Separabilität.

Satz. *Sei K ein Unterkörper von $\mathbb{C}$. Ist $f \in K[X]$ ein irreduzibles normiertes Polynom vom Grad n, so hat f in $\mathbb{C}$ genau n paarweise verschiedene Nullstellen $\alpha_1, \dots \alpha_n$, es ist also $f = \prod_{r=1}^{n}(X - \alpha_r)$.*

Irreduzible Polynome mit Koeffizienten in einem Körper, die in einem Oberkörper in paarweise verschiedene Linearfaktoren zerfallen, nennt man *separabel*.

Beweis: Da $\mathbb{C}$ algebraisch abgeschlossen ist, können wir f über $\mathbb{C}$ als Produkt von Linearfaktoen schreiben, etwa $f = \prod_{r=1}^{n}(X - \alpha_r)$ mit $\alpha_1, \dots, \alpha_n \in \mathbb{C}$. Angenommen, $\alpha_1 = \alpha_2 = \alpha$. Dann ist also $f = (X - \alpha) \cdot g$ für ein Polynom $g \in \mathbb{C}$ mit $g(\alpha) = 0$. Sei f' die Ableitung von f, dies ist ein Polynom in $K[X]$ vom Grad $n-1$ und die Produktregeln für das Ableiten besagt: $f' = (X - \alpha) \cdot g' + g$, also ist $f'(\alpha) = 0$. Sei $h \in K[X]$ der größte gemeinsame Teiler der Polynome f und f'. Beachte: man berechnet h mit dem Euklid'schen Algorithmus, dabei spielt es keine Rolle, ob man die Polynome f, f' als Elemente von $K[X]$ oder von $\mathbb{C}[X]$ auffasst. Da f, f' eine gemeinsame Nullstelle (in $\mathbb{C}$) besitzen, ist $\operatorname{grad} h \geq 1$. Da f' den Grad $n-1$ hat, ist $\operatorname{grad} h \leq \operatorname{grad} f' = n - 1$. Also besitzt f einen Teiler mit Grad zwischen 1 und $n-1$, ist also nicht irreduzibel, im Gegensatz zur Voraussetzung.

Warnung. Allgemeiner können wir einen beliebigen Körper K der Charakteristik Null betrachten. Es gilt: *Jedes irreduzible Polynom in $K[X]$ ist separabel,* mit dem gleichen Beweis. Dabei verwendet man das "formales Ableiten": Ist $f = \sum_{r=0}^{n} c_r X^r$ ein Polynom mit Koeffizienten $c_r \in K$, so definiert man $f' = \sum_{r=1}^{n} r c_r X^{r-1}$ (ohne sich um Fragen der Topologie oder Differentialgeometrie zu kümmern); das formale Ableiten ist also die Abbildung $K[X] \to K[T]$ mit $f \mapsto f'$, man rechnet leicht nach, dass die oben verwendete Produktregel gilt. Hat f den Grad n, und ist die Charakteristik $\operatorname{char} K$ von K beliebig, so hat f' **nicht** notwendigerweise den Grad $n-1$; ist nämlich $p = \operatorname{char} K > 0$ ein Teiler von n, so ist der Koeffizient von X^{n-1} in f' gleich Null! Demnach kann ein irreduzibles Polynom, dessen Grad ein Vielfaches von p ist, mehrfache Nullstellen haben — aber eben nicht, wenn $\operatorname{char} K = 0$ gilt.

Folgerung 1. *Ist K ein Zahlkörper, so gibt es $\alpha \in K$ mit $K = \mathbb{Q}[\alpha]$.* (Körpererweiterungen, die von einem Element erzeugt werden, nennt man *primitiv.*)

Beweis: Es reicht zu zeigen: Sind α, β algebraische Elemente in $\mathbb{C}$, so gibt es γ mit $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$. Dabei können wir ein derartiges $\gamma = \alpha + c\beta$ mit einem geeigneten $c \in \mathbb{Q}$ finden.

