_i\}$ anstatt m_i. Schreibe $f_i = g_i/r$, $r \in R \setminus \{0\}$, $g_i \in R[X]$, $\deg(g_i) < m$. Dann ist $(ra_i)^m = r^{m-1} g_i(a_i) = k_i(ra_j)$ mit $k_i(X) = r^{m-1} g_i(x/r) \in R[X]$.

Satz (Starke Form des Hilbertschen Nullstellensatzes)**.** *Ist k ein algebraisch abgeschlossener Körper, so gilt $IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ für jedes Ideal $\mathfrak{a}$ von $R_n = k[X_1, \ldots, X_n]$.*

Beweis mit Trick von Rabinowitsch. Aus $\mathfrak{a} \subseteq IV(A)$ folgt $\sqrt{\mathfrak{a}} \subseteq IV(A)$ gemäß Bemerkung. Umgekehrt sei $f \in IV(A)$. Zu zeigen ist: Es existiert ein $m \geq 1$ mit $f^m \in \mathfrak{a}$. Sei ohne Einschränkung $f \neq 0$. Für das Ideal $\mathfrak{a} = (\mathfrak{a} \cap \{1 - fX_{n+1}\})$ von $R_{n+1} = R_n[X_{n+1}]$ gilt $V(\mathfrak{a}) = \varnothing$ in k^{n+1}. [Für $p \in V(\mathfrak{a})$ mit $p = (p', t_{n+1})$, wobei $p' \in k^n$, ist $p' \in V(\mathfrak{a})$ und $1 - f(p')t_{n+1} = 0$, also $1 = 0$]. Mit der schwachen Form des Satzes folgt $\mathfrak{a} = R_{n+1}$, d.h. $1 \in \mathfrak{a}$, etwa $1 = \sum_{i=1}^{\ell} F_i f_i + G(1 - fX_{n+1})$ mit $F_i, G \in R_{n+1}$, $f_i \in \mathfrak{a}$. Nun sei $K = Q(R_n)$. Für den Ringhomomorphismus $\varphi\colon R_{n+1} \to K$ mit $\varphi(h) = h$ für $h \in R_n$ und $\varphi(X_{n+1}) = 1/f$ ist $\varphi(1 - fX_{n+1}) = 1 - f \cdot 1/f = 0$, sowie $\varphi(F_i) = g_i/f^m$ für ein $m \geq 1$ und geeignete $g_i \in R_n$ [$F_i = \sum_{j=0}^{m} h_j X_{n+1}^j$, $h_j \in R_n \Rightarrow \varphi(F_i) = (\sum_{j=0}^{m} h_j f^{m-j}) \cdot 1/f^m$]. Es folgt $f^m = \sum_{i=1}^{\ell} g_i f_i \in \mathfrak{a}$. □

Bemerkung. Aus der starken Form des Hilbertschen Nullstellensatzes folgt die schwache.

Korollar 1. *Ist k ein algebraisch abgeschlossener Körper, so entsprechen die algebraischen Teilmengen A von k^n genau den Radikalidealen $\mathfrak{a}$ von R_n, und zwar vermöge der die Inklusionsordnung umkehrenden, zueinander inversen Bijektionen $A \mapsto I(A)$, $\mathfrak{a} \mapsto V(\mathfrak{a})$.*

Beweis. $A \subseteq k^n$ algebraisch $\Rightarrow \sqrt{I(A)} = I(A) \wedge VI(A) = A$. $\mathfrak{a}$ Radikalideal von $R_n \Rightarrow V(\mathfrak{a}) \subseteq k^n$ algebraisch und $IV(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \mathfrak{a}$. □

Definition. Ein *minimales Primideal* eines kommutativen Rings R ist ein Primideal $\mathfrak{p}$ von R, so dass für jedes Primideal $\mathfrak{q}$ aus $\mathfrak{p} \supseteq \mathfrak{q}$ folgt dass $\mathfrak{p} = \mathfrak{q}$.

