Endliche Körper und Codierung

Vorlesung von Sophie Frisch

SS 2008

Inhaltsverzeichnis

1 Körpererweiterungen

Definition 1.1: $F : K$ Körpererweiterung heißt K, F Körper, $K \subseteq F$.

Anmerkung: $F : K$ Körpererweiterung $\Rightarrow F$ ist K–Vektorraum. Einschränkung der Multiplikation von F auf $\cdot K \times F \to F$ ist Skalarmultiplikation, $(F, +)$ mit dieser Skalarmultiplikation erfüllt Axiome eines K–Vektorraums.

Definition 1.2: $[F : K] := \dim_K F$ heißt *Index* der Körpererweiterung $F : K$.

Lemma 1.1: $K \subseteq E \subseteq F$ Körper $\Rightarrow [F : K] = [F : E] \cdot [E : K]$.

Beweis. Sei B K–Basis von E und C eine E–Basis von F. Zeigen: Die Ausdrücke $b \cdot c$ für $b \in B, c \in C$ sind für verschiedene Paare (b, c) paarweise verschieden und bilden eine K–Basis von F. Es folgt dann $\dim_K F = \left|\{b \cdot c \mid b \in B, c \in C\}\right| = |B \times C| = |B| \cdot |C| = \dim_K E \cdot \dim_E F$.

- Erzeugendensystem: gegeben $f \in F$, dann

$$\exists e_c \in E : \quad f = \sum_{c \in C} e_c c$$

wobei nur endlich viele $e_c \neq 0$ sind. Weiters existieren für jedes e_c Koeffizienten (davon nur endlich viele $\neq 0$)

$$k_{c,b} \in K : \quad e_c = \sum_{b \in B} k_{c,b} b$$

Also

$$f = \sum_{c \in C} e_c c = \sum_{c \in C} \sum_{b \in B} k_{c,b} bc$$

wobei nur endlich viele $k_{c,b} \neq 0$. Haben: jedes f ist K–Linearkombination von Elementen $b \cdot c$ mit $b \in B, c \in C$.

- Elemente $b \cdot c$ K–linear unabhängig und paarweise verschieden. Gegeben endlich viele Elemente aus $B \times C$, seien $b_1, \ldots, b_k$ alle vorkommenden B–Koordinaten, $c_1, \ldots, c_m$ alle vorkommenden C–Koordinaten, zeigen $(b_i, c_j), i = 1, \ldots, k,\ j = 1, \ldots, m$ sind K–linear unabhängig. Angenommen

$$0 = \sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq m}} k_{ij} b_i c_j = \sum_{1 \leq j \leq m} \underbrace{\left(\sum_{1 \leq i \leq k} k_{ij} b_i \right)}_{\in E} c_j$$

Da C E–l.u. $\Rightarrow \forall j : \sum_{1 \leq i \leq k} k_{ij} b_i = 0$ Da B K–l.u. $\Rightarrow \forall i, j : k_{ij} = 0$ ✓

□

Definition 1.3: $K \subseteq F$ Körper, $S \subseteq F$ Menge, dann sei $K[S]$ der von $K \cup S$ erzeugte Unterring von F, definiert als

$$K[S] := \bigcap_{\substack{R \text{ Ring} \\ K \cup S \subseteq R \subseteq F}} R$$

und $K(S)$ der von $K \cup S$ erzeugte Unterkörper von F definiert als

$$K(S) = \bigcap_{\substack{E \text{ Körper} \\ K \cup S \subseteq E \subseteq F}} E$$

Schreibe $K[s_1, \ldots, s_n]$ für $K[\{s_1, \ldots, s_n\}]$ und $K(s_1, \ldots, s_n)$ für $K(\{s_1, \ldots, s_n\})$.

Lemma 1.2: $K \subseteq F$ Körper, $S \subseteq F$ Menge, $s_1, \ldots, s_n, s \in F$. Dann

1. $K[s] = \{f(s) \mid f \in K[x]\} = \{a_0 + a_1 s + \ldots + a_n s^n \mid n \in \mathbb{N}_0, a_i \in K\}$
2. $K[s_1, \ldots, s_n] = \{f(s_1, \ldots, s_n) \mid f \in K[x_1, \ldots, x_n]\}$
3. $K[S] = \{f(s_1, \ldots, s_n) \mid n \in \mathbb{N}_0, s_1, \ldots, s_n \in S, f \in K[x_1, \ldots, x_n]\}$
4. $K(s) = \{\frac{f(s)}{g(s)} \mid f, g \in K[x], g(s) \neq 0\}$, $\frac{f(s)}{g(s)} = f(s) \cdot g(s)^{-1}$ (Inverses Element in F)
5. $K(s_1, \ldots, s_n) = \{\frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} \mid f, g \in K[x_1, \ldots, x_n], g(s_1, \ldots, s_n) \neq 0\}$
6. $K(S) = \{\frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} \mid n \in \mathbb{N}_0, s_1, \ldots, s_n \in S, f, g \in K[x_1, \ldots, x_n], g(s_1, \ldots, s_n) \neq 0\}$

Beweisskizze. Sei M die Menge rechts, zuerst zeigen: M enthält $K \cup S$ und ist Unterring (1,2,3) bzw Unterkörper (4,5,6) von F. Zeigt: $0 \in M$, $a, b \in M \Rightarrow a - b \in M$, $a, b \in M \Rightarrow a \cdot b \in M$. in 4,5,6 noch: $1 \in M$, $a, b \in M, b \neq 0 \Rightarrow a \cdot b^{-1} \in M$. Damit ist M unter den Objekten, die in Definition von $K[S]$ bzw $K(S)$ geschnitten werden, also $M \supseteq K[S]$ bzw $M \supseteq K(S)$.
Zweitens zu zeigen: jeder Unterring (bzw Unterkörper) von F, der $K \cup S$ enthält, enthält ganz M; das gilt, weil man M aus $K \cup S$ durch Operationen, bezüglich derer Ringe / Körper abgeschlossen sind, bekommt. Also $M \subseteq K[S]$, bzw $M \subseteq K(S)$. □

Definition 1.4: $K \subseteq F$ Körper, $v \in F$. v heißt *algebraisch über* K, wenn $\exists\, f \in K[x], f \neq 0$ mit $f(v) = 0$. v heißt *transzendent über* K, wenn v nicht algebraisch über K, dh. wenn aus $f(v) = 0$ mit $f \in K[x]$ folgt $f = 0$.

Satz 1.3 (Einfache transzendente Körpererweiterung)**:** Sei $K \subseteq F$, $v \in F$, v transzendent über K, dann $K(v) \simeq K(x)$ mittels eines Isomorphismus $\varphi : K(x) \to K(v)$ mit $\varphi\big|_K = \mathrm{id}_K$ und $\varphi(x) = v$. ($K(x)$ der "Körper der rationalen Funktionen über K", dh. $K(x)$ Quotientenkörper des Polynomrings $K[x]$)

Beweis. Einsetzen $\varphi : K[x] \to F$ mit $\varphi\big|_K = \mathrm{incl}_{K \hookrightarrow F}$ ($\forall\, k \in K : \varphi(k) = k$) und $\varphi(x) = v$. $\mathrm{Im}\, \varphi = \{f(v) \mid f \in K[x]\} = K[v]$, $\ker \varphi = (0)$ da v transzendent über K. Da jedes Element aus

$K[x] \setminus \{0\}$ von φ auf eine Einheit abgebildet wird, kann man φ zu $\overline{\varphi}(x) : K(x) \to F$ fortsetzen, wobei $\overline{\varphi}$ wieder injektiv, und so aussieht:

$$\overline{\varphi}\left(\frac{f}{g}\right) = \varphi(f)(\varphi(g))^{-1} = f(v)g(v)^{-1} = \frac{f(v)}{g(v)}$$

Damit ist

$$\operatorname{Im}\overline{\varphi} = \left\{\frac{f(v)}{g(v)} \mid f, g \in K[x]\right\} = K(v)$$

$\ker\overline{\varphi} = (0)$, also $\overline{\varphi} : K(x) \to K(v)$ Isomorphismus mit $\overline{\varphi}(k) = k, \overline{\varphi}(x) = v$. $\square$

Anmerkung: Haben verwendet: R kommutativer Ring, S multiplikativ $\subseteq R$, $\varphi : R \to T$ Ringhomomorphismus, sodass $\forall\, s \in S : \varphi(s)$ Einheit $\in T$, dann $\exists!\, \overline{\varphi} : R_S \to T$ mit $\overline{\varphi}\big|_R = \varphi$ nämlich $\overline{\varphi}\left(\frac{r}{s}\right) = \varphi(r)(\varphi(s))^{-1}$, und wenn φ injektiv, dann auch $\overline{\varphi}$.

Satz 1.4 (Einfache algebraische Körpererweiterungen)**:** $K \subseteq F$ Körper, $v \in F$ algebraisch über K. Dann:

1. $\exists!$ normiertes Polynom $g \in K[x]$, sodass

   $$\forall\, f \in K[x] : f(v) = 0 \Leftrightarrow g \mid f \text{ in } K[x]$$

   und dieses g ist irreduzibel in $K[x]$. Dieses g heißt Minimalpolynom von v über K.

2. $K(v) = K[v] \simeq K[x]/(g)$ (g das Minimalpolynom von v über K) wobei

   $$\varphi : K[x]/(g) \to K[v]$$

   definiert durch $\varphi(f + (g)) = f(v)$ ein Ringisomorphismus ist.

3. $\{1, v, v^2, \dots, v^{n-1}\}$ mit $n = \deg g$ bildet K–Basis von $K(v) = K[v]$, insbesondere $[K[v] : K] = \deg g$.

Beweis. Sei $\psi : K[x] \to F$ Einsetzhomomorphismus mit $\psi(k) = k$ für alle $k \in K$ und $\psi(x) = v$, dann $\operatorname{Im}\psi = \{f(v) \mid f \in K[x]\} = K[v]$ und $(0) \neq \ker\psi$ Ideal $\trianglelefteq K[x]$ Hauptidealring, also $\exists g \in K[x] : \ker\psi = (g) = g(x) \cdot K[x]$ (Elemente von $K[x]$ erzeugen dasselbe Ideal $\Leftrightarrow$ wenn sie sich nur um eine Multiplikation mit Konstante $\in K \setminus \{0\}$ unterscheiden $\Rightarrow$ jedes Ideal $\neq (0) \trianglelefteq K[x]$ hat eindeutig bestimmten normierten Erzeuger.) $\ker\psi \neq (0)$ weil v algebraisch über $K \Rightarrow \ker\psi = (g)$, g normiert, eindeutig bestimmt. Eindeutig bestimmtes normiertes g mit $f \in \ker\psi$ (dh. $f(v) = 0$) $\Leftrightarrow f \in (g)$ (dh. $g \mid f$ in $K[x]$). Zeigen g irreduzibel: $\psi : K[x] \to F$ mit $\operatorname{Im}\psi = K[v], \ker\psi = (g)$ nach erstem Isomorphiesatz $K[x]/(g) \simeq K[v]$ Integritätsbereich weil Unterring $\subseteq$ Körper. R kommutativer Ring mit 1 : R/I Integritätsbereich $\Rightarrow I$ Primideal, also (g) Primideal $\trianglelefteq K[x]$. (g) Primideal $\Rightarrow g$ prim; g prim $\Rightarrow g$ irreduzibel.
Zeigen $K[v] = K(v)$: genügt zu zeigen $K[v]$ ist Körper.

$$K[v] \simeq K[x]/(g)$$

(g) irreduzibel $\in K[x]$. g irreduzibel $\Rightarrow$ (g) maximal unter den Hauptidealen $\neq R$. $K[x]$ Hauptidealring $\Rightarrow$ (g) maximales Ideal $\trianglelefteq K[x]$. R kommutativer Ring mit 1, $I \trianglelefteq R \Rightarrow$ (R/I Körper $\Leftrightarrow$ I

maximal) also ${}^{K[x]}/_{(g)}$ Körper, dh. $K[v]$ Körper.
Ad 3: $1, v, \ldots, v^{n-1}$ erzeugt $K[v]$ als K–Vektorraum: jedes Element $\in K[v]$ der Form $f(v)$ für ein $f \in K[x]$ Division mit Rest durch g. $f(x) = q(x)g(x) + r(x) : \deg r < \deg g$ und $f(v) = r(v)$ weil $g(v) = 0$. $f(v) = a_0 + a_1 v + \ldots + a_{n-1} v^{n-1}, a_i \in K$ ✓. K–l.u. Angenommen $k_0 + k_1 v + \ldots + k_{n-1} v^{n-1} = 0$. Sei $h(x) = \sum k_i x^i$. $h(v) = 0$ also $g \mid h$ aber $\deg h < \deg g \Rightarrow h = 0$ alle $k_i = 0$. □

1.1 Adjungieren einer Nullstelle, Zerfällungskörper eines Polynoms

Satz 1.5: Sei $f \in K[x]$, $\deg f \geq 1$. Dann $\exists F : K$ Körpererweiterung mit $[F : K] \leq \deg f$, bzw. mit $[F : K] = \deg f$ wenn f irreduzibel $\in K[x]$, sodass f in F eine Nullstelle u hat, und $F = K[u]$.

Beweis. Sei $F = {}^{K[x]}/_{(f)}$, oBdA f irreduzibel, sonst irreduziblen Faktor von f verwenden. Da f irreduzibel, ist (f) maximales Ideal ($K[x]$ Hauptidealring). (f) maximales Ideal in $K[x] \Rightarrow {}^{K[x]}/_{(f)} = F$ Körper. (Eine isomorphe Kopie von) K ist enthalten in F: $\varphi : K[x] \to {}^{K[x]}/_{(f)}$ kanonische Projektion, dann $\varphi\big|_K : K \to F$ injektiv, da $\ker \varphi = (f)$, $\ker \varphi \cap K = \{0\}$, dh. $\ker \varphi\big|_K = \{0\}$. K also eingebettet in F als Elemente der Form $k + (f)$, $k \in K$. Nullstelle von f in F ist $x + (f)$. Nämlich: $f(x + (f)) = f(x) + (f) = f + (f) = (f) = 0 + (f) = 0_F$. F wird als Ring von $K \cup \{x\}$ erzeugt, da $K[x]$ von $K \cup \{x\}$ erzeugt wird und $F = \operatorname{Im} \varphi$, $\varphi : K[x] \to {}^{K[x]}/_{(f)} = F$ und Ringhomomorphismus ein Erzeugendensystem auf ein Erzeugendensystem abbildet. □

Definition 1.5: $f \in F[x]$, f zerfällt in Linearfaktoren über F (in $F[x]$), wenn in $F[x]$ gilt: $f = c \cdot (x - a_1) \cdot (x - a_2) \cdots (x - a_n)$ mit $a_1, \ldots, a_n \in F$.

Beispiel: Es kann passieren, dass nach Adjungieren einer Nullstelle u das Polynom in $K[u]$ zerfällt, muss aber nicht. n–tes zyklotomisches Polynom (Kreisteilungspolynom)

$$\varphi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{ggT}(k,n)=1}} \left(x - \mathrm{e}^{\frac{2\pi \mathrm{i}}{n} \cdot k} \right)$$

$\varphi_n \in \mathbb{Z}[x]$, irreduzibel in $\mathbb{Q}[x]$. Sei w eine Nullstelle von φ_n, dann zerfällt φ_n in $\mathbb{Q}[w]$ (andere Nullstellen sind Potenzen von w).

Beispiel: $x^3 - 2$ sei $\sqrt[3]{2}$ die reelle Nullstelle, dann $\mathbb{Q}\left[\sqrt[3]{2}\right] \subseteq \mathbb{R}$ enthält nicht die beiden anderen Nullstellen. f zerfällt nicht in $\mathbb{Q}\left[\sqrt[3]{2}\right]$.

Definition 1.6: $f \in K[x]$, $\deg f \geq 1$, F Körper $\supseteq K$ heißt Zerfällungskörper von f über K, wenn

1. f in $F[x]$ zerfällt und
2. $F = K[u_1, \ldots, u_n]$ mit $u_1, \ldots, u_n$ Nullstellen von f.

Satz 1.6: $f \in K[x]$, $\deg f = n \geq 1$. Dann $\exists F$ Zerfällungskörper von f über K, mit $[F : K] \leq n!$.

Beweis. Induktion nach $n = \deg f$. $n = 1$: $f = ax + b = a\left(x + {}^{b}/_{a}\right) = a\left(x - \left(-{}^{b}/_{a}\right)\right)$ mit $-{}^{b}/_{a} \in K$, f zerfällt über $K = K\left[-{}^{b}/_{a}\right]$. $n - 1 \to n$: $\deg f = n > 1$, adjungieren Nullstelle u von F: in $K[u]$

gilt $f = (x-u)g(x)$, $g(x) \in K[u][x]$, $\deg g \leq n-1$. Nach Induktionsvoraussetzung $\exists\, F$ Zerfällungskörper von g über $K[u]$, $F = K[u][u_1, \ldots, u_k] = K[u, u_1, \ldots, u_k]$; u_i Nullstelle von g, also von f, g zerfällt in F also auch f: F Zerfällungskörper von f über K. □

Zwei Arten, endliche Körper zu konstruieren, beide ausgehend von $\mathbb{Z}_p$ (p prim) als p-elementigem Körper:

1. zeigen, dass es für jedes $n \in \mathbb{N}$ ein irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ mit $\deg f = n$ gibt, dann Nullstelle von f adjungieren, erhält $F = \mathbb{Z}_p[u]$ mit $[F : \mathbb{Z}_p] = n$, F ist n–dimensionaler $\mathbb{Z}_p$–Vektorraum $\Rightarrow F$ hat p^n Elemente.
2. F mit $[F : \mathbb{Z}_p] = n$ (und daher $|F| = p^n$) konstruieren als Zerfällungskörper von $x^{p^n} - x$ über $\mathbb{Z}_p$.