Sei f das Minimalpoynom von α, sei g das Minimalpolynom von β, seien $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ die Nullstellen von f, seien $\beta_1 = \beta, \beta_2, \dots, \beta_m$ die Nullstellen von g. Wir suchen ein $c \in \mathbb{Q}$ mit

$$\alpha_i + c\beta_j \neq \alpha + c\beta \quad \text{für alle } 2 \leq i \leq n,\ 1 \leq j \leq m.$$

Betrachte die Menge $\mathcal{M} = \{(\alpha_i - \alpha)/(\beta_j - \beta) \mid 1 \leq i \leq n, 2 \leq j \leq m\}$ in $K = \mathbb{Q}[\alpha, \beta]$ (wir brauchen hier, dass die β_j paarweise verschieden sind). Da $\mathcal{M}$ endlich ist, gibt es $c \in \mathbb{Q} \setminus \mathcal{M}$. Es ist $c \neq \alpha_i - \alpha)/(\beta_j - \beta)$, also $c(\beta_j - \beta) \neq \alpha_i - \alpha)$, also $\alpha + c\beta + c\beta_j \neq \alpha_i$, für $2 \leq i \leq n$ und $1 \leq j \leq m$.

Sei nun $h(X) = f(\gamma - cX) \in \mathbb{Q}[\gamma][X]$. Es ist $h(\beta) = 0$, aber $h(\beta_j) = f(\gamma - c\beta_j) \neq 0$. Daher haben die Polynome h und g genau eine gemeinsame Nullstelle, nämlich β. Dies zeigt: der größte gemeinsame Teiler von h und g ist $X - \beta$, also ist $X - \beta \in \mathbb{Q}[\gamma][X]$, und demnach $\beta \in \mathbb{Q}[\gamma]$. Und es ist auch $\alpha = \gamma + c\beta \in \mathbb{Q}[\gamma]$.

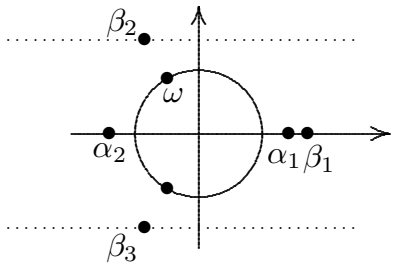
Beispiel: Man bestimme ein primitives Element zu $\mathbb{Q}[\sqrt{2}, \sqrt[3]{5}]$. Wähle $c = 1$. Es ist

$$\alpha_1 = \sqrt{2},\ \alpha_2 = -\sqrt{2}, \quad \beta_1 = \sqrt[3]{5},\ \beta_2 = \omega\sqrt[3]{5},\ \beta_3 = \omega^2\sqrt[3]{5},$$

mit $\omega = \frac{1}{2}(-1 + \sqrt{3}i)$. Hier ist $\alpha + \beta \in \mathbb{R}$, dagegen ist keines der Elemente

$$\alpha_1 + \beta_2,\ \alpha_1 + \beta_3,\ \alpha_2 + \beta_2,\ \alpha_2 + \beta_3$$

reell (diese Zahlen liegen ja auf den Parallelen zur reellen Achse durch β_2 und β_3).



Folgerung 2. *Sei K ein Zahlkörper vom Grad n. Dann gibt es genau n Körper-Homomorphismen $K \to \mathbb{C}$.*

Beweis: Sei $\alpha \in K$ ein primitives Element, sei f sein Minimalpolynom, seien $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ die Nullstellen von f. Betrachte die Ring-Homomorphismen

$$\sigma_i \colon \mathbb{Q}[X] \to \mathbb{C}, \qquad \text{mit } \sigma_i(X) = \alpha_i.$$

Wegen $f(\alpha_i) = 0$ wird das Ideal $\langle f \rangle$ von $\mathbb{Q}[X]$ jeweils auf Null abgebildet, es ist also $\langle f \rangle \subseteq \mathrm{Ker}(\sigma_i)$. Da $\langle f \rangle$ ein maximales Ideal, und $\sigma_i(1) = 1$ ist, folgt $\langle f \rangle = \mathrm{Ker}(\sigma_i)$. Demnach induziert jedes σ_i einen Körper-Homomorphismus

$$\overline{\sigma}_i \colon \mathbb{Q}[X]/\langle f \rangle \longrightarrow \mathbb{C},$$

und durch die Abbildungen

$$\overline{\sigma}_i(\overline{\sigma}_1)^{-1} \colon K \longrightarrow \mathbb{C}$$

erhalten wir n paarweise verschiedene Körper-Homomorphismen. Es kann keine weiteren geben, denn ist $\eta \colon K \to \mathbb{C}$ ein Körper-Homomorphismus, so ist $\eta(\alpha)$ ein Element von $\mathbb{C}$, das Nullstelle von f ist, also ist $\eta(\alpha) = \alpha_i$ für eines unserer i.