Korollar 2. *Ist k ein algebraisch abgeschlossener Körpe und $A \subseteq k^n$ eine algebraische Menge, so entsprechen die (maximalen) irreduziblen Teilmengen von A genau den (minimalen) Primidealen von $k[A] = R_n/I(A)$. Genauer: Für* $\operatorname{Spec}(k[A]) = \{\mathfrak{p} \subseteq k[A] \colon \mathfrak{p}$ *ist Primideal*$\}$ *und* $\operatorname{Irr}(A) = \{M \subseteq A \colon M$ *ist irreduzibel*$\}$ *wird mit* $\pi \colon \operatorname{Irr}(A) \to \operatorname{Spec}(k[A]), B \mapsto I(B)/I(A)$ *eine ordnungsumkehrende Bijektion definiert.*

Beweis. $B \in \operatorname{Irr}(A) \Rightarrow I(B) \supseteq I(A)$ und $I(B)$ Primideal von R_n, also ist π definiert. π ist offensichtlich injektiv. π surjektiv: Ist $\mathfrak{P} \in \operatorname{Spec}(k[A])$, d.h. $\mathfrak{P} = \mathfrak{p}/I(A)$ mit $\mathfrak{p} \in \operatorname{Spec}(R_n)$ und $\mathfrak{p} \supseteq I(A)$, so ist $B = V(\mathfrak{p})$ eine algebraische Teilmenge von k^n mit $B \subseteq VI(A) = A$ und $I(B) = IV(\mathfrak{p}) = \sqrt{\mathfrak{p}} = \mathfrak{p}$, speziell ist $B \in \operatorname{Irr}(A)$. □

Satz. *Zu jedem Ideal $\mathfrak{a}$ eine kommutativen* noetherschen *Rings R gibt es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ von R mit $\sqrt{\mathfrak{a}} = p_1 \cap \cdots \cap \mathfrak{p}_m$. Für $\mathfrak{a} \neq R$ ist $m \geq 1$.*

Beweis. Mit Noetherscher Induktion. O.B.d.A. sei $\mathfrak{a} \neq R$. Ist $\mathfrak{a}$ ein Primideal, so setze $m = 1$, $\mathfrak{p}_q = \mathfrak{a}$. Es sei also $\mathfrak{a}$ kein Primideal, d.h. es gibt $r, s \in R \setminus \mathfrak{a}$ mit $rs \in \mathfrak{a}$. Wegen $\mathfrak{a} \subsetneq \mathfrak{a} + (r)$ und $\mathfrak{a} \subsetneq \mathfrak{a} + (s)$ gibt es nach Induktion Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ von R, $m \geq 2$, und $\ell \in \{1, \ldots, m-1\}$ mit $\sqrt{\mathfrak{a} + (r)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_\ell$ und $\sqrt{\mathfrak{a} + (s)} = \mathfrak{p}_{\ell+1} \cap \cdots \cap \mathfrak{p}_m$. Ferner gilt „=“ in $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a} + (r)} \cap \sqrt{\mathfrak{a} + (s)}$, denn für $z \in \sqrt{\mathfrak{a} + (r)} \cap \sqrt{\mathfrak{a} + (s)}$, etwa $z^u = x + \lambda r$, $z^v = y + \mu s$ (mit $u, v \geq 1$, $x, y \in \mathfrak{a}$, $\lambda, \mu \in R$) ist $z^u z^v = z^{u+v} = xy + x\mu s + \lambda r y + \lambda \mu r s \in \mathfrak{a}$, also $z \in \sqrt{\mathfrak{a}}$. □

Korollar 1. *Mit den Bezeichneungen des Satzes und mit dessen Voraussetzungen gilt $\mathfrak{p}_i \subseteq \mathfrak{a}$ für alle i und ist $\mathfrak{p}$ ein Primideal von R mit $\mathfrak{p} \subseteq \mathfrak{a}$, so gibt es ein i mit $\mathfrak{p} \supseteq \mathfrak{p}_i$.*

Definition. Es sei $\mathfrak{a}$ ein Ideal eines kommutativen Rings R. Ein Primideal von R heißt *minimal über* $\mathfrak{a}$, wenn $\mathfrak{p} \supseteq \mathfrak{a}$ gilt und für alle Primideale $\mathfrak{q}$ von R mit $\mathfrak{q} \supseteq \mathfrak{a}$ aus $\mathfrak{p} \supseteq \mathfrak{q}$ folgt $\mathfrak{q} = \mathfrak{p}$. Die minimalen Primideale von R über $\mathfrak{a}$ entsprechen genau den minmalen Primidalen von $R/\mathfrak{a}$. Insbesonder sind die minimalen Primideale über 0 genau die minimalen Primideale.