Hier zuerst 2, dazu vorher noch einige Tatsachen über mehrfache Nullstellen zeigen.

1.2 Mehrfache Nullstellen, formale Ableitung

Definition 1.7: $f \in K[x]$, $f = a_0 + a_1x + \ldots + a_nx^n$. Die (formale) Ableitung von f ist f' mit

$$f' = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1} = \sum_{k=1}^{\deg f} ka_kx^{k-1}$$

Anmerkung: Aus $f' = 0$ folgt im allgemeinen nicht, dass f konstant ist, beispielsweise x^p in $\mathbb{Z}_p[x]$ ergibt in der Ableitung das Nullpolynom.

Definition 1.8: $f \in K[x]$, $u \in K$ heißt *mehrfache Nullstelle* von f, wenn $(x-u)^2 \mid f$ in $K[x]$, und für eine Nullstelle u von f heißt das maximale m mit $(x-u)^m \mid f$ die *Vielfachheit* der Nullstelle u.

Satz 1.7: $f \in K[x]$, $u \in K$. u ist mehrfache Nullstelle von $f \Leftrightarrow u$ ist Nullstelle von f und von f'.

Beweis. "$\Rightarrow$" $f(x) = (x-u)^2g(x)$, $f'(x) = 2(x-u)g(x) + (x-u)^2g'(x)$ mit Einsetzhomomorphismus $f'(u) = 0$, $f(u) = 0$.
"$\Leftarrow$" angenommen u ist einfache Nullstelle, dh. $f(x) = (x-u)g(x)$, $(x-u) \nmid g$, dann u keine Nullstelle von g; $f' = g(x) + (x-u)g'(x)$ mit Einsetzhomomorphismus $f'(u) = g(u) \neq 0$. □

Satz 1.8: $f \in K[x]$. f hat in irgendeinem Erweiterungskörper $F \supseteq K$ eine mehrfache Nullstelle $\Leftrightarrow \operatorname{ggT}(f, f') \neq 1$ (in $K[x]$).

Anmerkung: $f, g \in K[x]$, dann ist der in $K[x]$ vorhandene $\operatorname{ggT}(f, g)$ auch $\operatorname{ggT}(f, g)$ als Polynom in $F[x]$ für jeden Körper $F \supseteq K$. Euklidischer Algorithmus zur Bestimmung von $\operatorname{ggT}(f, g)$ in $K[x]$ ausgeführt ist gleichzeitig auch der Euklidische Algorithmus in $F[x]$.

Beweis des Satzes. "$\Rightarrow$" f hat in $F \supseteq K$ mehrfache Nullstelle u, dann sei φ das Minimalpolynom von u über K; $f(u) = 0$, $f'(u) = 0 \Rightarrow \varphi \mid f$, $\varphi \mid f'$. φ nichtkonstantes Polynom $\in K[x]$, das f, f' und daher $\operatorname{ggT}(f, f')$ teilt, $\operatorname{ggT}(f, f') \neq 1$.

"$\Leftarrow$" f, f' haben nichtkonstanten gemeinsamen Faktor g, im Zerfällungskörper von g haben f, f' gemeinsame Nullstelle, also f eine mehrfache Nullstelle. □

1.3 Charakteristik eines Ringes

Definition 1.9: R Ring, dann sei der *Annihilator* von R in $\mathbb{Z}$, $\operatorname{Ann}_{\mathbb{Z}} R = \{k \in \mathbb{Z} \mid \forall\, r \in R : kr = 0\}$. Dann $\operatorname{Ann}_{\mathbb{Z}} R \trianglelefteq \mathbb{Z}$, daher $\exists!\, n \in \mathbb{N}_0$, $\operatorname{Ann}_{\mathbb{Z}} R = n\mathbb{Z}$. Dieses n ist $\chi(R)$. $\chi(R)$ heißt *Charakteristik* von R.

Lemma 1.9: R nullteilerfrei $\Rightarrow \chi(R) = 0$ oder $\chi(R) = p$, p prim.

Beweis. Angenommen $\chi(R) = n \cdot m$, $1 < n, m < n \cdot m$. Konstruieren Nullteiler: Da $1 < n < \chi(R)$: $\exists\, r \in R :\ n \cdot r \neq 0$, analog $\exists\, s \in R :\ m \cdot s \neq 0$. $(nr)(ms) = (nm)(rs) = 0$, also nr, ms Nullteiler ✓ □

Korollar 1.10: Insbesondere hat jeder Körper Charakteristik 0 oder p prim.

Definition 1.10: Für Ring R mit 1 ist der *Primring* von R der von 1 erzeugte Unterring von R. Für Körper K ist der *Primkörper* der von 1 erzeugte Unterkörper von K.

Lemma 1.11: R Ring mit 1, $\chi(R) = 0 \Rightarrow$ Primring $\simeq \mathbb{Z}$. $\chi(R) = n \in \mathbb{N} \Rightarrow$ Primring $\simeq \mathbb{Z}_n$. K Körper: $\chi(K) = 0 \Rightarrow$ Primkörper $\simeq \mathbb{Q}$, $\chi(K) = p \Rightarrow$ Primkörper $\simeq \mathbb{Z}_p$.

Anmerkung: Da die additiven Vielfachen von 1 und -1 bezüglich Multiplikation abgeschlossen sind, ist die von 1 erzeugte Untergruppe von $(R, +)$ ein Ring, also der kleinste Ring, der 1 enthält, dh. der Primring. Im Ring mit 1 gilt für $k \in \mathbb{Z}$: $(\forall\, r \in R :\ kr = 0) \Leftrightarrow k1_R = 0$ $(r = 1r; k(1r) = (k1)r = 0)$, daher gilt in Ring mit 1: Wenn $\chi(R) \in \mathbb{N}$, dann ist $\chi(R)$ die Ordnung von 1 in der Gruppe $(R, +)$, und wenn $\chi(R) = 0$, dann ist die Ordnung von 1 in $(R, +)$ unendlich. Also ist der von 1 erzeugte Unterring im Falle $\chi(R) = n \in \mathbb{N}$ isomorph zu $\mathbb{Z}_n$ und im Falle $\chi(R) = 0$ isomorph zu $\mathbb{Z}$. Primkörper: Wenn $\chi(K) = p$, dann ist der von 1 erzeugte Ring $\mathbb{Z}_p$, also Körper, also der Primkörper. Wenn $\chi(K) = 0$, dann $\mathbb{Z} \subseteq K$, wegen Fortsetzbarkeit der Inklusion $\mathbb{Z} \hookrightarrow K$ auf Quotientenkörper $\mathbb{Q}$ ist $\mathbb{Q}$ in K eingebettet und besteht aus Ausdrücken $r \cdot s^{-1}$ mit r, s aus dem Primring, der in jedem Unterkörper von K enthalten ist, also diese Kopie von $\mathbb{Q}$ Primkörper.

Korollar 1.12: Jeder endliche Körper hat als Charakteristik eine Primzahl p.

2 Endliche Körper

Kennen schon $\mathbb{Z}_p$ für p prim als Körper: jede Restklasse $\neq 0$ in $\mathbb{Z}_p$ ist invertierbar: $\mathrm{ggT}(k,p) = 1 \Rightarrow \exists a, b \in \mathbb{Z} : 1 = ak + bp$, in $\mathbb{Z}_p$: $1 = a \cdot k$, a invers zu k.
Lemma 2.1: Jeder endliche Körper K hat p^n Elemente für ein p prim und $n \in \mathbb{N}$, nämlich für $p = \chi(K)$ und $n = \dim_{\mathbb{Z}_p} K$.

Beweis. Wissen: $\chi(K) = p$ prim, daher enthält K als Primring eine Kopie von $\mathbb{Z}_p$ (Körper), also K $\mathbb{Z}_p$–Vektorraum. $\dim_{\mathbb{Z}_p} K = n$ endlich (da K endlich), und wenn $\dim_{\mathbb{Z}_p} K = n$, dann $|K| = p^n$ (n–elementige Basis, jedes Element eindeutig als $\mathbb{Z}_p$–Linearkombination der Basiselemente darstellbar, p^n Möglichkeiten für die Koeffizienten). $\square$

2.1 Frobenius–Homomorphismus

Lemma 2.2 ("Freshman's Dream")**:** In einem kommutativen Ring R mit $\chi(R) = p$ gilt für $a, b \in R:\ (a+b)^p = a^p + b^p$.

Anmerkung: Binomischer Lehrsatz:

$$(a+b)^p = a^p + \sum_{1<k<p} \binom{p}{k} a^k b^{p-k} + b^p$$

und für $1 < k < p$ ist $\binom{p}{k}$ eine durch p teilbare ganze Zahl.

Korollar 2.3: K Körper mit $\chi(K) = p$, dann ist $\varphi : K \to K$ mit $\varphi(x) = x^p$ ein injektiver Endomorphismus von K.

Beweis.

- Homomorphismus: $(a+b)^p = a^p + b^p$; $(ab)^p = a^p \cdot b^p$ ✓
- injektiv: allgemein: ein Ringhomomorphismus $\varphi : K \to R$ (K Körper) ist entweder injektiv oder konstant 0, weil $\ker \varphi$ Ideal von K, einige Ideale von K sind (0) ($\to \varphi$ injektiv) und K ($\to \varphi$ konstant 0). Dieses φ mit $\varphi(x) = x^p$ nicht konstant 0, da $\varphi(1) = 1$.

$\square$

Anmerkung: $\varphi : K \to K$ mit $\varphi(x) = x^p$ wobei $\chi(K) = p$ heißt Frobenius–Homomorphismus.

Anmerkung: Frobenius–Homomorphismus nicht immer surjektiv: zB $\varphi : \mathbb{Z}_p(x) \to \mathbb{Z}_p(x)$ nicht surjektiv, x ist keine p–te Potenz.

Anmerkung: K endlicher Körper mit $\chi(K) = p$, dann Frobenius–Homomorphismus $\varphi : K \to K$, $\varphi(x) = x^p$ Automorphismus (K endlich, $\varphi : K \to K$ injektiv $\to$ auch surjektiv)

Lemma 2.4: K Körper, $f : K \to K$ Automorphismus von K, dann bildet

$$\mathrm{Fix}(f) = \{k \in K : f(k) = k\}$$

einen Körper.

Lemma 2.5: Sei K endlicher Körper mit q Elementen ($|K| = q$), dann gilt $\forall\, a \in K : a^q = a$ (insbesondere gilt in $\mathbb{Z}_p : a^p = a$).

Beweis. Für $a = 0$ ist $0^q = 0$ sowieso, für $a \neq 0$ gilt a Einheit; Einheitengruppe $(K \setminus \{0\}, \cdot) = G$ ist Gruppe mit $|G| = q - 1$. Für jedes Gruppenelement gilt $a^{q-1} = 1$, daher $a^q = a$. $\square$

Satz 2.6: Sei K Körper mit $|K| = q$, $n \in N$ gegeben. Dann $\exists\, F$ Körper mit $K \subseteq F$, $|F| = q^n$. (Insbesondere folgt aus der Existenz eines Körpers mit p Elementen die Existenz eines Körpers mit p^n Elementen für beliebiges n).

Beweis. Sei F Zerfällungskörper von $x^{q^n} - x$ über K. Sei $N = \{a \in F \mid a^{q^n} = a\}$ die Menge der Nullstellen von $x^{q^n} - x$ in F. Da N die Menge der Fixpunkte von $\varphi^n = \varphi \circ \ldots \circ \varphi$ (φ Frobenius–Homomorphismus) ist N Körper. Da $\forall\, a \in K$ ist $a^q = a$ und durch iterieren $a^{q^n} = a$ folgt $K \subseteq N$. Also ist N Körper mit $K \subseteq N$, N erzeugt von K und Nullstellen von $x^{q^n} - x$, sodass $x^{q^n} - x$ über N zerfällt. Daher $N = F$ Zerfällungskörper von $x^{q^n} - x$ über K. Außerdem hat $x^{q^n} - x$ in N keine mehrfache Nullstelle, da $(x^{q^n} - x)' = q^n x^{q^n - 1} - 1 = -1$ ($\chi(K) = p$, q Potenz von p) Also hat $x^{q^n} - x$ in seinem Zerfällungskörper q^n verschiedene Nullstellen $\to$ $|N| = q^n$. $N = F$ hat q^n Elemente $\checkmark$. $\square$

Anmerkung: D Integritätsbereich, $f \in D[x]$, dann hat f in D höchstens $\deg f$ Nullstellen.

Satz 2.7: F Körper, G endliche Untergruppe von $(F \setminus \{0\}, \cdot)$. Dann ist G zyklisch.

Korollar 2.8: Insbesondere gilt für jeden endlichen Körper K: $(K \setminus \{0\}, \cdot)$ zyklisch.

Beweis 1. G endliche Abelsche Gruppe, nach Struktursatz $G \simeq Z_{m_k} \times \mathbb{Z}_{m_{k-1}} \times \ldots \times \mathbb{Z}_{m_1}$, $m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$. Sei $|G| = n$, da für jedes $g \in G = Z_{m_k} \times \mathbb{Z}_{m_{k-1}} \times \ldots \times \mathbb{Z}_{m_1}$ gilt $g^{m_k} = 1$ ist jedes $g \in G$ Nullstelle von $x^{m_k} - 1$ also $|G| \leq m_k$, gleichzeitig $|G| = m_k \cdot m_{k-1} \cdots m_1 \Rightarrow |G| = m_k$ daher $G = \mathbb{Z}_{m_k}$. $\square$

Beweis 2. Verwenden wieder $\forall\, d \in \mathbb{Z}$ hat $x^d - 1$ höchstens d Nullstellen in F, also in G höchstens d Elemente mit $g^d = 1$. Daher hat G für jeden Teiler $d \mid |G|$ höchstens eine zyklische Untergruppe der Ordnung d. Daher hat G für jeden Teiler $d \mid |G|$ höchstens $\varphi(d)$ Elemente der Ordnung d. Da

$$|G| = \sum_{d \mid |G|} \#\{g \in G \mid \operatorname{ord} g = d\} \leq \sum_{d \mid |G|} \varphi(d) = |G|$$

Also Gleichheit, die nur gelten kann, wenn für alle $d \mid |G|$ die Anzahl der $g \in G$ mit $\operatorname{ord} g = d$ genau $\varphi(d)$ ist. Insbesondere hat G $\varphi(|G|) > 0$ Elemente der Ordnung $|G|$ und G ist zyklisch. $\square$

Korollar 2.9: K endlicher Körper mit $|K| = q = p$ (p prim), dann $\exists\, u \in K$ mit $K = \mathbb{Z}_p[u]$ (dh. $K = \mathbb{Z}_p$ ist einfache algebraische Erweiterung, dh. erzeugt von einem Element)

Beweis. Wähle u als Erzeuger von $(K \setminus \{0\}, \cdot)$. u algebraisch über $\mathbb{Z}_p$, da $u^q - u = 0$, u erzeugt K über $\mathbb{Z}_p$, da $0 \in \mathbb{Z}_p$ und jedes $a \in K \setminus \{0\}$ ist Potenz von u. $\square$

Korollar 2.10: $E \subseteq F$ endlicher Körper $\Rightarrow$ $\exists\, u \in F : F = E[u]$ (wähle u als Erzeuger von $(F \setminus \{0\}, \cdot)$).

Korollar 2.11: E endlicher Körper, $n \in \mathbb{N}$. Dann $\exists$ irreduzibles Polynom $f \in E[x]$ mit $\deg f = n$.

Beweis. Betrachte $F : E$ mit $[F : E] = n$ ($|E| = q, |F| = q^n$). Da $F = E[u]$ folgt $[F : E] = \deg f$, f Minimalpolynom von u über E. (Satz über einfache algebraische Körpererweiterungen). $\square$

Werden in Kürze sehen, dass es für jede Primzahlpotenz p^n (bis auf Isomorphie) genau einen Körper mit p^n Elementen gibt. Vorhergehendes Korollar gibt eine Darstellung des Körpers mit p^n Elementen als $K = \mathbb{Z}_p[x]/(f)$ mit f beliebig irreduzibel $\in \mathbb{Z}_p[x]$ mit $\deg f = n$. Rechnen mit Körperelementen wie mit Polynomen (Addition, Multiplikation) und Rest mod f mit $r < \deg f$ bilden. Elemente von K dargestellt als Repräsentantensystem: $\{g \in \mathbb{Z}_p[x] \mid \deg g < n\}$ sind Repräsentantensystem von $K = \mathbb{Z}_p[x]/(f)$.

2.2 Fortsetzbarkeit von Körperisomorphismen

Lemma 2.12: Seien K, F Körper, $\varphi : K \to F$ Körperisomorphismus, dann ist $\overline{\varphi} : K[x] \to F[x]$ mit $\overline{\varphi}(a_0 + a_1 x + \ldots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$ Isomorphismus der Polynomringe und $\overline{\overline{\varphi}} : K(x) \to F(x)$ definiert durch $\overline{\overline{\varphi}}\left(\frac{f}{g}\right) = \frac{\overline{\varphi}(f)}{\overline{\varphi}(g)}$ Isomorphismus der Körper der rationalen Funktionen. (Bezeichnen oft $\overline{\varphi}, \overline{\overline{\varphi}}$ einfach als φ).