Tautologisch: *Sei K Zahlkörper vom Grad n, seien $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ die paarweise verschiedenen Einbettungen. Dann gilt: Jede Multiplikationsabbildung*

$$(\beta\cdot) \colon K = \mathbb{Q}^n \to K = \mathbb{Q}^n \qquad \textit{mit } \beta \in K$$

ist (über $\mathbb{C}$) diagonalisierbar, und hat die Eigenwerte $\sigma_1(\beta), \ldots, \sigma_n(\beta)$.

Genauer gilt: Sei $\omega_1, \ldots, \omega_n$ eine $\mathbb{Q}$-Basis von K. Wir erhalten durch

$$(*) \qquad \beta\omega_i = \sum\nolimits_j c_{ij}\omega_j \qquad \text{mit } \; c_{ij} \in \mathbb{Q}.$$

eine $(n \times n)$-Matrix $C = (c_{ij})_{ij}$ mit Koeffizienten in $\mathbb{Q}$; dies ist die darstellende Matrix für die Multiplikationsabbildung $(\beta\cdot)$ bezüglich unserer Basiswahl.

(a) *Ist $\sigma\colon K \to \mathbb{C}$ ein Körper-Homomorphismus, so ist der Vektor*

$$\begin{bmatrix} \sigma(\omega_1) \\ \vdots \\ \sigma(\omega_n) \end{bmatrix} \quad \in \mathbb{C}^n$$

ein Eigenvektor für die Matrix C mit Eigenwert $\sigma(\beta)$.

(b) *Die Vektoren*

$$(**) \qquad \begin{bmatrix} \sigma_1(\omega_1) \\ \vdots \\ \sigma_1(\omega_n) \end{bmatrix}, \quad \cdots \quad , \begin{bmatrix} \sigma_n(\omega_1) \\ \vdots \\ \sigma_n(\omega_n) \end{bmatrix}$$

bilden eine Basis von Eigenvektoren von $\mathbb{C}^n$ für die Matrix C.

Zusatz: Da die Multiplikationsabbildungen miteinander vertauschbar sind, und alle diese Abbildungen über $\mathbb{C}$ diagonalisierbar sind, muss es natürlich eine simultane Basis aus Eigenvektoren geben. Interessant ist aber der tautologische Charakter dieser Basiselemente: Einer dieser Eigenvektoren ist

$$\begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}$$

(wenn wir K als Unterkörper von $\mathbb{C}$ auffassen). Und die anderen Basisvektoren haben die gleiche Form, nur eben unter Verwendung jeweils anderer Einbettungen.

Beweis: Wende σ auf die Gleichung $(*)$ an, wir erhalten:

$$\sigma(\beta)\sigma(\omega_i) = \sigma(\beta\omega_i) = \sigma(\sum\nolimits_j c_{ij}\omega_j) = \sum\nolimits_j c_{ij}\sigma(\omega_j),$$

also

$$\sigma(\beta) \begin{bmatrix} \sigma(\omega_1) \\ \vdots \\ \sigma(\omega_n) \end{bmatrix} \quad = \quad \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \\ c_{n1} & \cdots & c_{nn} \end{bmatrix} \begin{bmatrix} \sigma(\omega_1) \\ \vdots \\ \sigma(\omega_n) \end{bmatrix}$$

Hier sehen wir also, dass der genannte Vektor ein Eigenvektor mit Eigenwert $\sigma(\beta)$ ist. Auch sehen wir, dass die Menge dieser Eigenvektoren $(**)$ nur von der Wahl der Basis $\omega_1, \ldots, \omega_n$, nicht aber von β abhängt.

Wählen wir also für β ein primitives Element α für unsere Körpererweiterung $K : \mathbb{Q}$, also $K = \mathbb{Q}[\alpha]$, so sind die zugehörigen Eigenwerte $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ paarweise verschieden, also sind die genannten Eigenvektoren linear unabhängig und bilden demnach einen Basis von $\mathbb{C}^n$.

Für jedes β folgt, dass die komplexen Zahlen $\sigma_1(\beta), \ldots, \sigma_n(\beta)$ genau die Eigenwerte von $(\beta\cdot)$ (mit den richtigen Vielfachheiten) sind.