Korollar 2. *Für die $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ des Satzes kann man durch Aussondern erreichen, dass $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ für $i \neq j$. Damit hat man genau die minimalen Primideale von R über $\mathfrak{a}$ gewonnen.*

Beweis. Ist $\mathfrak{p} \supseteq \mathfrak{a}$ minimal, so gibt es nach Korollar 1 ein i mit $\mathfrak{p} \supseteq \mathfrak{p}_i \subseteq \mathfrak{a}$, also $\mathfrak{p} = \mathfrak{p}_i$. Ist $\mathfrak{p}_i \supseteq \mathfrak{p} \supseteq \mathfrak{a}$, so gibt es nach Korollar 1 ein j mit $\mathfrak{p} \supseteq \mathfrak{p}_j$, also $\mathfrak{p}_i \supseteq \mathfrak{p} \supseteq \mathfrak{p}_j$, also $i = j$, d.h. $\mathfrak{p} = \mathfrak{p}_i$. □

Bemerkung. Insbesondere gibt es zu jedem Ideal $\mathfrak{a}$ eines noetherschen Rings R mindestens ein, aber nur endlich viele minimale Primideale über $\mathfrak{a}$. Ist R nicht noethersch, so bekommt man die Existenz mit dem Zornschen Lemma, und die Endlichkeit ist im Allgemeinen nicht gegeben. Für $R = R_n = k[X_1, \ldots, X_n]$ mit einem Körper k ergibt sich nochmal die Zerlegung einer algebraischen Menge $A \subseteq k^n$ in ihre irreduziblen Komponenten:

$$I(A) = \underbrace{\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m}_{\text{minimales Primideal über } I(A)} \Longrightarrow A = \underbrace{V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_m)}_{\text{irreduzible Komponenten von } A}$$

Definition. Es sei R ein kommutativer Ring, sowie $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale von R. Dann ist

$$\prod_{i=1}^{n} \mathfrak{a}_i = \left\{ \sum_{j=1}^{m} \prod_{i=1}^{n} a_{ij} \colon m \geq 1 \wedge \forall i, j \colon a_{ij} \in \mathfrak{a}_i \right\}$$

ein Ideal mit $\prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$. Speziell hat man $\mathfrak{a}^n$ $(n \geq 1)$ mit $\mathfrak{a}^0 = R$.

Bemerkung. $\prod_{i=1}^{n}(a_i) = (\prod_{i=1}^{n} a_i)$, $(a)^n = (a^n)$.

Lemma.

a) $\sqrt{\prod_{i=1}^{n} \mathfrak{a}_i} = \sqrt{\bigcap_{i=1}^{n} \mathfrak{a}_i} = \bigcap_{i=1}^{n} \sqrt{\mathfrak{a}_i}$, *speziell* $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$

b) Ist $\mathfrak{a}_i + \mathfrak{a}_j = R$ *für* $i \neq j$, *so ist* $\prod_{i=1}^{n} \mathfrak{a}_i = \bigcup_{i=1}^{n} \mathfrak{a}_i$, *also auch* $\prod_{i=1}^{n} \sqrt{\mathfrak{a}_i} = \bigcap \sqrt{\mathfrak{a}_i}$

Beweis.

a) Klar: $\sqrt{\prod \mathfrak{a}_i} \subseteq \sqrt{\bigcap \mathfrak{a}_i} \subseteq \bigcap \sqrt{\mathfrak{a}_i}$. Ist $r \in \bigcap \sqrt{\mathfrak{a}_i}$, etwa $r^{\ell_i} \in \mathfrak{a}_i$ $(i \leq n)$, so ist $r^{\sum \ell_i} = \prod r^{\ell_i} \in \prod \mathfrak{a}_i$, also $r \in \sqrt{\prod \mathfrak{a}_i}$.

b) Klar: $\prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$. Zeige „$\supseteq$“ durch Induktion nach n. $n = 2$: Nach Voraussetzung ist $1 = a_1 + a_2$ mit $a_i \in \mathfrak{a}_i$. Für $r \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ ist $r = r1 = ra_1 + ra_2 \in \mathfrak{a}_1\mathfrak{a}_2$. $n \geq 3$: Es sei $\mathfrak{b} = \prod_{i<n} \mathfrak{a}_i$. Nach Voraussetzung ist $1 = x_i + y_i$ mit $x_i \in \mathfrak{a}_i$ und $y_i \in \mathfrak{a}_n$ für $i < n$. Es ergibt sich: $b \ni \prod_{i<n} x_i = \prod_{i<n}(1 - y_i) = 1 - z$ mit $z \in \mathfrak{a}_n$, also $b + \mathfrak{a}_n = R$. Nach Induktion ist $\mathfrak{a}b = \bigcap_{i<n} \mathfrak{a}_i$. Insgesamt: $\prod_{i \leq n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i \leq n} \mathfrak{a}_i$. □

Definition. Ideale $\mathfrak{a}, \mathfrak{b}$ mit $\mathfrak{a} + \mathfrak{b} = R$, d.h. $1 \in \mathfrak{a} + \mathfrak{b}$ heißen *koprim* oder *komaximal*.