Beweisskizze. $\overline{\varphi}$ Einsetzhomomorphismus mit $\overline{\varphi}\big|_K = \varphi$, $\overline{\varphi}(x) = x$, offensichtlich $\overline{\varphi}$ bijektiv. $\overline{\varphi}$ bildet alle Elemente von $K[x] \setminus \{0\}$ auf Einheiten in $F(x)$ ab. ($\overline{\varphi}$ als Homomorphismus $K[x] \to F(x) \supseteq F[x]$ betrachten). Daher $\overline{\varphi}$ fortsetzbar zu Homomorphismus $\overline{\overline{\varphi}} : K(x) \to F(x)$ ($K(x)$ ist Quotientenkörper $(K[x] \setminus \{0\})^{-1}K[x]$ von $K[x]$) wobei die Fortsetzung $\overline{\overline{\varphi}}\left(\frac{f}{g}\right) = \frac{\overline{\varphi}(f)}{\overline{\varphi}(g)}$ ist und $\overline{\overline{\varphi}}$ injektiv, da $\overline{\varphi}$ injektiv. Surjektivität: jedes der Elemente von $F(x)$ ist von der Form $\frac{\varphi(a_0)+\ldots+\varphi(a_n)x^n}{\varphi(b_0)+\ldots+\varphi(b_m)x^m}$, da φ surjektiv: $K \to F$. $\square$

Proposition 2.13 (Fortsetzbarkeit von Isomorphismen auf einfache transzendente Körpererweiterungen)**:** K, F Körper, $\varphi : K \to F$ Körperisomorphismus, $K \subseteq E, F \subseteq L$ Körpererweiterungen mit $u \in E$ transzendent über K und $v \in L$ transzendent über F. Dann existiert genau ein Isomorphismus: $K(u) \simeq F(v)$ via $\overline{\varphi} : K(u) \to F(v)$ mit $\overline{\varphi}\big|_k = \varphi$ und $\overline{\varphi}(u) = v$.

Beweis. Nach Satz über einfache transzendente Körpererweiterungen $\exists\, \psi : K(x) \to K(u)$ mit $\psi\big|_K = \mathrm{id}$, $\psi(x) = u$, analog $\exists\, \theta : F(x) \to F(v)$ mit $\theta\big|_F = \mathrm{id}$, $\theta(x) = v$. $K(u) \xrightarrow{\psi^{-1}} K(x) \xrightarrow{\varphi} F(x) \xrightarrow{\theta} F(v)$; der gewünschte Isomorphismus: $\theta \circ \varphi \circ \psi^{-1} : K(u) \to F(v)$. $\square$

Satz 2.14 (Fortsetzbarkeit von Isomorphismen auf einfache algebraische Erweiterungen)**:** K, F Körper, $K \subseteq E, F \subseteq L$ Körpererweiterungen; $\varphi : K \to F$ Körperisomorphismus, $u \in E$ Nullstelle von f irreduzibel $\in K[x]$, $v \in L$ Nullstelle von $\varphi(f) \in F[x]$, dann existiert genau ein Isomorphismus $\overline{\varphi} : K[u] \to F[v]$ mit $\overline{\varphi}\big|_K = \varphi$ und $\overline{\varphi}(u) = v$.

Beweis. f irreduzibel $\to$ f bis auf multiplikative Konstante $\in K \setminus \{0\}$ gleich Minimalpolynom von u über K. f erzeugt dasselbe Ideal von $K[x]$ wie das Minimalpolynom von u über K. f irreduzibel, $\varphi : K[x] \to F[x]$ Isomorphismus $\to$ $\varphi(f)$ irreduzibel, daher: $\varphi(f)$ erzeugt dasselbe Ideal von $F[x]$ wie das Minimalpolynom von v über F. Nach Satz über einfache algebraische Körpererweiterungen:

$$K[u] \xrightarrow{\psi^{-1}} {}^{K[x]}/_{(f)} \xrightarrow{\tilde{\varphi}} {}^{F[x]}/_{(\varphi(f))} \xrightarrow{\theta} F[v]$$

$\exists\, \psi : {}^{K[x]}/_{(f)} \to K[u]$ Isomorphismus mit $\psi(k+(f)) = k$ und $\psi(x+(f)) = u$, $\exists\, \theta : {}^{F[x]}/_{(\varphi(f))} \to F[v]$ mit $\theta(a + (\varphi(f))) = a$ für alle $a \in F$ und $\theta(x + (\varphi(f))) = v$. Außerdem ist $\tilde{\varphi} : {}^{K[x]}/_{(f)} \to {}^{F[x]}/_{(\varphi(f))}$ definiert durch $\tilde{\varphi}(g+(f)) = \varphi(g) + (\varphi(f))$ ein Isomorphismus (weil $\varphi : K[x] \to F[x]$ Isomorphismus und allgemein, wenn $\varphi : R \to S$ Ringisomorphismus und $I \trianglelefteq R$ dann $\tilde{\varphi} : {}^{R}/_{I} \to {}^{S}/_{\varphi(I)}$ definiert durch $\tilde{\varphi}(r+I) = \varphi(r) + \varphi(I)$ Ringisomorphismus). Schließlich ist $\theta \circ \tilde{\varphi} \circ \psi^{-1} : K[u] \to F[v]$ Isomorphismus mit $\overline{\varphi}\big|_K = \varphi$ und $\overline{\varphi}(u) = v$. □

Satz 2.15: K, F Körper, $\varphi : K \to F$ Körperisomorphismus, f irreduzibel $\in K[x]$, E Zerfällungskörper von f über K. L Zerfällungskörper von $\varphi(f)$ über $F[x]$. Dann $\exists\, \overline{\varphi} : E \to L$ Isomorphismus mit $\overline{\varphi}\big|_K = \varphi$.

Satz 2.16 (Fortsetzung von Körperisomorphismen auf Zerfällungskörper eines Polynoms)**:** $\varphi : K \to F$ Körperisomorphismus, $f \in K[x]$ ($\deg f \geq 1$), E Zerfällungskörper von f über K, L Zerfällungskörper von $\varphi(f)$ über F. Dann $\exists\, \overline{\varphi} : E \to L$ Körperisomorphismus mit $\overline{\varphi}\big|_K = \varphi$.

Beweis. Induktion nach $[E : K]$ (endlich, da $\leq (\deg f)!$).
$[E : K] = 1$ heißt $E = K$, f zerfällt über K: $f = a(x - b_1) \cdots (x - b_n)$ mit $a, b_i \in K$. Da φ Körperhomomorphismus, ist $\varphi(f) = \varphi(a)(x - \varphi(b_1)) \cdots (x - \varphi(b_n))$ und $\varphi(f)$ zerfällt über F, also F Zerfällungskörper von $\varphi(f)$ über F, $\overline{\varphi} = \varphi$ Isomorphismus zwischen den beiden Zerfällungskörpern.
$[E : K] > 1$:

$$\begin{aligned} E &\xrightarrow{\overline{\varphi}} L \\ K(b) &\xrightarrow{\psi} F(\varphi(b)) \quad \text{laut Induktionsvoraussetzung} \\ K &\xrightarrow{\varphi} F \quad \text{Fortsetzung von } \varphi \text{ auf einfache Erweiterung} \end{aligned}$$

f zerfällt nicht über K; sei $b \in F \setminus K$ Nullstelle von f und zwar b Nullstelle eines irreduziblen Faktors $g \in K[x]$ von f. Dann $\varphi(b)$ Nullstelle von $\varphi(g)$ irreduzibel $\in F[x]$ mit $\varphi(g) \mid \varphi(f)$ (weil φ Homomorphismus). Können φ fortsetzen zu $\psi : K[b] \to K[\varphi(b)]$ Isomorphismus mit $\psi\big|_K = \varphi$. Da $[K(b) : K] > 1$, ist $[E : K(b)] < [E : K]$. E ist Zerfällungskörper von f auch über $K(b)$, L Zerfällungskörper von $\varphi(f)$ auch über $F(\varphi(b))$, ψ fortsetzbar nach Induktionsvoraussetzung zu $\overline{\varphi} : E \to L$ Körperisomorphismus mit $\overline{\varphi}\big|_{K(b)} = \psi$ also $\overline{\varphi}\big|_K = \psi\big|_K = \varphi$. □

Lemma 2.17: $E \subseteq F$ endlicher Körper, $|E| = q, |F| = q^n$, dann ist F Zerfällungskörper von $x^{q^n} - x$ über E.

Beweis. $|F| = q^n \to$ jedes $a \in F$ erfüllt $a^{q^n} = a$, ist also Nullstelle von $x^{q^n} - x$. Dieses Polynom hat also $\deg f$ verschiedene Nullstellen in F und zerfällt daher über F.
(Verwendet, dass $F[x]$ ZPE-Ring ist, a, b Nullstellen von f, dann f durch $(x - a)$ und durch $(x - b)$ teilbar, daher f durch $\mathrm{kgV}((x - a), (x - b)) = (x - a) \cdot (x - b)$ teilbar; insbesondere $\deg f = n$, f

hat verschiedene Nullstellen $a_1, \ldots, a_n$, dann $f = c \cdot (x - a_1) \cdots (x - a_n)$).
Da F nur aus Nullstellen von $x^{q^n} - x$ besteht und E enthält, ist F Zerfällungskörper von $x^{q^n} - x$ über E. □

Korollar 2.18: Je zwei Erweiterungskörper desselben Grades über einem endlichen Körper E sind E-isomorph, dh. E endlicher Körper, $F_1 \supseteq E$, $F_2 \supseteq E$, $[F_1 : E] = [F_2 : E]$, dann $\exists \varphi : F_1 \to F_2$ Körperisomorphismus mit $\varphi\big|_E = \mathrm{id}_E$.
Notation: E-Isomorphismus zwischen zwei Erweiterungskörpern von E ist Körperisomorphismus, der E punktweise fix lässt.

Korollar 2.19: Je zwei endliche Körper mit p^n Elementen sind isomorph (weil beide Zerfällungskörper von $x^{p^n} - x$ über $\mathbb{Z}_p$).

2.3 Nachtrag zu Körpererweiterungen im Allgemeinen

Anmerkung: endlichdimensional $\Leftrightarrow$ algebraisch und endlich erzeugt

Proposition 2.20: $[F : K] = n$ endlich $\to$ $F : K$ algebraisch (jedes Element von F algebraisch von Grad $\leq n$ über K) und F endlich erzeugt über K ($F = K[a_1, \ldots, a_n]$).

Beweis. Je $n + 1$ Elemente von F sind K-linear abhängig, insbesondere für jedes $a \in F$:
$1, a, a^2, \ldots, a^n$ K-linear abhängig, dh. $\exists\, c_0, c_1, \ldots, c_n \in K$ nicht alle 0 mit $c_0 + c_1 a + \ldots + c_n a^n = 0$
$f = \sum_{k=0}^{n} c_k x^k$ ist Polynom $\in K[x] \setminus \{0\}$ mit $f(a) = 0$, $\deg f \leq n$. F erzeugt als K-Vektorraum von n Basiselementen $a_1, \ldots, a_n \in F$, jedes $a \in F$ ist K-Linearkombination der a_i, insbesondere jedes $a \in F$ in $K[a_1, \ldots, a_n]$. □

Proposition 2.21: $K \subseteq F$, $F = K(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in F$ algebraisch über K $\Rightarrow$ $[F : K]$ ist endlich. ("endlich erzeugt von algebraischen Elementen $\Rightarrow$ endlichdimensional")

Beweis. $K_i = K(a_1, \ldots, a_i)$, $K_0 = K$, $K_n = F$, $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{n-1} \subseteq K_n = F$. $K_{i+1} = K_i(a_{i+1})$. a_{i+1} algebraisch über K_i, da algebraisch über K, daher $[K_{i+1} : K_i] = \deg f_i$, f_{i+1} Minimalpolynom von a_{i+1} über K_i, insbesondere endlich. $[F : K] = [F : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K]$ endlich. □

Korollar 2.22: $F : K$, sodass $F = K(S)$, $S \supseteq F$ sodass jedes $s \in S$ algebraisch über K, dann $F : K$ algebraisch.

Beweis. Jedes $a \in F$ ist der Form $a = f(s_1, \ldots, s_n)$ für gewisse $s_1, \ldots, s_n \in S$ (endlich viele!) und $f \in K[x_1, \ldots, x_n]$, daher $a \in K[s_1, \ldots, s_n]$ mit $[K[s_1, \ldots, s_n] : K]$ endlich, daher a algebraisch über K. □

Korollar 2.23: $K \subseteq F$ Körpererweiterung, $E = \{a \in F \mid a \text{ algebraisch über } K\}$, dann E Körper.

Beweis. $E = K(E)$ mit $E \subseteq K(E)$ und andererseits jedes Element von $K(E)$ algebraisch über K, also $K(E) \subseteq E$. □

Beispiel: $\mathbb{A}$ die Menge aller Elemente in $\mathbb{C}$, die algebraisch über $\mathbb{Q}$ sind, dann ist $\mathbb{A} : \mathbb{Q}$ Beispiel einer unendlich-dimensionalen algebraischen Körpererweiterung (unendlich-dimensional, da es nach Eisenstein $\forall n \in \mathbb{N}$ ein $f \in \mathbb{Q}[x]$ irreduzibel mit $\deg f \leq n$ gibt.)

2.4 Algebraischer Abschluss eines Körpers

Definition 2.1: K Körper, $S \subseteq K[x]$ eine Menge von Polynomen mit $\deg \geq 1$, $F \supseteq K$ heißt Zerfällungskörper der Menge S von Polynomen in $K[x]$, wenn

1. jedes $f \in S$ zerfällt über F
2. $F = K(W)$, W besteht nur aus Nullstellen der Polynome $\in S$.

(Für $S = \{f_1, \ldots, f_n\}$ endlich ist der Zerfällungskörper von S über K einfach der Zerfällungskörper von $f_1 \cdot f_2 \cdots f_n$ über K.)

Definition 2.2: K heißt algebraisch abgeschlossen, wenn jedes $f \in K[x]$ mit $\deg f \geq 1$ über K zerfällt (es genügt: jedes $f \in K[x]$ mit $\deg f \geq 1$ hat eine Nullstelle in K).

Definition 2.3: $F \supseteq K$, F heißt algebraischer Abschluss von K, wenn

1. $F : K$ algebraisch
2. F algebraisch abgeschlossen

Anmerkung (Als Übung)*:* $F \supseteq K$. F ist algebraischer Abschluss von $K \Leftrightarrow F$ Zerfällungskörper der Menge aller Polynome $\in K[x]$ mit $\deg \geq 1$ (es genügt: Zerfällungskörper der Menge aller normierten irreduziblen Polynome $\in K[x]$).

Satz 2.24: Der Zerfällungskörper einer beliebigen Menge $S \subseteq K[x]$ über K existiert und ist bis auf K-Isomorphie eindeutig.

Zeige zuerst Eindeutigkeit:
Satz 2.25: $\varphi : K \to F$ Körperisomorphismus, $S \subseteq K[x]$ (mit $\deg f \geq 1$ für alle $f \in S$), E Zerfällungskörper von S über K, L Zerfällungskörper von $\varphi(S) = \{\varphi(f) \mid f \in S\}$ über F. Dann $\exists \overline{\varphi} : E \to L$ Körperisomorphismus mit $\overline{\varphi}\big|_K = \varphi$.

Beweis. Betrachten Menge T aller (E_i, L_i, φ_i) mit $K \subseteq E_i \subseteq E$, $F \subseteq L_i \subseteq L$. $\varphi_i : E_i \to L_i$ Körperisomorphismus mit $\varphi_i\big|_K = \varphi$; geordnet durch $(E_i, L_i, \varphi_i) \leq (E_k, L_k, \varphi_k) \Leftrightarrow E_i \subseteq E_k$, $L_i \subseteq L_k$, $\varphi_k\big|_{E_i} = \varphi_i$. Da jede Kette in dieser Menge T eine obere Schranke in T hat $(\bigcup_{i\in I} E_i, \bigcup_{i\in I} L_i, \bigcup_{i\in I} \varphi_i)$ für $\{(E_i, L_i, \varphi_i) \mid i \in I\}$ Kette. Also hat T maximales Element $(\tilde{E}, \tilde{L}, \tilde{\varphi})$.
Behauptung: $\tilde{E} = E$, $\tilde{L} = L$. Angenommen $\tilde{E} \subsetneqq E$, dann $\exists$ Nullstelle b eines $f \in S$, die in $E \setminus \tilde{E}$ liegt. (Wären alle Nullstellen von Polynomen $\in S$ in $\tilde{E}$, dann wäre $\tilde{E} = E$, da E über K von den Nullstellen erzeugt wird). Dann $\tilde{\varphi}$ zu Isomorphismus $\psi : \tilde{E}(b) \to \tilde{L}(\tilde{\varphi}(b))$ fortsetzbar und $(\tilde{E}(b), \tilde{L}(\tilde{\varphi}(b)), \psi) > (\tilde{E}, \tilde{L}, \tilde{\varphi})$ in T, Widerspruch zur Maximalität. Wenn $\tilde{L} \subsetneqq L$, dann analog $\tilde{\varphi}^{-1} : \tilde{L} \to \tilde{E}$ fortsetzen zu $\psi : \tilde{L}(c) \to \tilde{E}(\tilde{\varphi}^{-1}(c))$. $\square$

Lemma 2.26: K Körper, $F : K$ algebraische Erweiterung, dann

$$|F| \leq \aleph_0 \cdot |K| = \begin{cases} |K| & \text{falls } K \text{ unendlich} \\ \aleph_0 & \text{falls } K \text{ endlich} \end{cases}$$

Beweis. Elemente von F sind Nullstellen von irreduziblen Polynomen $\in K[x]$, jedes Polynom hat nur endlich viele Nullstellen;

$$\begin{aligned} |F| &\leq \left| \sum_{n \in \mathbb{N}} n \cdot \left|\{f \in K[x] \;\middle|\; \deg f = n\}\right| \right| \\ &= \left| \sum_{n \in \mathbb{N}} n \cdot |K|^{n+1} \right| \\ &\leq \aleph_0 \cdot \aleph_0 \cdot |K| \leq \aleph_0 \cdot |K| \end{aligned}$$

□

Satz 2.27: Jeder Körper K hat algebraischen Abschluss $\overline{K}$.

Beweis. Sei S Menge mit $|S| > \aleph_0 \cdot |K|$ (existiert, zB. Potenzmenge von $\mathbb{N} \times K$). K eingebettet als Teilmenge in S: $K \subseteq S$. Betrachten Körpererweiterungen von K, die in S eingebettet sind: $K \subseteq E \subseteq S$, wobei $\cdot : E \times E \to E$, $+ : E \times E \to E$ so definiert sind, dass sie $\cdot : K \times K \to K$, $+ : K \times K \to K$ fortsetzen. Betrachten Menge T aller Tripel $(E, +, \cdot)$ mit $K \subseteq E \subseteq S$, $+, \cdot$ Funktionen $E \times E \to E$, sodass Körperaxiome erfüllt und E algebraisch über K sowie $+, \cdot$ die Operationen $K \times K \to K$ fortsetzen. Axiome der Mengenlehre (Zermelo-Fraenkel, ZF) garantieren, dass T tatsächlich eine Menge ist. Auf T Ordnungsrelation $\leq$ $(E_1, +_1, \cdot_1) \leq (E_2, +_2, \cdot_2)$ wenn $E_1 \subseteq E_2$ und $+_2$ Fortsetzung von $+_1$, $\cdot_2$ Fortsetzung von $\cdot_1$; Zornsches Lemma anwenden: Jede Kette hat obere Schranke $(\bigcup E_i, \bigcup +, \bigcup \cdot)$, also $\exists$ maximales Element von T.
Behauptung: maximales Element $(F, +, \cdot)$ von T ist algebraischer Abschluss von K. $F : K$ algebraisch, da $(F, +, \cdot) \in T$. Angenommen F nicht algebraisch abgeschlossen. Dann sei $E : F$ einfache algebraische Körpererweiterung, $[E : F] = n > 1$. In S ist genug Platz, um eine Kopie von E einzubetten: $|E \setminus F| \leq \aleph_0 \cdot |K|$, $|S \setminus F| > \aleph_0 \cdot |K|$. Verwirklichen E auf eienr Teilmenge von S, die F umfasst, so, dass Multiplikation und Addition von E die Operationen von F fortsetzen, dann $(E, +, \cdot) \in T$ echt größer als $(F, +, \cdot)$, Widerspruch zur Maximalität von $(F, +, \cdot)$. □

Korollar 2.28: K Körper, $S \subseteq K[x]$ (sodass $\forall f \in S : \deg f \geq 1$), dann $\exists F : K$ Zerfällungskörper von S über K.

Beweis. Algebraischen Abschluss $\overline{K}$ bilden, $F = K(W)$ mit $W = \{v \in \overline{K} \mid \exists f \in S : f(v) = 0\}$ ist Zerfällungskörper von S über K. □

2.5 Separable Körpererweiterungen

Definition 2.4: Irreduzibles Polynom $f \in K[x]$ heißt *separabel*, wenn f in seinem Zerfällungskörper über K $\deg f$ viele verschiedene Nullstellen hat (äquivalent: in keiner Körpererweiterung von K eine mehrfache Nullstelle hat).

Anmerkung (Zur Erinnerung)*:* $f \in K[x]$ hat in keiner Erweiterung von K mehrfache Nullstelle $\Leftrightarrow$ $\operatorname{ggT}(f, f') = 1$. Mehrfache Nullstelle $u \Rightarrow$ Nullstelle von f und f', Minimalpolynom von u müsste in $K[x]$ f und f' teilen. Umgekehrt: $\operatorname{ggT}(f, f') = g \neq 1$, im Zerfällungskörper von g mehrfache Nullstelle.

Anmerkung: f irreduzibel $\in K[x] \Rightarrow$ (f hat in irgendeiner Erweiterung von K mehrfache Nullstelle $\Leftrightarrow f' = 0$). Weil für f irreduzibel: $\operatorname{ggT}(f, f') \neq 1 \Leftrightarrow \operatorname{ggT}(f, f') = f$, $f \mid f'$ mit $\deg f' < \deg f \Rightarrow$ $f' = 0$.

Satz 2.29: K Körper. Alle f irreduzibel $\in K[x]$ separabel $\Leftrightarrow \chi(K) = 0 \vee (\chi(K) = p \wedge \psi : K \to K, \psi(x) = x^p$ surjektiv).

Beweis. "$\Leftarrow$" Wenn $\exists f$ irreduzibel nicht separabel, dann $f' = 0$, $a_n \neq 0$,

$$f = \sum_{k=0}^{n} a_k x^k, \quad f' = \sum_{k=1}^{n} k a_k x^{k-1} = 0$$

dh. $\forall\, k : k a_k = 0$. Da K keine Nullteiler hat, folgt $\chi(K) = p \neq 0$ und für alle K mit $a_k \neq 0$ gilt $p \mid k$. Dh. $\chi(K) = p$ prim und

$$f = \sum_{k=0}^{m} a_{kp} x^{kp}$$

Wenn jedes $a \in K$ eine p-te Potenz ist, dann sei b_k, sodass $a_{kp} = (b_k)^p$. Dann

$$f = \sum_{k=0}^{m} (b_k)^p x^{kp} = \left(\sum_{k=0}^{m} b_k x^k \right)^p$$

also f nicht irreduzibel. Also folgt aus Existenz eines nicht separablen irreduziblen Polynoms, dass $K^p \subsetneqq K$, nicht jedes Element von K p-te Potenz.
"$\Rightarrow$" Angenommen $\chi(K) = 0$ und $K^p \subsetneqq K$, dann existiert nicht separables irreduzibles Polynom $\in K[x]$. Sei $a \in K \setminus K^p$, betrachte $f = x^p - a$. Im Zerfällungskörper F von f über K sei b eine Nullstelle von f, dh. b, sodass $b^p = a$, dann

$$f = x^p - a = x^p - b^p = (x - b)^p$$

f hat in seinem Zerfällungskörper über K eine p-fache Nullstelle. ∎

Definition 2.5: Ein Körper heißt *vollkommen* oder *perfekt*, wenn jedes f irreduzibel $\in K[x]$ auch separabel ist.

Anmerkung: Insbesondere: Jeder Körper mit $\chi(K) = 0$ ist perfekt. Jeder endliche Körper ist perfekt.

Beispiel: Beispiele für nicht perfekten Körper: $\mathbb{F}_q(x)$, zB in $\mathbb{Z}_p(x)$ ist x keine p-te Potenz, daher $y^p - x$ ein nicht separables Polynom in $\mathbb{Z}_p(x)[y]$.

Definition 2.6: $F : K$ algebraische Körpererweiterung heißt *separabel*, wenn jedes f irreduzibel $\in K[x]$, das in F eine Nullstelle hat, separabel ist. (Körper perfekt $\Leftrightarrow$ jede algebraische Erweiterung separabel).

Anmerkung: Für nicht algebraische Erweiterungen Separabilität anders definieren.

2.6 Normale Körpererweiterungen

Definition 2.7: $F : K$ Körpererweiterung heißt *normal*, wenn jedes irreduzible $f \in K[x]$, das in F eine Nullstelle hat, über F zerfällt.

Satz 2.30: $F : K$ algebraische Körpererweiterung. Dann ist äquivalent

1. $F : K$ normal
2. F ist Zerfällungskörper einer Menge von Polynomen in $K[x]$ über K
3. $\forall$ K-monomorphen $\psi : F \to \overline{K}$ ($\overline{K}$ der algebraische Abschluss von K) gilt $\psi(F) = F$.

Beweis.

$1 \to 2$ Sei F über K erzeugt von S ($F = K[S]$), dann F Zerfällungskörper der Menge der Minimalpolynome in $K[x]$ der Elemente von S.

$2 \to 3$ F Zerfällungskörper von $\mathcal{F} \subseteq K[x]$. Sei S die Menge aller Nullstellen aller $f \in \mathcal{F}$ in F, $F = K[S]$. Sei $a \in F$, dann

$$\exists\, s_1, \ldots, s_n \in S,\ \exists\, g \in K[x_1, \ldots, x_n] : \quad a = g(s_1, \ldots, s_n)$$

$$\psi(a) = g(\psi(s_1), \ldots, \psi(s_n)) = g(t_1, \ldots, t_n)$$

mit $t_1, \ldots, t_n \in S$, also $\psi(a) \in K[S] = F$. Verwendet: ψ lässt Elemente von K punktweise fest, dh. ψ lässt Koeffizienten von jedem $f \in \mathcal{F} \subseteq K[x]$ fix, daher bildet ψ Nullstellen von $f \in \mathcal{F}$ wieder auf Nullstellen von f ab, $\psi(S) \subseteq S$, ψ injektiv $\Rightarrow$ ψ auf Nullstellen eines jeden $f \in \mathcal{F}$ bijektiv,

$$\forall\, t_1, \ldots, t_n \in S\ \exists\, s_1, \ldots, s_n \in S : \quad \psi(s_i) = t_i$$

Also $\forall\, a \in F : a = g(s_1, \ldots, s_n), g \in K[x_1, \ldots, x_n], s_i \in S$. $\exists t_1, \ldots, t_n \in S$ mit $\psi(t_i) = s_i$, also für $b = g(t_1, \ldots, t_n) : \psi(b) = a$. $\psi : F \to F$ surjektiv.

$3 \to 1$ f irreduzibel $\in K[x]$, $K \subseteq F \subseteq \overline{K}$. f hat Nullstelle $a \in F$. Seien $a = a_1, \ldots, a_n$ alle Nullstellen von f in $\overline{K}$, dann gibt es einen Isomorphismus $\psi : K[a] \to K[a_i]$ (für beliebige i) mit

$$\psi(a) = a_i, \quad \psi(k) = k \text{ für } k \in K$$

$\overline{K}$ ist algebraischer Abschluss von $K[a]$ und von $K[a_i]$, ψ lässt sich auf algebraischen Abschluss fortsetzen zu $\overline{\psi} : \overline{K} \to \overline{K}$ Isomorphismus mit $\overline{\psi}\big|_{K[a]} = \psi$, insbesondere mit $\psi(a) = a_i$, $\overline{\psi}\big|_F = \tilde{\psi} : F \to \overline{K}$ K-Monomorphismus. Nach Voraussetzung $\tilde{\psi}(F) = F$, also $a_i = \psi(a) = \tilde{\psi}(a) \in F$. Jede Nullstelle von f in $\overline{K}$ schon in F, also zerfällt f über F.

□

Korollar 2.31: F, K endliche Körper mit $K \subseteq F$, dann $F : K$ normal (weil F Zerfällungskörper von $x^{|F|} - x$ über K).

Definition 2.8: Eine algebraische Körpererweiterung $F : K$, die normal und separabel ist, heißt *Galois-Erweiterung.*

2.7 Einheitswurzel, Kreisteilungskörper

Definition 2.9: K Körper, $w \in K$ heißt *n-te Einheitswurzel*, wenn $w^n = 1$ und w heißt *primitive n-te Einheitswurzel*, wenn die Ordnung von w in $(K \setminus \{0\}, \cdot)$ gleich n ist, dh. $w^n = 1$, aber $w^k \neq 1$ für $0 < k < n$.

Anmerkung: n-te Einheitswurzeln gibt es immer, da 1 eine n-te Einheitswurzel für jedes n. Primitive n-te Einheitswurzeln gibt es nicht immer, zB in $\mathbb{Q}$ von $1, -1$ keine primitive dritte Einheitswurzel, aber im Zerfällungskörper von $x^n - 1$ über $\mathbb{Q}$ gibt es primitive n-te Einheitswurzel $e^{2\pi \mathrm{i}/n}$. Nicht über jedem Körper kann man durch Adjungieren von Nullstellen von $x^n - 1$ n verschiedene n-te Einheitswurzeln bekommen, zB K endlicher Körper mit $\chi(K) = p$, $|K| = p^m$, $|(K \setminus \{0\}, \cdot)| = p^m - 1$. Jedes Element in $(K \setminus \{0\}, \cdot)$ hat als Ordnung einen Teiler von $p^m - 1$, zB Ordnung p nicht möglich.

Beispiel (Übung)*:* K Körper, $n \in \mathbb{N} \Rightarrow$ die n-ten Einheitswurzeln in K bilden endliche zyklische Gruppe, da Ordnung ein Teiler von n ist.

Lemma 2.32: K Körper, $n \in \mathbb{N}$. Wenn $\chi(K) \nmid n$ ($\chi(K) = 0$ oder $\chi(K) = p \nmid n$), dann hat $x^n - 1$ in seinem Zerfällungskörper über K n verschiedene Nullstellen; wenn $\chi(K) = p \bigm| n$, $n = p^m k$, $p \nmid k$ da $x^n - 1 = (x^k - 1)^{p^m}$ und $x^n - 1$ hat in seinem Zerfällungskörper k verschiedene Nullstellen (die Nullstellen von $x^k - 1$), jeder zur Vielfachheit p^m.

Beweis. $\chi(K) \nmid n$, $(x^n - 1)' = nx^{n-1}$, $\mathrm{ggT}(x^n - 1, nx^{n-1}) = 1$, $x^n - 1$ hat im Zerfällungskörper keine mehrfachen Nullstellen $\to$ n verschiedene Nullstellen. $\chi(K) = p$, $n = p^m k$; Frobenius: $(x^{p^m k} - 1) = (x^k - 1)^{p^m}$, Punkt 1 anwenden auf $x^k - 1$. □

Definition 2.10: w primitive n-te Einheitswurzel (pnE), dann sei

$$\varphi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{ggT}(k,n)=1}} (x - w^k) = \prod_{u \text{ pnE}} (x - u)$$

das *n-te Kreisteilungspolynom* $\in K[x]$. Offenbar

$$\deg \varphi_n = \varphi(n) = \bigl|\{k \bigm| 1 \leq k \leq n, \mathrm{ggT}(k,n) = 1\}\bigr|$$

Satz 2.33:

1. Das n-te Kreisteilungspolynom φ_n wie oben (w primitive n-te Einheitswurzel in K) ist in $R[x]$, R Primring von K (der von 1_K erzeugte Ring).

2. $\varphi_n \in \mathbb{F}_q[x] \supseteq \mathbb{Z}_p[x]$ zerfällt in ${\varphi(n)}/{d}$ Stück irreduzible Faktoren vom Grad d, $d \in \mathbb{N}$ minimal, sodass $n \mid q^d - 1$.

Beweis.

Ad 1. Induktion nach n: $\varphi_1 = x - 1$ ✓

$$x^n - 1 = \prod_{d \mid n} \varphi_d(x) = \varphi_n(x) \cdot \prod_{\substack{d \mid n \\ d<n}} \varphi_d(x)$$

Nach IV gilt

$$g(x) = \prod_{\substack{d \mid n \\ d<n}} \varphi_d(x) \quad \in R[x]$$

Wegen Eindeutigkeit von Quotient und Rest bei Polynomdivision: $\varphi_n(x) \in R[x]$ ($\chi(K) = p$, $R = \mathbb{Z}_p$, Polynomdivision in $\mathbb{Z}_p[x]$, $\chi(K) = 0$, $R = \mathbb{Z}$, Division durch normierte Polynome aus $\mathbb{Z}[x]$ und $g(x)$ normiert). $x^n - 1$, $g(x)$ normiert in $R[x]$. Division mit Rest in $R[x]$: $x^n - 1 = q(x)g(x) + r(x)$, $\deg r < \deg g$, in $K[x]$ folgt wegen Eindeutigkeit $g = \varphi_n$, $r = 0$.

Ad 2. primitive n-te Einheitswurzel in Körper F, der $\mathbb{F}_q$ enthält $\Rightarrow$ $F = \mathbb{F}_{q^d}$ und $n \mid q^d - 1$. Für minimales d mit $n \mid q^d - 1$: kleinste Körpererweiterung von $\mathbb{F}_q$, der eine primitive n-te Einheitswurzel enthält, dh. wenn man eine Nullstelle w eines irreduziblen Faktors von $\varphi_n \in \mathbb{F}_q[x]$ adjungiert, dann $[\mathbb{F}_q[x] : \mathbb{F}_q] = d$ (d minimal, sodass $n \mid q^d - 1$), daher ist auch der Grad dieses irreduziblen Faktors d.

□

Definition 2.11: K Körper, der Zerfällungskörper von $x^n - 1$ über K heißt *n-ter Kreisteilungskörper* über K.

Wenn Gruppe der n-ten Einheitswurzeln in einem Körper zyklisch, ist die Existenz von n verschiedenen n-ten Einheitswurzeln äquivalent zur Existenz einer primitiven n-ten Einheitswurzel.

n-ter Kreisteilungskörper über K ist definiert als Zerfällungskörper von $x^n - 1$ über K; wenn $\chi(K) \nmid n$, dann im n-ten Kreisteilungskörper über K n verschiedene Einheitswurzeln (davon $\varphi(n)$ primitiv); wenn $p = \chi(K) \mid n$, dann $n = p^k m$ mit $p \nmid m$, $x^n - 1 = (x^m - 1)^{p^k}$ und im n-ten Kreisteilungskörper über K nur m verschiedene n-te Einheitswurzeln, nämlich nur die m-ten Einheitswurzeln (n-te Kreisteilungskörper ist gleich m-ter Kreisteilungskörper für $n = mp^k$, $p = \chi(K) \nmid m$).
Wenn $\chi(K) = p \nmid n$, dann sei F der n-te Kreisteilungskörper über K und $\varphi_n = \prod_w (x - w)$ (w primitive n-te Einheitswurzeln in F) (n-tes Kreisteilungspolynom), $\deg \varphi_n = \varphi(n)$.

Induktives Verfahren, die Kreisteilungspolynome zu konstruieren, aus dem hervorgeht, dass die Koeffizienten der φ_n im Primring ($\mathbb{Z}_p$ bzw $\mathbb{Z}$) liegen:

$$x^n - 1 = \prod_{d \mid n, d<n} \varphi_d(x) = \varphi_n(x), \quad \varphi_1(x) = x - 1$$

Nach Induktionsvoraussetzung hat

$$g(x) = \prod_{d \mid n, d<n} \varphi_d$$

Koeffizienten im Primring, $x^n - 1$, φ_n, $g(x)$ normiert. Allgemein $R \subseteq S$ kommutative Ringe mit 1, $f, g, h \in S[x]$, h normiert, $f, h \in R[x]$, $f(x) = g(x)$. $h(x) \Rightarrow g \in R[x]$ und wenn φ_d für $d < n$ schon konstruiert,

$$\varphi_n = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d<n}} \varphi_d(x)}$$

(in $\mathbb{Q}$ sind die Kreisteilungspolynome irreduzibel). $\mathbb{Z}_p \subseteq \mathbb{F}_q$ Kreisteilungspolynom $\in \mathbb{Z}_p[x] \subseteq \mathbb{F}_q[x]$. Über $\mathbb{F}_q$ zerfällt $\varphi_n, p \nmid n$ in irreduzible Faktoren vom Grad (= Grad der Körpererweiterung, wenn man eine primitive n-te Einheitswurzel adjungiert) m mit m minimal, sodass $n \mid q^m - 1$.