Bemerkung. Ist R ein Integritätsring und $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ koprim, so sind a und b teilerfremd., da $(a, b) = (d)$ für jeden ggT d. Ist R ein Hauptidealring, so gilt auch die Umkehrung. Speziell sind zwei Primideale $\mathfrak{p} \neq \mathfrak{q}$ eines Hauptidealrings stets koprim. Allgemein sind zwei maximale Ideale $\mathfrak{m} \neq \mathfrak{n}$ eines beliebigen Ringes koprim. Für $R = R_n = k[X, \ldots, X_n]$ mit einem Körper k sind X_1, X_2 zwar teilerfremd (da verschiedene Primelemente), jedoch sind (X_1), (X_2) nicht koprim, (X_1, X_2) ist sogar ein Primideal bzw. für $n = 2$ ein maximales Ideal.

Bemerkung. cEs sei R ein Integritätsring. Sind $p_1, \ldots, p_n \in R$ Primelemente mit $p_i \not\sim p_j$ für $i \neq j$, so gilt

$$\bigcap_{i \leq n} (p_i) \overset{*}{=} \left(\prod_{i \leq n} p_i \right) = \prod_{i \leq n} (p_i)$$

Beweis. Nur „$\subseteq$“ von $(*)$ ist zu zeigen. Zu $a \in \bigcap(p_i)$ gibt es $x_1 \in R$ mit $a = x_1 p_1$ (da $a \in (p_1)$). Wegen $p_2 \mid a$ und $p_2 \nmid p_1$ ist $p_2 \mid x_1$, d.h. $x_1 = x_2 p_2$ mit $x_2 \in R$, also $a = x_2 p_1 p_2$ etc. bis hin zu $a = x_n p_n \cdots p_1$. □

Beispiel. Es sei k ein algebraisch abgeschlossener Körper und $A \subseteq k^n$ eine Hyperfläche, d.h. $A = V(f)$ für ein $f \in R_n \setminus k$. Ist $f = \prod_{i=1}^{m} f_i^{\ell_i}$ eine Primfaktorzerlegung mit $\ell_i \geq 1$ und $f_i \not\sim f_j$, so sind $V(f_1), \ldots, V(f_m)$ die irreduziblen Komponenten von A und $I(A) = (f_1 \cdots f_m)$. Die $(f_1), \ldots, (f_m)$ sind nämlihc die minimalen Primideale über (f), da

$\sqrt{(f)} = \sqrt{\prod(f_i^{\ell_i})} = \bigcap\sqrt{(f_i^{\ell_i})} = \bigcap\sqrt{(f_i)} = \bigcap(f_i)$ und die (f_i) sind Primideale mit $(f_i) \not\subseteq (f_j)$ für $i \neq j$. Es folgt auch $I(A) = IV(f) = \sqrt{(f)} = \bigcap(f_i) = (\prod f_i)$. Insbesondere ist $I(A)$ ein Hauptideal. Jedes $g \in R_n$ mit $I(A) = (g)$ heißt *Minimalpolynom der Hyperfläche* A. Dieses ist bis auf $\sim$, d.h. bis auf einen Faktor aus $R_n^\times = k^\times$ eindeutig durch A bestimmt. Speziell hängt $\deg(g)$ nur von A ab und heißt *Grad der Hyperfläche* A. Zum Beispiel hat das Achsenkreuz $V(X_1 \cdot X_2)$ in k^2 Grad 2, dito für $V(X_1^u \cdot X_2^v)$ $(u, v \geq 1)$

Satz (Chinesischer Restsatz)**.** *Es seien $\mathfrak{a}, \ldots, \mathfrak{a}_n$ Ideale eines kommutativen Rings R. Der Ringhomomorphismus $\varphi\colon R \to \prod_{i\leq n} R/\mathfrak{a}_i, x \mapsto (x + \mathfrak{a}_i)_{i\leq n}$ mit Kern $\bigcap_{i\leq n}\mathfrak{a}_i$ ist genau dann surjektiv, wenn $\mathfrak{a}, \ldots, \mathfrak{a}_n$ paarweise koprim sind. Dann hat man $R/\cap_{i\leq n}\mathfrak{a}_i \cong_\varphi \prod_{i\leq n} R/\mathfrak{a}_i$.*