2.8 Konkrete Darstellung von endlichen Körpern

2.8.1 Polynom-Darstellung

f beliebig irreduzibel $\in \mathbb{Z}_p[x]$ mit $\deg f = m$, dann ist

$$\mathbb{Z}_p[x]/(f) \simeq \mathbb{F}_{p^m}$$

(genauso $\mathbb{F}_q$ endlicher Körper, $f \in \mathbb{F}_q[x]$ irreduzibel, $\deg f = m$, dann gilt $\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^m}$)
Rechnet in $\mathbb{Z}_p[x]/(f) = \mathbb{F}_{p^m}$ so: Restklassen $\bmod p$ addieren und multiplizieren; Repräsentantensystem bestehend aus allen $g \in \mathbb{Z}_p[x]$ mit $\deg g < m$, f irreduzibel $\in \mathbb{F}_q[x]$ mit $\deg f = m$ heißt *primitiv*, wenn eine Nullstelle α von f in $\mathbb{F}_q[\alpha]$ die multiplikative Gruppe erzeugt (wenn das für eine Nullstelle gilt, dann für alle wegen Isomorphismus $\mathbb{F}_q[\alpha] \simeq \mathbb{F}_q[\beta]$, $\alpha \mapsto \beta$ für Nullstellen α, β desselben irreduziblen Polynoms $\in \mathbb{F}_q[x]$.
Wenn f primitiv $\in \mathbb{F}_q[x]$, dann $x + f$ Erzeuger von

$$\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^m}$$

mit $m = \deg f$.
Potenzen von $x+f = \zeta$ auflisten $\zeta, \ldots, \zeta^{m-1}$, für $\zeta^m, \ldots, \zeta^{q^m-1}$ Rest $\bmod f$ bilden, "Index-Tabelle", dann hat man Darstellung der Elemente des endlichen Körpers, die sowohl für Addition (Polynome vom Grad $< m$) als auch für Multiplikation (Potenzen von ζ, Exponent $\bmod q^m - 1$) praktisch sind. Da $\mathbb{F}_{q^m}$ der $(q^m - 1)$-te Kreisteilungskörper (Zerfällungskörper von $x^{q^m-1} - 1$) über $\mathbb{F}_q$ ist, ist jeder irreduzible Faktor von φ_{q^m-1} ein primitives Polynom.

2.8.2 Matrix-Darstellung

Allgemein K Körper, $\subseteq A$ Algebra (Ring mit $1_A = 1_K \Rightarrow K$-Vektorraum), $a \in A$ beliebiges Element (algebraisch über K), $K[a] \simeq K[x]/(f)$, f Minimalpolynom von a, dh. normierter Erzeuger des Ideals

$$\{g \in K[x] \mid g(a) = 0\} \trianglelefteq K$$

(iA Minimalpolynom nicht irreduzibel). f normiert $\in K[x]$, dann ${}^{K[x]}/_{(f)} = K[a]$ weiters isomorph zu dem von der *Gefährtenmatrix* C_f von f erzeugten Unterring von $M_n(K)$ ($n = \deg f$), wobei

$$C_f = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ \vdots & & & & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-1} \end{pmatrix}$$

Dieser Unterring ist auch isomorph zu ${}^{K[x]}/_{(f)}$, da f das Minimalpolynom von C_f ist. Offenbar ist das charakteristische Polynom von C_f gleich f, aber auch das Minimalpolynom (Erzeuger des Ideals $\{g \in K[x] \mid g(C_f) = 0\}$). Allgemein:

Satz 2.34 (Satz von McCoy)**:** *R kommutativer Ring, $C \in M_n(R)$, dann ist das Ideal*

$$\{f \in R[x] \mid f(C) = 0\}$$

genau

$$(F_0(xI - C) : F_1(xI - C)) = \big\{ f \in R[x] \bigm| \forall g \in F_1(xI - C) : f \cdot g \in F_0(xI - c) \big\}$$

wobei für $k = 0, \dots, n-1$ $F_k(M)$ (M Matrix mit Eintragungen in S, hier $= R[x]$), das von den $(n-k) \times (n-k)$ Minoren erzeugte Ideal von M ist.

$M \in M_n(S)$ (S kommutativer Ring). $(n-k) \times (n-k)$ *Minor* von M ist eine Determinante einer $(n-k) \times (n-k)$-Untermatrix von M (einer Matrix, die aus M durch Streichung von k Zeilen und k Spalten hervorgeht). Insbesondere $F_0 = (\det M) \cdot S$ das von $\det M$ erzeugte Hauptideal von S, F_{n-1} das von den Eintragungen von M erzeugte Ideal von S.

Anmerkung: Elementare Zeilen- und Spaltenoperationen (Addition des s-fachen ($s \in S$) einer Zeile i zur Zeile j ($j \neq i$) analog für Spalten) ändern nichts an $F_0, F_1, \dots, F_{n-1}$.

Anmerkung:

$$C_f = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ \vdots & & & & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-1} \end{pmatrix}, \quad xI - C_f = \begin{pmatrix} x & -1 & 0 & \dots & 0 \\ 0 & x & -1 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & x & -1 \\ a_0 & a_1 & \dots & \dots & x + a_{n-1} \end{pmatrix}$$

2.9 Satz von McCoy

Anmerkung (Zutaten)*:*

1. Ring-Isomorphismus $M_n(R[x]) \simeq (M_n(R))[x]$ (R kommutativer Ring) via

$$\left(\sum_{k \geq 0}' a_{ij}^{(k)} x^k \right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \mapsto \sum_{k \geq 0}' (a_{ij}^{(k)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} x^k$$

Elemente in $R[x]$ sind jeweils eingebettet: $g = \sum a_k x^k \in R[x]$ in $M_n(R[x])$ als "Skalarmatrix",

$$g(x) \cdot I = \begin{pmatrix} g(x) & 0 & \dots & 0 \\ 0 & g(x) & \dots & 0 \\ \vdots & & \ddots & \\ 0 & \dots & & g(x) \end{pmatrix}$$

in $(M_n(R))[x]$

$$g(x) = a_0 I + a_1 I x + \ldots + a_m I x^m = \begin{pmatrix} a_0 & & \\ & \ddots & \\ & & a_0 \end{pmatrix} + \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_1 \end{pmatrix} x + \ldots + \begin{pmatrix} a_m & & \\ & \ddots & \\ & & a_m \end{pmatrix} x^m$$

Anmerkung: S kommutativer Ring, dann Zentrum (Menge der Elemente, die mit allen Elementen kommutieren) von $M_n(S)$ ist in S eingebettet als Menge der Skalarmatrizen $\{sI \mid s \in S\}$.

2. Linearfaktoren - Nullstellen eines Polynoms: der Zusammenhang gilt auch für nichtkommutativen Koeffizientenring (eventuell mit Nullteilern). S Ring mit 1, $g = \sum a_k x^k \in S[x]$, $s \in S$, dann

   $$\sum_{k \geq 0} a_k s^k = 0 \Leftrightarrow \exists\, h \in S[x] : g(x) = h(x)(x - s)$$

   (mit s rechts eingesetzt $\Rightarrow$ rechter Linearfaktor)

   $$\sum_{k \geq 0} s^k a_k = 0 \Leftrightarrow \exists\, \ell \in S[x] : g(x) = (x - s)\ell(x)$$

   (mit s links eingesetzt $\Rightarrow$ linker Linearfaktor)

3. Adjungierte einer Matrix: R kommutativer Ring, $A \in M_n(R)$, dann $\exists\, B \in M_n(R)$, $B = \operatorname{adj} A$, sodass

   $$A \cdot B = B \cdot A = (\det A) I = \begin{pmatrix} \det A & & \\ & \ddots & \\ & & \det A \end{pmatrix}$$

   Nämlich:

   $$B = \left((-1)^{i+j} \det A^i_j\right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

   wobei A^i_j die aus A durch Streichen der i-ten Spalte und j-ten Zeile hervorgehende Matrix bezeichnet.
   Anmerkung: Die Eintragungen der Adjungierten sind bis auf Vorzeichen die $(n-1) \times (n-1)$ Minoren von A

Definition 2.12: $A \in M_n(R)$. Eine $k \times k$-*Minor* von A ist die Determinante einer $k \times k$-Untermatrix von A (einer Matrix, die durch Streichen von $n - k$ Zeilen und $n - k$ Spalten aus A hervorgeht).

Spezialfall des Satzes von McCoy:
Satz 2.35 (Cayley-Hamilton)**:** $A \in M_n(R), \chi(x) = \det(xI - A)$, dann $\chi(A) = 0$.

Beweis. $B = \operatorname{adj}(xI - A)$:

$$B(xI - A) = \chi(x)I \text{ in } M_n(R[x])$$
$$B(x - A) = \chi(x) \text{ in } (M_n(R))[x]$$

$\Rightarrow\ \chi(A) = 0$ □

Anmerkung (Zusätzliche Notation)*:*

1. "Fitting-Invarianten": S kommutativer Ring: $A \in M_n(S)$, $F_k(A)$ das von den $k \times k$-Minoren von A erzeugte Ideal von S, $F_1(A) \supseteq F_2(A) \supseteq \ldots \supseteq F_{n-1}(A) \supseteq F_n(A)$. F_1 ist das von den Eintragungen von A erzeugte Ideal von S, F_n das von $\det A$ erzeugte Hauptideal von S, $F_n(A) = (\det A)S$
   Anmerkung: Die Eintragungen der Adjungierten von A erzeugen $F_{n-1}(A)$

2. "Idealquotient":

   $$(I :_K J) = \{k \in K \mid \forall\, j \in J : kj \in I\}$$

   wann immer das Sinn hat (insbesondere wenn K Ring, I, J K-Moduln, enthalten in K-Modul $L \supseteq I, J$.

Definition 2.13: R kommutativer Ring mit 1, $(M, +)$ kommutative Gruppe. $(M, +)$ ist R-*Modul*, wenn Skalarmultiplikation $\cdot : R \times M \to M$ definiert ist, sodass

1. $r(m + n) = rm + rn$ für alle $r \in R, m, n \in M$
2. $(rs)m = r(sm)$ für alle $r, s \in R, m \in M$
3. $(r + s)m = rm + sm$ für alle $r, s \in R, m \in M$

Zusätzlich für *unitären* Modul:

4. $1_R m = m$ für alle $m \in M$

Anmerkung: Jeder R-Modul M ist direkte Summe $M = M_0 \oplus M_1$, M_1 unitär, M_0 hat 0-Multiplikation, dh. $\forall\, r \in R\, \forall\, m \in M_0 : rm = 0$

Anmerkung: Wenn M ein R-Modul, dann

$$\operatorname*{Ann}_R M := \{r \in R \mid \forall m \in M : rm = 0\}$$

Ideal $\trianglelefteq R$. M heißt *treuer* (faithful) R-Modul, wenn

$$\operatorname*{Ann}_R M = \{0_R\}$$

Definition 2.14: R kommutativer Ring mit 1, $(M, +, \cdot)$ Ring mit 1 (eventuell nicht kommutativ), dann heißt M eine *R-Algebra*, wenn M ein R-Modul ist und sich Multiplikation im Ring M und Skalarmultiplikation $\cdot : R \times M \to M$ vertragen wie folgt: $r(mn) = (rm)n = m(rn)$ für alle $m, n \in M, r \in R$.

Anmerkung: $R \subseteq S$, R kommutativer Ring, S Ring $\Rightarrow$ S ist treue R-Algebra (durch Einschränkung der Multiplikation $S \times S \to S$ auf $R \times S \to S$). Jede treue R-Algebra von dieser Form: M treue R-Algebra, dann R isomorph eingebettet in M durch $r \mapsto r1_M$ und Skalarmultiplikation mit $r \in R$ ist dasselbe wie Multiplikation in M mit $r1_M$.

Satz 2.36 (Satz von McCoy)**:** R kommutativer Ring mit 1, $A \in M_n(R)$. Sei

$$N_A := \{f \in R[x] \mid f(A) = 0\}$$

und $C = xI - A$. Dann

$$N_A = (F_n(C) :_{R[x]} F_{n-1}(C))$$

Beweis. Angenommen $g \in R[x]$ ist in $(F_1 : F_{n-1})$. Das ist äquivalent zu: für ein Erzeugendensystem E des Ideals $F_{n-1}(C)$:

$$\forall\, e \in E : g \cdot e \in \chi(x) \cdot R[x]$$

insbesondere äquivalent zu: für $B = \mathrm{adj}(C)$ gilt:

$$\exists D \in M_n(R[x]) : g(x) \cdot B = \chi(x) \cdot D$$

Multiplikation mit $C = xI - A$ (kein Nullteiler in $M_n(R[x])$, also kürzbar) ergibt äquivalente Aussage:

$$g(x) \cdot \chi(x) = \chi(x) \cdot D \cdot (xI - A)$$

bzw.

$$\chi(x) \cdot g(x) = \chi(x) \cdot D \cdot (xI - A)$$

($\chi(x)$ im Zentrum von $M_n(R[x])$). Kürzen von $\chi(x)$ (kein Nullteiler da normiert, also kürzbar) ergibt äquivalente Aussage

$$g(x) = D \cdot (xI - A) \quad \text{für } D \in M_n(R[x])$$

in $(M_n(R))[x]$:

$$g(x) = D \cdot (x - A) \quad \text{für } D \in (M_n(R))[x]$$

äquivalent zu $g(A) = 0$. □

Anmerkung: Haben verwendet: im Polynomring $S[x]$ (S Ring mit 1) sind normierte Polynome (Leitkoeffizient ist 1), kürzbar, da sicher keine Nullteiler (Nullteiler im Polynomring haben als Leitkoeffizienten Nullteiler in S)

Korollar 2.37: R kommutativer Ring mit 1, $f \in R[x]$, f normiert, A die Gefährtenmatrix von f, dh.

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ 0 & & & 0 & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-1} \end{pmatrix}$$

dann ist

$$N_A = f(x)R[x]$$

(dh. $\forall\, g \in R[x] : g(A) = 0 \;\Leftrightarrow\; f \bigm| g$ in $R[x]$)

$$C = xI - A = \begin{pmatrix} x & -1 & 0 & \dots & 0 \\ 0 & x & -1 & \dots & 0 \\ \vdots & & & \ddots & \\ 0 & \dots & 0 & x & -1 \\ a_0 & a_1 & \dots & \dots & x + a_{n-1} \end{pmatrix}$$

$F_{n-1}(C) = R[x]$, da ± 1 als $(n-1) \times (n-1)$-Minor auftritt (bei Streichung von letzter Zeile und erster Spalte),

$$N_A = (\chi(x) \cdot R[x] : R[x]) = \chi(x) \cdot R[x]$$

und $\chi(x) = f(x)$ ($\det(x - A)$, A Gefährtenmatrix von f, ist f). Damit bekommt man eine Matrixdarstellung einer einfachen algebraischen Erweiterung von R (R kommutativer Ring mit 1), nämlich: $R \subseteq S$ (S Ring), $s \in S$ fix und algebraisch über R. $R[s]$, der von $R \cup \{s\}$ erzeugte Unterring von S, besteht genau aus den Ausdrücken $a_0 + a_1 s + \ldots + a_m s^m$ für $m \in \mathbb{N}, a_i \in R$. Daher Einsetzhomomorphismus $\varphi : R[x] \to S$ mit $\varphi(x) = s$, $\varphi\big|_R = \mathrm{id}_R$ surjektiv auf $R[s]$, $\ker\varphi = \{f \in R[x] : f(s) = 0\} \neq (0)$, daher nach dem ersten Isomorphiesatz: $R[x]/\ker\varphi \simeq R[s]$, wobei $\ker\varphi$ Hauptideal $= f(x) \cdot R[x]$, mit $f \neq 0$, erhalten Isomorphismus zu dem von R und A_f (der Gefährtenmatrix von f) erzeugten Unterring $M_n(R)$ ($n = \deg f$).

$$R[s] \simeq R[x]/(f) \simeq R[A_f]$$

$$\begin{aligned} s &\longleftarrow\!\shortmid (x + f) \longmapsto A_f \\ r &\longleftarrow\!\shortmid (r + f) \longmapsto rI \end{aligned}$$

In jedem Fall Einsetzhomomorphismus mit $x \mapsto s$ bzw $x \mapsto A_f$ und Einschränkung auf R gleich id_R ein Epimorphismus φ mit $\ker\varphi = (f)$, das zugehörige $\overline{\varphi}$ (erster Isomorphiesatz) ergibt Isomorphismus.