Beweis. Für $i \leq n$ sei $e_i = (\delta_{i\nu})_{\nu\leq n} \in \prod_{\nu\leq n} R/\mathfrak{a}_\nu$, d.h. $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. „⇒“ Für $i \leq n$ nehme $x \in R$ mit $\varphi(x) = e_i$, d.h. $x - 1 \in \mathfrak{a}_i$ und $x \in \mathfrak{a}_j$ für $j \neq i$, wofür $1 = (1 - x) + x \in \mathfrak{a}_i + \mathfrak{a}_j$. „⇐“ Es reicht, für $i \leq n$ zu zeigen, dass $e_i \in \operatorname{Im}\varphi$, denn jedes $(x_i + \mathfrak{a}_i)_{i\leq n} \in \prod_{i\leq n} R/\mathfrak{a}_i$ ist $\sum_{i\leq n} x_i e_i$. Wegen $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $j \neq i$ ist $1 = \mathfrak{a}_j + v_j$ mit $u_j \in \mathfrak{a}_i$ und $v_j \in \mathfrak{a}_j$. Für $x = \prod j \neq i v_j = \prod_{j\neq i}(1 - u_j) = 1 - u$ mit $u \in \mathfrak{a}_i$ ist $x \in \mathfrak{a}_j$ für $j \neq i$, also $\varphi(x) = e_i$. □

7.3 Algebraische Unabhängigkeit

Definition. Es sei $k \subseteq K$ eine Körpererweiterung, $n \geq 0$. Man nennt $a_1, \ldots, a_n \in K$ *algebraisch (un)abhängig über k*, wenn es (k)ein $f \in k[X_1, \ldots, X_n]$ gibt mit $f \neq 0$ und $f(a_1, \ldots, a_n) = 0$. Diese Definition hängt nicht von der Reihenfolge der $a_1, \ldots, a_n$ ab. Man kann also von der algebraischen (Un-)Abhängigkeit endlicher Teilmengen von K über k reden. Eine beliebige Teilmenge $T \subseteq K$ heißt algebraisch unabhängig, wenn jede endliche Teilmenge $S \subseteq T$ algebraisch abhängig ist.

Beispiel. $\varnothing$ ist algebraisch unabhängig. Für $n = 1$ ist $a_1 \in K$ genau dann algebraisch (un)abhängig über k, wenn a_1 (nicht) algebraisch über k ist. Für $n \geq 1$ sind $X_1, \ldots, X_n \in k(X_1, \ldots, X_n)$ algebraisch unabhängig über k. Schließlich sind k-linear abhängige $a_1, \ldots, a_n \in K$ auch algebraisch unabhängig über k.

Bemerkung. Für endliche Teilmengen $S \subseteq T$ von K gilt: Ist S algebraisch abhängig über k, so auch T.

Lemma. *Genau dann sind $a_1, \ldots, a_n \in K$ algebraisch abhängig über k, wenn es ein $i \in \{1, \ldots, n\}$ gibt mit a_i algebraisch über $k(a_1, \ldots, a_{i-1})$.*

Beweis. „⇒“: Induktion über n. $n = 0$: %. $n \geq 1$: Ist $g \in k[X_1, \ldots, X_n]$ mit $g \neq 0$ und $g(a_1, \ldots, a_n) = 0$, so ist $h = g(a_1, \ldots, a_{n-1}, X_n) \in A[X_n]$ für $A = k[a_1, \ldots, a_{n-1}]$ mit $h(a_n) = 0$. Ist $h \neq 0$, so ist a_n algebraisch über $Q(A) = k(a_1, \ldots, a_{n-1})$. Ist $h = 0$, so ist $g_j(a_1, \ldots, a_{n-1}) = 0$ für alle j, wobei $g = \sum g_j X_n^j$ mit $g_j \in k[X_1, \ldots, X_{n-1}]$. Wegen $g \neq 0$ ist $g_j \neq 0$ für ein j, also sind $a_1, \ldots, a_{n-1}$ algebraisch abhängig über k. □

Korollar (Austauscheigenschaft der Algebraizität)**.** *Für $x, y \in K$ gilt: Ist x algebraisch über $k(y)$, so ist y algebraisch über $k(x)$ oder x algebraisch über k. Allgemeiner*

für $x, y_1, \ldots, y_n \in K$: Ist x algebraisch über $k(y_1, \ldots, y_n)$, so ist y_n algebraisch über $k(y_1, \ldots, y_{n-1}, x)$ oder x algebraisch über $k(y_1, \ldots, y_{n-1})$.