Beispiel: $\mathbb{C} = \mathbb{R}[i]$ als Ring von 2×2-Matrizen über $\mathbb{R}$. Minimalpolynom von i in $\mathbb{R}[x]$ ist $f = x^2+1$;

$$A_f = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Jeder Matrix in $\mathbb{R}[A_f]$ lässt sich, da $A_f^2 = -1$, darstellen als Polynom vom Grad ≤ 1 in $\mathbb{R}[x]$ mit A_f eingesetzt:

$$a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \leftrightarrow a + b\mathrm{i}$$

Isomorphismus

Anmerkung: $a \in S$ Ring, R kommutativer Ring $\subseteq S$. Wenn a Nullstelle eines normierten $f \in R[x]$ ($\deg f = n$), dann besteht der von a über R erzeugte Unterring von S (a priori $R[a]$) aus R-Linearkombinationen von $1, a, a^2, \ldots, a^{n-1}$; und wenn $f \in R[x]$ von minimalem Grad mit $f(a) = 0$, dann ist diese Darstellung eindeutig.

$$f = x^n + b_{n-1}x^{n-1} + \ldots + b_0$$

dann

$$a^n = -b_{n-1}a^{n-1} \ldots - b_0$$

a^n und induktiv alle höheren Potenzen von a als R-Linearkombination von $1, a, \ldots, a^{n-1}$ darstellbar. Wenn zwei Darstellungen, dann gibt Subtraktion Polynom vom Grad $\leq n-1$ mit a als Nullstelle.

2.10 Berlekamp-Algorithmus zur Faktorisierung von Polynomen über endlichen Körpern

Wollen $f \in \mathbb{F}_q[x]$ in irreduzible Polynome faktorisieren.
Lemma 2.38: $f \in \mathbb{F}_q[x]$ gegeben. Wenn $g \in \mathbb{F}_q[x]$, sodass $f \mid g^q - g$, dann

$$f = \prod_{c\in\mathbb{F}_q} \mathrm{ggT}(f, g - c)$$

Wenn zusätzlich $0 < \deg g < \deg f$, dann ist diese Faktorisierung von f nichttrivial, dh. die Faktoren sind nicht lauter Einheiten und ein zu f assoziiertes Polynom.

Beweis. In $\mathbb{F}_q[x]$:

$$x^q - x = \prod_{c\in\mathbb{F}_q} (x - c)$$

also $\forall\, g \in \mathbb{F}_q[x]$

$$g^q - g = \prod_{c\in\mathbb{F}_q} (g - c)$$

Die $g-c$ für verschiedene c paarweise relativ prim. Wenn $f \mid g^q - g$, dann

$$f = \mathrm{ggT}(f, g^q - g) = \mathrm{ggT}\left(f, \prod_{c\in\mathbb{F}_q}(g-c)\right) \stackrel{!}{=} \prod_{c\in\mathbb{F}_q} \mathrm{ggT}(f, g-c)$$

weil die Faktoren $g-c$ paarweise relativ prim. Der Fall $f \mid g-c$ für ein c kann nur vorkommen, wenn $\deg g (= \deg g - c) \geq \deg f$ oder wenn $g - c = 0$ (dh. g konstant). □

Lemma 2.39: $f \in \mathbb{F}_q[x]$, $f = f_1^{k_1} \cdots f_s^{k_s}$, wobei $f_1, \ldots, f_s$ verschiedene irreduzible Polynome sind, dann ist die Anzahl der $g \in \mathbb{F}_q[x]$ mit $f \mid g^q - g$ und $\deg g < \deg f$ genau q^s.

Beweis. Wenn $f \mid g^q - g = \prod(g-c)$, dann $\forall f_i \, \exists! \, c \in \mathbb{F}_q$ mit $f_i^{k_i} \mid g - c$. Umgekehrt, wenn $\forall f_i \, \exists c$ mit $f_i^{k_i} \mid g - c$, dann $f \mid \prod(g-c) = g^q - g$ (die $f_i^{k_i}$ für verschiedene i relativ prim). Für jede Wahl von $(c_1, \ldots, c_s) \in \mathbb{F}_q^s : \exists! \, g \in \mathbb{F}_q[x]$ mit $f_i^{k_i} \mid g - c_i$ und $\deg g < \deg f$, weil nach Chinesischem Restsatz: $g \equiv c_i \mod f_i^{k_i}$ $(1 \leq i \leq s)$ lösbar, eindeutig lösbar mod $\prod_{i=1}^s f_i^{k_i} = f$. Also genau q^s solche g, für jede Wahl von $(c_1, \ldots, c_s)$ eines. □

Definition 2.15: Ein $g \in \mathbb{F}_q[x]$ mit $f \mid g^q - g$ und $0 < \deg g < \deg f$ heißt f*-reduzierend*

Unter den q^s Polynomen g mit $f \mid g^q - g$, $\deg g < \deg f$ alle q Konstanten $\in \mathbb{F}_q$ vorkommen, gibt es zu $f \in \mathbb{F}_q[x]$ genau $q^s - q$ f-reduzierende Polynome, wobei s die Anzahl der verschiedenen irreduziblen Faktoren von f ist.

Algorithmus 2.40 (Berlekamp-Algorithmus)**:** Zum Finden derjenigen g mit $\deg g < \deg f$ und $f \mid g^q - g$: Division mit Rest von x^{jq} für $j = 0, \ldots, n-1$ ($n = \deg f$) durch f:

$$\begin{aligned} x^{jq} &= f(x)h_j(x) + r_j(x) \\ r_j(x) &= b_{j0} + b_{j1}x + \ldots + b_{jn-1}x^{n-1} \end{aligned}$$

Matrix

$$\begin{aligned} B &= (b_{jk})_{\substack{0\leq j\leq n-1 \\ 0\leq k\leq n-1}} \\ g &= c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \end{aligned}$$

erfüllt $f \mid g^q - g$ genau dann, wenn $(c_0, c_1, \ldots, c_{n-1})$ Lösung von

$$(c_0, \ldots, c_{n-1})(B - I) = 0$$

ist.

Beweis.

$$g = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$$

erfülle $g \mid g^q - g$. Da

$$g^q = c_0 + c_1 x^q + c_2 x^{2q} + \ldots + c_{n-1}x^{(n-1)q}$$

ist $g^q - g \equiv 0 \mod f$ äquivalent zu

$$c_0 b_0(x) + c_1 b_1(x) + \ldots + c_{n-1} b_{n-1}(x) - (c_0 1 + c_1 x + \ldots + c_{n-1} x^{n-1}) \equiv 0 \mod f$$

Da Grad der vorkommenden Polynome $< \deg f$, ist in diesem Fall $\equiv 0 \mod f$ äquivalent zu $= 0$ in $\mathbb{F}_q[x]$, dh. äquivalent zu

$$c_0 b_{00} - c_0 + c_1 b_{10} + c_2 b_{20} + \ldots + c_{n-1} b_{n-10} = 0 \quad \text{(Koeffizienten von } x^0\text{)}$$

$$c_0 b_{0k} - c_1 b_{1k} + \ldots + c_k(b_{kk} - 1) + \ldots + c_{n-1} b_{n-1k} = 0 \quad \text{(Koeffizienten von } x^k\text{)}$$

dh. $(c_0, c_1, \ldots, c_{n-1})(B - I) = 0$. Beim Lösung des linearen Gleichungssystems findet man auch die Dimension dieses Lösungsraums: q^s, und erfährt dabei $s =$ Anzahl der verschiedenen irreduziblen Faktoren von f. Als Lösungen erhält man (wenn $s > 1$), nach Wegwerfen der Konstanten, $q^s - q$ f-reduzierende Polynome. □

Algorithmus 2.41: Berlekamp erlaubt uns, quadratfreie Polynome $f = f_1 \cdots f_s$ (f_i verschiedene irreduzible Polynome $\in \mathbb{F}_q[x]$) zu faktorisieren: Wenn $\deg f = n$, dann x^{qk}, $0 \leq k \leq \deg f$ mit Rest durch f dividieren,

$$x^{qk} = h_k(x) f(x) + r_k(x), \quad r_k(x) = \sum_{j=0}^{n-1} b_k j x^j$$

$B = (b_{kj})_{\substack{0 \leq k \leq n-1 \\ 0 \leq j \leq n-1}}$; Lineares Gleichungssystem

$$(c_0, \ldots, c_{n-1})(B - I) = 0$$

lösen: Dimension als $\mathbb{F}_q$-Vektorraum des Lösungsraums ist $s =$ Anzahl der verschiedenen irreduziblen Faktoren von f; $(c_0, c_1, \ldots, c_{n-1}) \neq (c_0, 0, \ldots, 0)$ (falls vorhanden, dh. falls $s > 1$) liefert f reduzierendes Polynom

$$g = \sum_{i=0}^{k} c_i x^i$$

$$f = \prod_{c \in \mathbb{F}_q} \mathrm{ggT}(f, g - c)$$

ist nichttriviale Faktorisierung, iterieren, falls f noch nicht komplett faktorisiert. Jetzt müssen wir Faktorisierung eines beliebigen $f \in \mathbb{F}_q[x]$ auf Faktorisierung von quadratfreien Polynomen zurückführen. Gegeben f, zuerst f' bilden. Wenn $f' = 0$ ($f = \sum a_k x^k, f' = \sum k a_k x^{k-1} = 0 \Rightarrow$ jedes k mit $a_k \neq 0$ ist Vielfaches von p (Charakteristik)), dann $f = \sum a_k x^{pk}$. f ist also p-te Potenz: sei $b_k \in \mathbb{F}_q$ mit $b_k^p = a_k$, dann

$$f = \sum a_k x^{pk} = \sum b_k^p x^{pk} = \left(\sum b_k x^k\right)^p$$

p-te Wurzel aus $f = \sum a_k x^{pk}$ ziehen erfordert Finden von $b \in \mathbb{F}_q$ mit $b^p = a$ für beliebiges $a \in \mathbb{F}^q$. Für $a = 0, b = 0$: ✓. Für $a \neq 0$: $\mathrm{ggT}(p, q-1) = 1$, finden $\alpha, \beta \in \mathbb{Z}$, so dass $\alpha p + \beta(q-1) =$

1. $b := a^\alpha$, dann $b^p = a^{\alpha p} = a^{\alpha p} \cdot 1 = a^{\alpha p} \cdot a^{(q-1)\beta} = a^1 = a$. Also, wenn $f' = 0$, dann p-te Wurzel aus f berechnen (iterieren, bis $f' \neq 0$). Gegeben f mit $f' \neq 0$; bilden $\mathrm{ggT}(f, f') = d$ und f/d quadratfrei. $g = f/d$ mit Berlekamp faktorisieren, irreduzible Faktoren von g aus f wegdividieren (zur höchstmöglichen Potenz). Man erhält eine p-te Potenz, iterieren. Wenn nämlich $f = h^p f_1^{k_1} \cdots f_s^{k_s}$, $1 \leq k_i < p$, dann

$$f' = h^p (f_1^{k_1} \cdots f_s^{k_s})'$$

$$\mathrm{ggT}(f, f') = h^p f_1^{k_1 - 1} \cdots f_s^{k_s - 1}$$

und

$$\frac{f}{\mathrm{ggT}(f, f')} = f_1 \cdots f_s$$

Anmerkung: Man kann (Berlekamp-Zassenhaus) einen Algorithmus zur Faktorisierung von Polynomen in $\mathbb{Z}_p[x]$ auch zum Faktorisieren von Polynomen in $\mathbb{Z}$ verwenden (zB in Mignotte / Stefanescu).

2.11 Irreduzible Polynome in $\mathbb{F}_q[x]$

Anmerkung (Zur Erinnerung)*:* $\forall f$ irreduzibel in $\mathbb{F}_q[x]$ ist der Zerfällungskörper über $\mathbb{F}_q$ derselbe, nämlich der eindeutig bestimmte Körper mit q^n Elementen (der Zerfällungskörper aller irreduziblen Polynome $\in \mathbb{F}_q$ vom Grad n enthält nur einen Körper mit Ordnung q^n). Außerdem reicht es, eine Nullstelle eines irreduziblen $f \in \mathbb{F}_q[x]$ zu adjungieren, dann $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^n}$, wo f und alle anderen irreduziblen Polynome von Grad n über $\mathbb{F}_q$ zerfallen.

Lemma 2.42: $x^{q^n} - x \in \mathbb{F}_q[x]$. Dann ist $x^{q^n} - x$ das Produkt aller normierten irreduziblen Polynome aus $\mathbb{F}_q[x]$, deren Grad n teilt.

Beweis. In $\mathbb{F}_{q^n}[x]$ zerfällt

$$x^{q^n} - x = \prod_{c \in \mathbb{F}_{q^n}} (x - c)$$

Keine mehrfachen Nullstellen, also in $\mathbb{F}_q[x]$ keine mehrfachen irreduziblen Faktoren. Jedes irreduzible $f \in \mathbb{F}_q[x]$ mit $\deg f = d \mid n$ hat Nullstelle in $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$, daher teilt f (Minimalpolynom $\in \mathbb{F}_q[x]$ eines der $c \in \mathbb{F}_{q^n}$) in $\mathbb{F}_q[x]$ das Polynom $x^{q^n} - x$. Keine anderen irreduziblen Faktoren als die Minimalpolynome der $c \in \mathbb{F}_{q^n}$ in $\mathbb{F}_q[x]$ können vorkommen, und die Elemente aus $\mathbb{F}_{q^n}$ haben Minimalpolynom, dessen Grad $[\mathbb{F}_q[c] : \mathbb{F}_q]$ n teilt, da $\mathbb{F}_q[c] \subseteq \mathbb{F}_{q^n} \Rightarrow \mathbb{F}_q[c]$ hat q^d Elemente für ein $d \mid n$, also $[\mathbb{F}_q[c] : \mathbb{F}_q] = d \mid n$. Anders ausgedrückt: $\prod_c (x - c)$ da in $\mathbb{F}_q[x]$, Produkt aller Minimalpolynome aller $c \in \mathbb{F}_{q^n}$ über $\mathbb{F}_q$ (je eins). Diese Minimalpolynome sind genau die irreduziblen normierten Polynome $\in \mathbb{F}_q[x]$ mit $\deg \mid n$. $\square$

Anmerkung (Notation)*:* $N_q(d)$ ist die Anzahl der verschiedenen normierten irreduziblen Polynome $\in \mathbb{F}_q[x]$ mit Grad d.

Anmerkung (Notation)*:* Sei $I(q, n)(x)$ das Produkt aller normierten irreduziblen Polynome $\in \mathbb{F}_q[x]$ mit Grad n. Dann

1.

$$x^{q^n} - x = \prod_{d|n} I(q, d)(x)$$

2.

$$q^n = \sum_{d|n} dN_q(d)$$

Daraus können wir mit Möbius-Inversion Formeln für $I(n, q)$ und $N_q(d)$ ableiten.

3 Zahlentheoretische Möbius-Funktion und Möbius-Inversion

Definition 3.1: Für $n \in \mathbb{N} = \{1, 2, \dots\} = \{n \in \mathbb{Z} \mid n > 0\}$ definiere

$$\mu(n) = \begin{cases} (-1)^s & n = p_1 \cdots p_s \text{ quadratfrei, } p_i \text{ prim} \\ 0 & \text{sonst } (n \text{ nicht quadratfrei}) \end{cases}$$

Anmerkung: n heißt quadratfrei, wenn $\nexists p$ prim: $p^2 \mid n$ (n ist Produkt von s verschiedenen Primzahlen, $n = p_1 \cdots p_s$, 1 gilt als Produkt von 0 Primzahlen).

Lemma 3.1:

$$\sum_{d \mid n} \mu(d) = \begin{cases} 0 & n \neq 1 \\ 1 & n = 1 \end{cases}$$

($d \mid n$ im Summationsindex heißt Summieren über alle $d \in \mathbb{N}$ mit $1 \leq d \leq n$ und $d \mid n$)

Beweis.

- $n = 1$ ✓
- $n \neq 1$:

$$\sum_{d \mid n} \mu(d) = \sum_{\substack{d \mid n \\ d \text{ quadratfrei}}} \mu(d) = \sum_{k=0}^{n} \binom{s}{k} (-1)^s = (1-1)^s = 0$$

wobei $n = p_1 \cdots p_s$ und es $\binom{s}{k}$ quadratfreie Teiler $d = p_{i_1} \cdots p_{i_k}$ mit k verschiedenen Primfaktoren gibt, die jeweils $\mu(d) = (-1)^k$ beitragen.

□

Satz 3.2 (Möbius-Inversion)**:** Seien f, g Funktionen $\mathbb{N} \to (G, +)$ (G kommutative Gruppe), sodass

$$g(n) = \sum_{d \mid n} f(d)$$

dann

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{\substack{(c,d) \\ cd = n \\ 1 \leq c, d \leq n}} \mu(c) g(d)$$

Dasselbe multiplikativ geschrieben: Wenn $f, g : \mathbb{N} \to (G, \cdot)$, sodass

$$g(n) = \prod_{d \mid n} f(d)$$

dann

$$f(n) = \prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{\substack{(c,d)\\ cd=n\\ 1\le c,d\le n}} g(d)^{\mu(c)}$$

und es gilt jeweils auch die Umkehrung.