Satz. *Es seien $S, T \subseteq K$ endliche Teilmengen. Ist $K/k(S)$ algebraisch, so ist T algebraisch abhängig über k oder es gibt $S_0, S_1 \subseteq K$ mit $S = S_0 \sqcup S_1$ und $|S_0| = |T|$, so dass $K/k(T \cup S_1)$ algebraisch ist.*

Beweis. Induktion nach $m = |T \setminus S|$. Im Fall $m = 0$ ist $T \subseteq S$, also $S_0 = T$ und $S_1 = S \setminus T$ wie verlangt. Ist $m > 0$, so nehme $x \in T \setminus S$. Schreibe $S = \{s_1, \ldots, s_\ell\}$ mit $T \cap S = \{s_1, \ldots, s_{\ell_0}\}$ für $\ell_0 \leq \ell$. Nach Voraussetzung ist x algebraisch über $k(s_1, \ldots, s_{\ell-1})(s_\ell)$, also nach Korollar s_ℓ algebraisch über $k(s_1, \ldots, s_{\ell-1})(x)$ oder x algebraisch über $k(s_1, \ldots, s_{\ell-1})$ etc. So erhält man $i \in \{0, \ldots, \ell\}$ mit i) x algebraisch über $k(s_1, \ldots, s_{i-1})(s_i)$ und, falls $i > 0$, ii) s_i algebraisch über $k(s_1, \ldots, s_{i-1})(x)$. Ist $i = 0$, so ist x algebraisch über k, also T algebraisch abhängig über k. Nun sei $i > 0$. Ist $s_i \in T$, d.h. $i \leq \ell_0$, so ist T algebraisch abhängig über k. Nun sei $i > 0$ und $s_i \notin T$. Setze $(S' = S \setminus \{s_i\}) \cup \{x\}$. Es gilt $T \cap S \subseteq S \setminus \{s_i\} \subseteq S$, also $T \setminus S' \subsetneq T \setminus S$. Wegen $K/k(S)$ algebraisch und ii) ist $K/k(S')$ algebraisch. Nach Induktion ist T algebraisch abhängig über k oder $S' = S'_0 \sqcup S'_1$ mit $|T| = |S'_0|$ und $K/k(T \cup S'_1)$ algebraisch. Ist $x \in S'_0$, so setze $S_0 = (S'_0 \setminus \{x\}) \cup \{s_i\}$, $S_1 = S'_1$. Ist $x \in S'_1$, so setze $S_0 = S'_0$ und $S'_1 = (S_1 \setminus \{x\}) \cup \{s_i\}$. Damit ist $S = S_0 \sqcup S_1$ und $|S_0| = |T|$, sowie $K/k(T \cup S_1)$ algebraisch wegen i) im Fall $x \in S'_1$. □

Definition. Ist eine Teilmenge B von K algebraisch unabhängig über k, so nennt man $k \subseteq k(B)$ eine *rein transzendente* Körpererweiterung. Ist zudem $K/k(B)$ eine algebraische Körpererweiterung, so heißt B eine *Transzendenzbasis* von K über k.

Korollar. *Sind S, T endliche Transzendenzbasen von K über k, so gilt $|S| = |T|$.*

Bemerkung. Eine Teilmenge B von K ist genau dann eine Transzendenzbasis von K über k, wenn B eine maximale algebraisch unabhängige Teilmenge von K über k ist, d.h. B ist über k algebraisch unabhängig und aus $B \subsetneq C \subseteq K$, dass C über k algebraisch abhängig ist.

Beweis. „⇒“: Für $x \in C \setminus B$ ist $x \in K$ algebraisch über $k(B)$, also ist $B \sqcup \{x\}$ algebraisch abhängig über k, also ist C algebraisch abhängig über k. „⇐“: Z.z.: $\forall x \in K \setminus k(B)$: x algebraisch über $k(B)$. Dazu betrachte $C = B \sqcup \{x\}$ und verwende die Austauscheigenschaft. □

Präzisierung. Eine endliche Teilmenge S von K heißt *algebraisch (un)abhängig*, wenn gilt: Schreibt man $S = \{a_1, \ldots, a_n\}$ mit $n \geq 0$ verschiedene $a_1, \ldots, a_n$, so sind $a_1, \ldots, a_n$ algebraisch (un)abhängig. Eine beliebige Teilmenge S von K heißt algebraisch (un)abhängig, wenn S (k)eine endliche Teilmenge S_0 hat, die algebraisch abhängig ist. Zum Beispiel ist S algebraisch abhängig über k, wenn es ein $a \in S$ gibt, das algebraisch ist über k. Wie für endliche $B \subseteq K$ definiert man für beliebige $B \subseteq K$, dass B eine *Transzendenzbasis* ist (kurz TB), sowie „*K/k rein transzendent*“.

Bemerkung. Ist K/k rein transzendent, so ist jedes $a \in K \setminus k$ transzendent über k. [Fischer-Sacher, S.228f.]

Bemerkung. Es folgt aus dem vorletzten Satz für endliche $S \subseteq K$ mit $K/k(S)$ algebraisch: Hat ein beliebiges $T \subseteq K$ mehr Elemente als S, so ist T algebraisch abhängig über k. [wähle $T_0 \subseteq T$, $|T_0| = |S| + 1$]. Mit anderen Worten: Ist ein beliebiges $T \subseteq K$ algebraisch unabhängig über k, so hat T höchstens $|S|$ Elemente. Insbesondere: Hat K eine endliche Transzendenzbasis S über k, so ist jede Transzendenzbasis T von K über k endlich und nach Korollar ist $|S| = |T|$.

Definition. Die Länge einer (und damit jeder) endlichen Transzendenzbasis heißt *Transzendenzgrad* $\mathrm{tr.deg}_k(K)$ von K über k. Hat K keine endliche Transzendenbasis über k, so ist $\mathrm{tr.deg}_k(K) = \infty$.

Beispiel.

a) K/k algebraisch $\Longrightarrow \mathrm{tr.deg}_k(K) = 0$ [Transzendenzbasis $\varnothing$].

b) $\mathrm{tr.deg}\, k(X_1, \ldots, X_n) = n$ [Transzendenzbasis $\{X_1, \ldots, X_n\}$].

Bemerkung. Haben $k \subseteq L$ und $L \subseteq K$ endliche Transzendenbasen, so hat auch $k \subseteq K$ eine endliche Transzendenzbasis und $\mathrm{tr.deg}_k(K) = \mathrm{tr.deg}_k(L) + \mathrm{tr.deg}_L(K)$.

Fakt. Für $a \subseteq K$ gilt: a ist algebraisch über $k(S)$ mit $S \subseteq K$ genau dann, wenn es ein endliches $S_0 \subseteq S$ gibt mit a algebraisch über $k(S_0)$.

Lemma. *Ein $S \subseteq K$ ist algebraisch abhängig über k genau dann, wenn es ein $a \in S$ gibt mit a algebraisch über $k(S \setminus \{a\})$.*

Bemerkung. Ein $B \subseteq K$ ist genau dann eine Transzendenzbasis von K über k, wenn B eine maximale über k algebraisch unabhängige Teilmenge von K ist, d.h. B ist algebraisch unabhängig und aus $B \subsetneq S \subseteq K$ folgt, dass S algebraisch abhängig über k ist.

Beweis. „$\Rightarrow$“ Übung. Hier ist „B algebraisch unabhängig“ überflüssig. „$\Leftarrow$“ Zu zeigen: $K/k(B)$ ist algebraisch. Dazu sei $z \in K \setminus B$. Für $S = B \sqcup \{z\}$ ist $B \subsetneq S$, also ist S algebraisch abhängig, d.h. (Lemma) es gibt ein $a \in S$ mit a algebraisch über $k(S \setminus \{a\})$, also ist a algebraisch über $L(z)$ für $L = k(B \setminus \{a\})$, da $S \setminus \{a\} \subseteq (B \setminus \{a\}) \cup \{z\}$. Gemäß der Austauscheigenschaft ist z algebraisch über $L(a) = k(B)$ oder a algebraisch über $L \subseteq k(B)$. Im letzteren Fall muss $a = z$ sein, denn $a \in B$ ist (nach Lemma wegen B algebraisch unabhängig) $\square$

Satz (ZL). *Zu jeder über k algebraisch unabhängigen Teilmenge A von K gibt es eine Transzendenzbasis B von K über k mit $B \supseteq A$.*

Korollar. *Jede Körpererweiterung hat eine Transzendenzbasis.*

Ohne ZL kann man zeigen, dass jede Körpererweiterung von endlichem Typ eine endliche Transzendenzbasis hat. Definiert man nämlich nämlich algebraische (un)abhängigkeit völlig analog für Ringerweiterungen, so hat man die *Noether-Normalisierung.*