Beweis. Zeigen

$$g(n) = \sum_{d|n} f(d) \;\Rightarrow\; f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) \qquad \text{[Umkehrung: Übung]}$$

$$\begin{aligned}
\sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) &= \sum_{d|n}\Big(\sum_{c\left|\frac{n}{d}\right.} f(c)\Big)\mu(d)\\
&= \sum_{\substack{(c,d)\\ cd|n}} f(c)\mu(d)\\
&= \sum_{c|n} f(c) \underbrace{\sum_{d\left|\frac{n}{c}\right.} \mu\left(\frac{n}{c}\right)}_{=0 \text{ außer } n=c} = f(n)
\end{aligned}$$

□

Korollar 3.3:

$$I(q,n)(x) = \prod_{d|n}\left(x^{q^d} - x\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{\substack{(c,d)\\ cd=n\\ 1\le c,d\le n}} \left(x^{q^d} - x\right)^{\mu(c)}$$

und

$$N_q(n) = \frac{1}{n}\sum_{d|n} q^d \mu\left(\frac{n}{d}\right) = \frac{1}{n}\sum_{\substack{(c,d)\\ cd=n}} q^d\mu(c)$$

Beweis. Möbius-Inversion angewendet auf

$$x^{q^n} - x = \prod_{d|n} I(q,d)(x)$$

und auf

$$q^n = \sum_{d|n} dN_q(d)$$

mit

$$g(n) = q^n, \quad f(n) = nN_q(n)$$

□

Proposition 3.4: Für $n > 1$:

$$I(q,n)(x) = \prod_{\substack{m \mid q^n-1 \\ m \nmid q^k-1 \text{ für } 1\le k<n}} \varphi_m(x)$$

Beweis. Im Zerfällungskörper von $x^{q^n} - x$, welcher der Zerfällungskörper von $x^{q^n-1} - 1$ ist

$$x^{q^n-1} - 1 = \prod_{\substack{c\in\mathbb{F}_{q^n} \\ c\neq 0}} (x-c)$$

Die Elemente $c \in \mathbb{F}_{q^n} \setminus \{0\}$ sind d-te Einheitswurzeln jeweils für ein $d \bigm| q^n - 1$ (d die Ordnung von c in $(\mathbb{F}_{q^n} \subseteq \{0\}, \cdot)$).

$$\prod_{\substack{c\in\mathbb{F}_{q^n} \\ c\ d\text{-te EW}}} (x-c) = \varphi_d(x)$$

Der kleinste Oberkörper von $\mathbb{F}_q$, der alle d-ten Einheitswurzeln enthält, ist $\mathbb{F}_{q^\ell}$ mit ℓ minimal, sodass $d \bigm| q^\ell - 1$, dh. Produkt über alle $x - c$ mit c d-te primitive Einheitswurzel in $\mathbb{F}_{q^n}$, die in keinem kleineren Erweiterungskörper von $\mathbb{F}_q$ enthalten ist, ist einerseits

$$\prod_{\substack{d\mid q^n-1 \\ d\nmid q^k-1, 1\le k\le n}} \varphi_d(x)$$

und andererseits Produkt aller irreduziblen Polynome, deren Grad n ist: jedes Element $\neq 0$ von $\mathbb{F}_{q^n}$ ist primitive d-te Einheitswurzel für ein $d \bigm| n$, und genau dann erzeugt c den Körper $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ ($\mathbb{F}_{q^n} = \mathbb{F}_q[c]$), wenn entweder das Minimalpolynom von c über $\mathbb{F}_q$ Grad n hat oder äquivalent, n der kleinste Exponent von q ist, sodass $\mathbb{F}_{q^n}$ eine primitive d-te Einheitswurzel hat, dh. $d \bigm| q^n - 1, d \nmid q^k - 1$, $1 \le k \le n$. $\square$

3.1 Möbius-Funktion eines endlichen Verbandes

Sei $(P, \le)$ endliche halbgeordnete Menge, $\zeta : P \times P \to \mathbb{Z}$ Funktion,

$$\zeta(x,y) = \begin{cases} 1 & x \le y \\ 0 & \text{sonst} \end{cases}$$

bezeichnen auch die Matrix indiziert mit Elementen von P mit Eintragungen $\zeta(x, y)$ als ζ.
Proposition 3.5: ζ invertierbar in $M_{|P|}(\mathbb{Z})$ und die Inverse μ hat die Eigenschaft $\mu(x, y) \neq 0$ nur für solche x, y mit $x \le y$.

Anmerkung: Man nennt die $\mathbb{Z}$-Algebra $\mathcal{A}(P)$ der Matrizen $M_{|P|}(\mathbb{Z})$ mit der Eigenschaft Eintragungen $\neq 0$ nur an Stellen (x, y) mit $x \le y$ in P die Inzidenzalgebra von P. Die Proposition heißt also: Die Inzidenzmatrix ζ von P ist in der Inzidenzalgebra von P invertierbar

Beweis. $\mu\zeta = I$ und $\mu \in \mathcal{A}(P)$ äquivalent zu

$$\sum_{\substack{z \\ x \leq z \leq y}} \mu(x,z) = \begin{cases} 1 & x = y \\ 0 & \text{sonst} \end{cases}$$

und $\mu \in \mathcal{A}(P)$. Das kann man erreichen, indem man (für fixes x) $\mu(x,y)$ induktiv definiert wie folgt:

$$\begin{aligned} &\mu(x,y) = 0 \quad \text{falls } x \not\leq y \\ &\mu(x,x) = 1 \\ &\mu(x,y) = -\sum_{\substack{z \\ x \leq z < y}} \mu(x,z) \end{aligned}$$

Induktiv nach Höhe über x vorgehen: wenn $z \geq x$, Höhe von z über x ist minimale Länge einer maximalen Kette $x = x_0 < x_1 < \ldots < x_n = z$.

Inverse $\mu \in \mathcal{A}(P)$ von ζ existiert, und erfüllt auch $\zeta\mu = I$ (befinden uns im Ring $M_n(\mathbb{Z})$), dh. es gilt auch

$$\sum_{x \leq z \leq y} \mu(z,y) = \begin{cases} 1 & x = y \\ 0 & \text{sonst} \end{cases}$$

$\square$

Proposition 3.6 (Möbius-Inversion)**:** f, g, h Funktionen $P \to (G,+)$ ($(G,+)$ Gruppe, $(P,\leq)$ endliche halbgeordnete Menge), sodass

$$g(x) = \sum_{\substack{a \in P \\ a \leq x}} f(a), \quad h(x) = \sum_{\substack{b \in P \\ b \geq x}} f(b)$$

dann

$$f(x) = \sum_{\substack{a \in P \\ a \leq x}} \mu(a,x) g(a), \quad f(x) = \sum_{\substack{b \in P \\ b \geq x}} \mu(x,b) h(b)$$

Beweis.

$$\begin{aligned} \sum_{\substack{a \in P \\ a \leq x}} \mu(a,x) g(a) &= \sum_{\substack{a \in P \\ a \leq x}} \sum_{\substack{b \in P \\ b \leq a}} \mu(a,x) f(b) \\ &= \sum_{b \in P} \underbrace{\left(\sum_{\substack{a \in P \\ b \leq a \leq x}} \mu(a,x) \right)}_{\delta_{x,b}} f(b) = f(x) \end{aligned}$$

bzw

$$g(x) = \sum_{\substack{a \in P \\ a \leq x}} f(a)$$

äquivalent zu

$$f \cdot \zeta = g \quad (f(a_1)f(a_2)\dots f(a_n)) \cdot \zeta = (g(a_1)g(a_2)\dots g(a_n))$$

für $P = \{a_1, \dots, a_n\}$, also wegen $\zeta\mu = I$ folgt $f = g\mu$. Analog für h. $\square$

Beispiel: $(P, \leq)$ sei $(\mathcal{P}(X), \subseteq)$, Potenzmenge einer endlichen Menge. Behauptung:

$$\mu(A, B) = \begin{cases} (-1)^{|B \setminus A|} & A \subseteq B \\ 0 & A \not\subseteq B \end{cases}$$

Es genügt zu überprüfen

1. $\mu(A, B) = 0$ für $A \not\subseteq B$ ✓
2. für fixes A, B mit $A \subseteq B$

$$\sum_{\substack{C \in \mathcal{P}(X) \\ A \subseteq C \subseteq B}} \mu(A, C) = \begin{cases} 1 & A = B \\ 0 & \text{sonst} \end{cases}$$

$$\begin{aligned} \sum_{\substack{C \in \mathcal{P}(X) \\ A \subseteq C \subseteq B}} \mu(A, C) &= \sum_{\substack{D \in \mathcal{P}(X) \\ D \subseteq B \setminus A}} \mu(A, A \dot{\cup} D) \\ &= \sum_{\substack{D \in \mathcal{P}(X) \\ D \subseteq B \setminus A}} (-1)^{|D|} \\ &= \sum_{k=0}^{|D|} \binom{|D|}{k} (-1)^k \\ &= \begin{cases} 0 & D \neq \emptyset \\ 1 & D = \emptyset \end{cases} \end{aligned}$$

Summe ist 0 für $A \subsetneqq B$, 1 für $A = B$.

Anmerkung:

$$\mu(A, B) = \begin{cases} 0 & A \not\subseteq B \\ \mu(\emptyset, B \setminus A) & A \subseteq B \end{cases}$$

Beispiel: Möbius-Inversion im Verband $(\mathcal{P}(X), \subseteq)$ ist Inklusion-Exklusion: Seien $A_1, \dots, A_n \subseteq X$ endlich; $I = \{1, \dots, n\}$. Für eine Teilmenge J der Indexmenge I sei

$$\begin{aligned}
f(J) &= \left|\{x \in X \mid x \in A_i\}\right| \\
&= \left|\{x \in X \mid \{i \in I \mid x \in A\} = J\}\right| \\
g(J) &= \left|\{x \in X \mid i \in J \Rightarrow x \in A_i\}\right| \\
&= \left|\bigcap_{i \in J} A_i\right| \\
&= \sum_{\substack{L \\ L \supseteq J}} f(L)
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \; f(J) &= \sum_{\substack{L \\ L \supseteq J}} \mu(J, L) g(L) \\
&= \sum_{\substack{L \\ L \supseteq J}} (-1)^{|L \setminus J|} \left|\bigcap_{i \in L} A_i\right| \\
&= \sum_{C \subseteq I \setminus J} (-1)^{|C|} \left|\bigcap_{i \in J \dot\cup C} A_i\right|
\end{aligned}$$

für $J \neq \emptyset$.

$$f(J) = \left|X \setminus \bigcup_{i \in I} A_i\right| = \sum_{k=0}^{|I|} (-1)^k \sum_{\{i_1, \dots, i_k\}_{\neq}} |A_{i_1} \cap \ldots \cap A_{i_k}|$$

Beispiel: Zahlentheoretische Möbius-Funktion: Verband der Teiler von n mit $a \leq b :\Leftrightarrow a \mid b$,

$$\mu(a, b) = \begin{cases} 0 & a \nmid b \\ 0 & b = ac, c \text{ nicht quadratfrei} \\ (-1)^s & b = ac, c = p_1 \cdots p_s, p_i \text{ verschiedene Primzahlen} \end{cases}$$

zeigt man durch Überprüfen von $\mu(a, b) = 0$ für $a \nmid b$ und

$$\sum_{a \leq d \leq b} \mu(a, d) = \begin{cases} 0 & a \neq b \\ 1 & a = b \end{cases}$$

$\mu(a, b)$ für $a \mid b$ hängt nur von b/a ab, eigentliche zahlentheoretische Möbius-Funktion in einer Variablen ist $\mu(a) = \mu(1, a)$ bzw. umgekehrt:

$$\mu(a, b) = \begin{cases} \mu\left(\frac{b}{a}\right) & a \mid b \\ 0 & a \nmid b \end{cases}$$

Beispiel: Verband der $\mathbb{F}_q$-Unterräume eines n-dimensionalen $\mathbb{F}_q$-Unterraums V bezüglich $\subseteq$ $(U, W \leq V)$:

$$\mu(U,W) = \begin{cases} 0 & U \not\subseteq W \\ (-1)^k q^{\binom{k}{2}} & U \subseteq W (k = \dim {}^{W}/{}_{U} = \dim W - \dim U) \end{cases} = \begin{cases} 0 & U \not\subseteq W \\ \mu\left(0, {}^{W}/{}_{U}\right) & U \subseteq W \end{cases}$$

Satz 3.7 (Satz von Weiser für Möbius-Funktion eines endlichen Verbandes)**:** (Verband: halbgeordnete Menge $(V, \leq)$, sodass $\forall\, a, b \in V : \exists \sup(a,b) = a \vee b$, $\exists \inf(a,b) = a \wedge b$) Nennen das Minimum des Verbandes 0 und das Maximum 1. Dann gilt für beliebiges $a \in V$ mit $a \neq 0$:

$$\sum_{\substack{x \\ x \vee a = 1}} \mu(0,x) = 0$$

Beweis.

$$\begin{aligned} S &= \sum_x \sum_{\substack{y \\ y \geq x \\ y \geq a}} \mu(0,x)\mu(y,1) \\ &= \sum_x \mu(0,x) \underbrace{\sum_{\substack{y \\ 1 \geq y \geq x \vee a}} \mu(y,1)}_{1 \text{ für } x \vee a = 1, 0 \text{ sonst}} \\ &= \sum_{\substack{x \\ x \vee a = 1}} \mu(0,x) \end{aligned}$$

andererseits

$$S = \sum_{y \geq a} \mu(y,1) \underbrace{\sum_{\substack{x \\ 0 \leq x \leq y}} \mu(0,x)}_{=0} = 0$$

da $y \geq a > 0$. □

Beweis. Beweis der Formel für Möbius-Funktion des Verbandes der $\mathbb{F}_q$-Unterräume von V (n-dimensionaler $\mathbb{F}_q$-Unterraum). Es genügt zu zeigen

$$\mu(0,V) = (-1)^n q^{\binom{n}{2}}$$

Induktion nach n:

- $n = 0$ ✓
- $n > 0$: P beliebiger 1-dimensionaler Teilraum von V: Weiser

$$\sum_{\substack{U \\ P \vee U = V}} \mu(0,U) = 0$$

bzw.

$$\mu(0,V) = -\sum_{\substack{U \\ P\vee U=V}} (-1)^{n-1} q^{\binom{n-1}{2}}$$

(nach IV gilt

$$\mu(0,U) = (-1)^k q^{\binom{k}{2}}$$

für $\dim U = k < n$). Anzahl der U mit $\dim U = n-1$, $U \vee P = V$ ist:

$$\begin{aligned}
\begin{bmatrix} n \\ n-1 \end{bmatrix}_q &= \frac{(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-2})}{q^{n-1}-q)(q^{n-1}-q^2)\cdots(q^{n-1}-q^{n-2})} \\
&= \begin{bmatrix} n \\ n-1 \end{bmatrix}_q - \begin{bmatrix} n \\ n-1 \end{bmatrix}_q \cdot \frac{(q^{n-1}-1)}{(q^n-1)} \\
&= \frac{q^n-1}{q-1} \cdot \left(1 - \frac{q^{n-1}-1}{q^n-1}\right) \\
&= \frac{q^n-q^{n-1}}{q-1} = q^{n-1}
\end{aligned}$$

$$\begin{aligned}
\Rightarrow\ \mu(0,V) &= (-1)^n q^{n-1+\binom{n-1}{2}} \\
&= (-1)^n q^{\binom{n}{2}}
\end{aligned}$$

□

Abzählen der surjektiven $\mathbb{F}_q$-Homomorphismen $\varphi : V \to W$ analog zum Abzählen der surjektiven Abbildungen zwischen endlichen Mengen (Möbius-Inversion).

Sei V n-dimensionaler, W m-dimensionaler $\mathbb{F}_q$-Vektorraum, U Teilraum $\leq W$. Dann sei

$$\begin{aligned}
g(U) &= \#\{\varphi \in \operatorname{Hom}_{\mathbb{F}_q}(V,W) \mid \operatorname{Im}\varphi \subseteq U\} \\
f(U) &= \#\{\varphi \in \operatorname{Hom}_{\mathbb{F}_q}(V,W) \mid \operatorname{Im}\varphi = U\} \\
g(U) &= \left|\operatorname{Hom}_{\mathbb{F}_q}(V,U)\right| = q^{n\cdot\dim U}
\end{aligned}$$

Es gilt

$$g(U) = \sum_{A\leq U} f(A)$$

Möbius-Inversion:

$$\begin{aligned}
f(U) &= \sum_{A \leq U} \mu(A,U) \cdot g(A) \\
&= \sum_{A \leq U} (-1)^{\dim U/A} \cdot q^{\binom{\dim U/A}{2}} \cdot q^{n \cdot \dim A} \\
&= \sum_{j=0}^{l} (-1)^{l-j} \begin{bmatrix} l \\ j \end{bmatrix}_q q^{\binom{l-j}{2}+nj}
\end{aligned}$$

Anzahl der surjektiven $\mathbb{F}_q$-Homomorphismen $V \to W$ ist $f(W)$ (mit $\dim W = m$)

$$= \sum_{k=0}^{m} \begin{bmatrix} m \\ k \end{bmatrix}_q (-1)^{m-k} q^{\binom{m-k}{2}+nk}$$

Korollar 3.8: Die Anzahl der $n \times m$-Matrizen über $\mathbb{F}_q$ vom Rang l ist

$$\begin{bmatrix} m \\ l \end{bmatrix}_q \sum_{j=0}^{l} (-1)^{l-j} \begin{bmatrix} l \\ j \end{bmatrix}_q q^{\binom{l-j}{2}+nj}$$

4 Galoistheorie

Der “triviale Anteil” am Hauptsatz der Galois-Theorie besteht aus folgenden Tatsachen über “Galois-Korrespondenzen”.

Definition 4.1: Eine *Galois-Korrespondenz* besteht aus zwei halbgeordneten Mengen $(X, \leq)$, $(Y, \leq)$ mit Abbildungen $\varphi : X \to Y$, $\psi : Y \to X$, die folgende Bedingungen erfüllen: Da die Bedingungen symmetrisch in φ, ψ sind, schreiben wir a' für $\varphi(a)$ bzw. $\psi(a)$ je nachdem, ob $a \in X$ oder $a \in Y$.

1. $a \leq b \Rightarrow b' \leq a'$
2. $a \leq a''$

Beispiel: O Menge von Objekten, E Menge von Eigenschaften (zB. Bücher in einer Bibliothek und Schlagworte im Katalog), $X = (\mathcal{P}(O), \subseteq)$, $Y = (\mathcal{P}(E), \subseteq)$.

$$\begin{array}{ll} A \subseteq O & A \mapsto A' = \{e \in E \mid \forall a \in A : a \text{ hat Eigenschaft } e\} \\ B \subseteq E & B \mapsto B' = \{a \in O \mid \forall b \in B : a \text{ hat Eigenschaft } e\} \end{array}$$

Beispiel: $O = K[x_1, \ldots, x_n]$, $E = K^n$, Galois-Korrespondenz zwischen $\mathcal{P}(O), \mathcal{P}(K^n)$ gegeben durch

$$\begin{aligned} A \subseteq K[x_1, \ldots, x_n] &\mapsto Z(A) = A' = \{b \in K^n \mid \forall f \in A : f(b) = 0\} \\ B \subseteq K^n &\mapsto J(B) = B' = \{f \in K[x_1, \ldots, x_n] \mid \forall b \in B : f(b) = 0\} \end{aligned}$$

Lemma 4.1: Wenn zwischen $(X, \leq)$, $(Y, \leq)$ eine Galois-Korrespondenz $x \mapsto x'$ besteht, dann

1. $a''' = a'$
2. äquivalent ist $a'' = a$ und $\exists\, b : a = b'$
3. Bijektion zwischen allen Galois-abgeschlossenen Elementen von X und allen von Y gegeben durch (Einschränkung von) $x \mapsto x'$.