Satz. *Es sei k ein Körper, R ein Ring, $k \subseteq R$. Ist $R = k[x_1, \ldots, x_n]$, so gibt es $z_1, \ldots, z_n \in R$ mit $R = k[z_1, \ldots, z_n]$ und $m \leq n$, so dass R ganz über $k[z_1, \ldots, z_m]$ und $z_1, \ldots, z_m$ algebraisch unabhängig über k sind.*

Beweis. Induktion über n: Sind $x_1, \ldots, x_n$ algebraisch unabhängig, etwa für $n = 0$, so setze $m = n$ und $z_i = x_i$ für $i \leq m$. Es sein also $x_1, \ldots, x_m$ algebraisch abhängig, d.h. $0 \overset{(1)}{=} \sum_j \alpha_j x_1^{j_1} \cdots x_n^{j_n}$ mit $\alpha_j = 0$ für fast alle $j = (j_1, \ldots, j_n)$. Nehme $d \geq 1$ mit $d > j_i$ für alle i, j mit $\alpha_j \neq 0$. Setze $y_i = x_i - x_n^{d^{n-i}}$ für $i < n$. Aus (1) ergibt sich mit $x_i = y_i + x_n^{d^{n-i}}$ die Gleichung $0 \overset{(2)}{=} \sum_j \alpha_j x_n^{j^*} + f(y_1, \ldots, y_{n-1}, x_n)$ mit $j^* = \sum_{i=1}^n j_i d^{n-i}$ für $\alpha_j \neq 0$ und „$\deg_{x_n}(G) < j^*$ für ein j mit $\alpha_j \neq 0$“ gilt für jedes Monom g von f. Nun besagt (2), dass x_n ganz über $S = k[y_1, \ldots, y_{n-1}]$ ist, d.h. $R = S[x_n]$ ist ganz über S. Nach Induktion hat man $S = k[z_1, \ldots, z_{n-1}]$ und $m \leq n - 1$ mit $z_1, \ldots, z_m$ algebraisch unabhängig über k und S ist ganz über $T = k[z_1, \ldots, z_m]$ Es folgt: R ist ganz über T. Setze $z_n = x_n$. □

Es folgt der Satz von Zariski (die körpertheoretische Form des Hilbertschen Nullstellensatzes), denn dies ist der Spezialfall „$\mathfrak{a}$ ist ein maximales Ideal“ des folgenden Korollars.

Korollar. *Ist k ein Körper, so gibt es zu jedem Ideal $\mathfrak{a}$ von $R_n = k[X_1, \ldots, X_n]$ mit $\mathfrak{a} \neq R_n$ ein Ideal $\mathfrak{b}$ von R_n mit $\mathfrak{b} \neq R_n$ und $\mathfrak{b} \supseteq \mathfrak{a}$, so dass $R_n/\mathfrak{b}$ ganz über k ist.*

Beweis. Es sei $R = R_n$, $\overline{R} = R/\mathfrak{a} = k[x_1, \ldots, x_n]$ mit $x_i = \overline{X_i}$. Nach Satz gibt es über k algebraisch unabhängige $y_1, \ldots, y_r \in \overline{R}$ mit $\overline{R}$ ganz über $S = k[y_1, \ldots, y_r]$. Es reicht zu zeigen, dass $y_1 \notin \overline{R}^\times$. Denn dann ersetze man $\mathfrak{a}$ durch $\mathfrak{a} + (Y_1)$ mit $\overline{Y_1} = y_1$ und führe Induktion nach r. Im Fall $r = 0$ setze man $\mathfrak{b} = \mathfrak{a}$. Nun: Ist $y_1 \in \overline{R}^\times$, so ist $y_1 \in S^\times$ nach folgendem Fakt, d.h. $y_1 s - 1 = 0$ für ein $s \in S$, was unmöglich ist, da $y_1, \ldots, y_r$ algebraisch unabhängig sind. □

Fakt. Ist $A \subseteq B$ eine beliebige Ringerweiterung, $y \in B^\times$ und y^{-1} ganz über A, so ist $y \in A[y]^\times$.

Beweis. Für $z = y^{-1}$ hat man $z^m + a_{m-1} z^{m-1} + \cdots + a_1 z + a_0 = 0$ mit $a_i \in A$, also $1 + a_{m-1} y + \cdots + a_1 y^{m-1} + a_0 y^m = 0$ und damit $y \in A[y]^\times$. □