Notation: Die Elemente mit $a'' = a$ heißen *Galois-abgeschlossen*.

Die Galois-Korrespondenz, die der Theorie ihren Namen gegeben hat, ist: für eine Körpererweiterung $K \subseteq F$ sei X die Menge der Zwischenkörper $\{L \mid L \text{ Körper } K \subseteq L \subseteq F\}$ und $G = \operatorname{Aut}_K F = \{\sigma \in \operatorname{Aut} F \mid \forall k \in K : \sigma(k) = k\}$, Y die Menge der Untergruppen von G (X, Y durch $\subseteq$ geordnet) mit der Korrespondenz Körper $L \mapsto L' = \{\sigma \in G \mid \forall l \in L : \sigma(l) = l\}$, $H \leq G$, $H \mapsto H'$ (Fixkörper von H)

$$\begin{aligned} H' &= \{a \in F \mid \forall \sigma \in H : \sigma(a) = a\} \\ &= \bigcap_{\sigma \in H} \operatorname{Fix} \sigma \leq F \end{aligned}$$

$K \subseteq H' \subseteq F$.

Definition 4.2: Nennen eine Körper-Erweiterung $F:K$ eine *Galois-Erweiterung*, wenn $G' = K$, dh. wenn $K'' = (\operatorname{Aut}_K F)' = K$ (die Gruppe der K-Automorphismen von F hat als Fixkörper nur K, nicht etwa einen größeren Körper $K'' \supseteq K$).

$$\begin{array}{ccc} F & & F' \\ \vdots & & \vdots \\ L & \longmapsto & L' \\ H' & \longleftarrow\!\!\shortmid & H \\ \vdots & & \vdots \\ G' & \longleftarrow\!\!\shortmid & G \end{array}$$

mit $\{\mathrm{id}\} = F'$, $\{\mathrm{id}\}'' = F''' = F' = \{\mathrm{id}\}$, $G = \operatorname{Aut}_K F = K'$, $G' = K''$, $G'' = K''' = K' = G$.

Es sind F, $\{\mathrm{id}\}$, $G = \operatorname{Aut}_K F$ immer Galois-abgeschlossen; es könnte $G' = K'' \supsetneqq K$ sein, Galois $:\Leftrightarrow K'' = K$.

Anderer Zugang zur Galois-Theorie: startet mit Körper F und Gruppe $G \leq \operatorname{Aut} F$, setzt

$$K := \operatorname{Fix} G = \bigcap_{g \in G} \operatorname{Fix} g$$

dann $F:K$ Galois-Erweiterung.

4.1 Hauptsatz der Galois-Theorie, 1. Teil

Satz 4.2 (Hauptsatz der Galois-Theorie, 1. Teil)**:** $F:K$ endlichdimensionale Galois-Erweiterung (dh. K Fixkörper von $\operatorname{Aut}_K F$), dann ist durch $L \mapsto L' = \{\sigma \in \operatorname{Aut}_K F \mid \forall\, l \in L : \sigma(l) = l\}$ für L Körper mit $K \subseteq L \subseteq F$ und $H \mapsto H' = \{a \in F \mid \forall\, \sigma \in H : \sigma(a) = a\}$ für $H \subseteq \operatorname{Aut}_K F$ eine Bijektion zwischen allen Zwischenkörpern L ($K \subseteq L \subseteq F$) und allen Untergruppen von $\operatorname{Aut}_K F$ gegeben, und $[A:B] = [B':A']$ für alle A, B Zwischenkörper von $F:K$ bzw. A, B Untergruppen von $\operatorname{Aut}_K F$ (wegen Bijektion zwischen Galois-abgeschlossenen Elementen einer Galois-Korrespondenz genügt es, zu zeigen, alle Zwischenkörper, alle Untergruppen sind Galois-abgeschlossen: $A'' = A$)

Anmerkung (Übung)*:* $F:K$ endlicher Körper $\Rightarrow$ $F:K$ Galois (Fortsetzbarkeit von Isomorphismen auf einfacher Erweiterungen).

Anmerkung (Vorschau)*:* Es gilt für algebraische Körpererweiterungen $F:K$: $F:K$ Galois $\Leftrightarrow$ $F:K$ separabel und normal $\Leftrightarrow$ $F:K$ separabel und F Zerfällungskörperüber K einer Menge von Polynomen $\subseteq K[x]$). Daher insbesondere für perfekten Körper K (insbesondere endliche Körper und solche mit $\chi(K) = 0$) gilt: $F:K$ algebraisch $\Rightarrow$ ($F:K$ Galois $\Leftrightarrow$ $F:K$ Zerfällungskörper).

Anmerkung: $\sigma \in \operatorname{End} F$, $K \subseteq F$, $f \in K[x]$; wenn σ die Elemente von K elementweise fix lässt, dann bildet σ Nullstellen von f auf Nullstellen von f ab: $u \in F$ mit $f(u) = 0$, dann $f(\sigma(u)) =$

$\sigma(f(u)) = \sigma(0) = 0$, $f(\sigma(u)) = \sigma(f(u))$ weil, wenn $f = \sum a_k x^k$, $a_k \in K$, dann

$$\begin{aligned}\sigma(f(u)) &= \sigma\left(\sum a_k u^k\right) = \sum \sigma(a_k)\sigma(u)^k \\ &= \sum a_k \sigma(u)^k = f(\sigma(u))\end{aligned}$$

Insbesondere: $\sigma \in \operatorname{Aut} F$, dann permutiert σ die Nullstellen in F von $f \in K[x]$.

Lemma 4.3: $F:K$ Körpererweiterung, $F \supseteq M \supseteq L \supseteq K$, $M:L$ Zwischenkörper mit $[M:L]$ endlich, dann $[L':M']$ (endlich) $\leq [M:L]$.

Korollar 4.4: $F:K$ endlichdimensional, dann $|\operatorname{Aut}_K F| \leq [F:K]$.

Beweis Spezialfall einfache algebraische Erweiterung. $M = L[u], L' = \operatorname{Aut}_L F, M' = \operatorname{Aut}_M F = \{\sigma \in \operatorname{Aut}_L F \mid \sigma(u) = u\} = \operatorname{Stab}_{\operatorname{Aut}_L F}(u)$. $[L':M'] = [\operatorname{Aut}_L F : \operatorname{Stab}_{\operatorname{Aut}_L F}(u)]$ ist die Anzahl der Links-Nebenklassen von $\operatorname{Stab}(u)$ in $\operatorname{Aut}_L F$, es gibt eine Bijektion zwischen Links-Nebenklassen von $\operatorname{Stab}(u)$ in $\operatorname{Aut}_L F$ und dem Orbit von u unter $\operatorname{Aut}_L F$ dh. der Menge der Bilder $\sigma(u)$, $\sigma \in \operatorname{Aut}_L F$. Da u algebraisch über L, u Nullstelle seines Minimalpolynoms $f \in L[x]$ über K, alle $\sigma(u)$ mit $\sigma \in \operatorname{Aut}_L F$ sind auch Nullstellen von f, von denen es genau $[L[u]:L]$ viele gibt: also
$[L':M'] \leq [L[u]:L] = [M:L]$ □

Beweis allgemeiner Fall. Durch Induktion nach $[M:L]$:

- $[M:L] = 1, M = L \Rightarrow M' = L'$.
- $[M:L] = n > 1$: Wähle $u \in M \setminus L$, wenn $M = L[u]$ fertig, sonst

  Nach Induktionsvoraussetzung ist $[L':L[u]'] \leq [L[u]:L]$ und $[L[u]':M'] \leq [M:L[u]]$. Insgesamt: $[L':M'] = [L':L[u]'] \cdot [L[u]':M'] \leq [L[u]:L] \cdot [M:L[u]] = [M:L]$ ✓.

□

Korollar 4.5 (Übung)**:** Nach voriger Übung gilt für K, F endlich, dass $F:K$ Galois). $\operatorname{Aut}_K F$ erzeugt von ψ, $\psi(x) = x^q$, $|K| = q$.

Anmerkung: $\operatorname{Aut}_K F$ Galoisgruppe von F über K.

Lemma 4.6: $K \subseteq F$ Körpererweiterung, $J, H \leq \operatorname{Aut}_K F$, $H \subseteq J$. Wenn $[J:H]$ endlich, dann $[H':J'] \leq [J:H]$.

Beweis. $\sigma_1, \dots, \sigma_k$ Repräsentantensystem der Linksnebenklassen von H in J.
Angenommen $[H':J'] > k$, seien $u_1, \dots, u_{k+1} \in H'$ so gewählt, sodass sie J'-linear unabhängig sind. Betrachten lineares Gleichungssystem

$$\begin{aligned}\sigma_1(u_1)x_1 + \sigma_1(u_2)x_2 + \ldots + \sigma_1(u_{k+1})x_{k+1} &= 0 \\ &\vdots \\ \sigma_k(u_1)x_1 + \sigma_k(u_2)x_2 + \ldots + \sigma_k(u_{k+1})x_{k+1} &= 0\end{aligned}$$

Mehr Variablen als Gleichungen, es existiert eine nichttriviale Lösung $(a_1, \dots, a_{k+1}) \in F^{k+1}$. Sei $(a_1, \dots, a_{k+1}) \in F^{k+1} \setminus \{0\}$ Lösung mit minimal vielen $a_i \neq 0$, also oBdA $a_1, \dots, a_r \neq 0, a_{r+1}, \dots, a_{k+1} = 0$.
Anmerkung: für $\sigma \in J$ gilt: $(a_1, \dots, a_{k+1})$ Lösung, dann auch $(\sigma(a_1), \dots, \sigma(a_{k+1})$. Klarerweise ist dieses $(\sigma(a_1), \dots, \sigma(a_{k+1}))$ Lösung von

$$\sigma\sigma_1(u_1)x_1 + \ldots + \sigma\sigma_1(u_{k+1})x_{k+1} = 0$$
$$\vdots$$
$$\sigma\sigma_k(u_1)x_1 + \ldots + \sigma\sigma_k(u_{k+1})x_{k+1} = 0$$

Dieses Gleichungssystem ist aber dasselbe mit vertauschten Gleichungen, da erstens $\sigma_i(u_j)$ nur von der Linksnebenklasse von H in J abhängt ($\pi \in H \Rightarrow \pi(u_j) = u_j$, daher $\sigma_i\pi(u_j) = \sigma_i(u_j)$) und $\{\sigma\sigma_1, \sigma\sigma_2, \dots, \sigma\sigma_k\}$ wieder Repräsentantensystem der Linksnebenklassen von H in J ist.

$(a_1, \dots, a_{k+1})$ Lösung $\neq 0$ mit minimal vielen $a_i \neq 0$, durch Multiplikation mit $a_1^{-1} \in F$ erhält man Lösung $(1, a_2, \dots, a_{k+1})$, wobei eines der a_i nicht aus J' ist. Zeile des Gleichungssystems mit $\sigma_i H = H$ ergibt $u_1a_1 + u_2a_2 + \ldots + u_{k+1}a_{k+1} = 0$. Die u_i waren J'-linear unabhängig, also ein $a_i \notin J'$. Dieses a_i ist $\notin \{0, 1\}$ (0, 1 werden von allen $\sigma \in \operatorname{Aut} F$ fix gelassen), oBdA $a_2 \notin J'$. Sei $\sigma \in J$ mit $\sigma(a_2) \neq a_2$, dann $(1, a_2, \dots, a_{k+1}) - (\sigma(1), \sigma(a_2), \dots, \sigma(a_{k+1})) = (0, a_2 - \sigma(a_2) \neq 0, b_3, \dots, b_r, 0, \dots, 0)$ Lösung $\neq 0$ mit weniger als r Koordinaten ungleich 0, Widerspruch zur Minimalität. □

Lemma 4.7: $F : K$ Körpererweiterung, A, B Zwischenkörper von $F : K$ oder Untergruppen von $\operatorname{Aut}_K F$ mit $B \subseteq A$. Dann gilt: wenn B Galois-abgeschlossen, dann auch A und weiters $[A : B] = [B' : A']$.

Beweis. Sei $[A : B]$ endlich, dann $[B' : A']$ endlich $\leq [A : B]$ und weiters $[A'' : B''] \leq [B' : A']$. Wenn also $B'' = B$, dann ($A'' \supseteq A$) $[A : B] \leq [A'' : B] = [A'' : B''] \leq [B' : A'] \leq [A : B]$. Daher $[A'' : B] = [A : B]$ endlich, wegen $A'' \supseteq A$ folgt $A'' = A$, außerdem $[A : B] = [B' : A']$. Haben gezeigt: $F : K$ Körpererweiterung, endlichdimensional. Dann $|\operatorname{Aut}_K F| = [F : K]$ endlich und alle Untergruppen von $\operatorname{Aut}_k F$ Galois-abgeschlossen. Wir haben Bijektion zwischen Galois-abgeschlossenen Zwischenkörpern (Übung: das sind genau die Körper L mit $K'' \subseteq L$) gegeben durch $A \mapsto A'$ mit $[A : B] = [B' : A']$ für alle A, B Untergruppen von $\operatorname{Aut}_K F$ oder abgeschlossene Zwischenkörper. Im Falle $F : K$ endlichdimensional Galois, dh. $(\operatorname{Aut}_K F)' = K$ [bzw. $K'' = K$] Bijektion zwischen allen Zwischenkörpern und allen Untergruppen gegeben durch $A \mapsto A'$ und es gilt $[A : B] = [B' : A']$. □

4.2 Hauptsatz der Galois-Theorie, 2. Teil

Satz 4.8 (Hauptsatz der Galois-Theorie, 2. Teil)**:** Sei $F : K$ endlichdimensionale Galois- Erweiterung und E Zwischenkörper. Dann ist äquivalent:

1. $E : K$ Galois
2. E stabil unter $\operatorname{Aut}_K F$ (dh. $\forall \sigma \in \operatorname{Aut}_K F : \sigma(E) = E$)
3. E' Normalteiler in $\operatorname{Aut}_K F$

Wenn diese äquivalenten Bedingungen auf E zutreffen, dann ist

$$\operatorname{Aut}_K E = {}^{\operatorname{Aut}_K F}/_{E'}$$

Anmerkung: $\operatorname{Aut}_K F$ heißt Galois-Gruppe der Körpererweiterung $F:K$, auch geschrieben als $\operatorname{Gal}(F:K)$. In dieser Notation

$$\operatorname{Gal}(E:K) = {}^{\operatorname{Gal}(F:K)}/_{E'}, \quad E' = \{\sigma \in \operatorname{Gal}(F:K) \mid \sigma(e) = e\,\forall\, e \in E\}$$

sofern E stabil unter $\operatorname{Gal}(F:K$ bzw. äquivalent $E' \trianglelefteq \operatorname{Gal}(F:K)$

Anmerkung: $E \subseteq F$, G Gruppe $\subseteq \operatorname{Aut} F$. E heißt stabil unter G, wenn $\forall\,\sigma \in G : \sigma(E) = E$. Da G Gruppe, folgt E stabil unter G schon aus $\forall\,\sigma \in G : \sigma(E) \subseteq E$. (Surjektion von $\sigma\big|_E : E \to E$ folgt aus $\sigma^{-1}(E) \subseteq E$ und Bijektivität von $\sigma : F \to F$).

Lemma 4.9: $F:K$ Körpererweiterung.

1. $H \leq \operatorname{Aut}_K F$, dann gilt $H \trianglelefteq \operatorname{Aut}_K F \;\Rightarrow\; H'$ stabil unter $\operatorname{Aut}_K F$.
2. L Zwischenkörper, $K \subseteq L \subseteq F$, dann L stabil unter $\operatorname{Aut}_K F \;\Rightarrow\; L' \trianglelefteq \operatorname{Aut}_K F$.

Beweis.

zu 2 L stabil, sei $\pi \in L'$, $\sigma \in \operatorname{Aut}_K F$. Zu zeigen ist $\sigma^{-1}\pi\sigma \in L'$. Für $l \in L$ gilt

$$\sigma^{-1}\pi\,\underbrace{\sigma(l)}_{\in L} = \sigma^{-1}\sigma(l) = l$$

weil $\sigma(l) \in L$ (wegen Stabilität von L) und daher $\sigma(l)$ fix unter $\pi \in L'$ ✓. Haben gezeigt: $\sigma^{-1}\pi\sigma \in L'$ für $\pi \in L', \sigma \in \operatorname{Aut}_K F$, also L' Normalteiler ✓.

zu 3 $H \trianglelefteq \operatorname{Aut}_K F$. Angenommen H' nicht stabil, sei $\sigma \in \operatorname{Aut}_K F$, $u \in H'$ mit $\sigma(u) \notin H'$. Wählen $\pi \in H$ mit $\pi(\sigma(u)) \neq \sigma(u)$, dann $\sigma^{-1}\pi\sigma(u) \neq u$, da aus $\pi(\sigma(u)) \neq \sigma(u)$ und Bijektivität von σ^{-1} folgt $\sigma^{-1}\pi\sigma(u) \neq \sigma^{-1}(\sigma(u)) = u$.

□

Anmerkung: $F:K$ endlichdimensionale Galois-Erweiterung, dann $F:E$ Galois für jeden Zwischenkörper ($E'' = E$ äquivalent dazu), bzw für beliebige Körpererweiterung $F:K$ ist $F:E$ Galois äquivalent zu E Galois-abgeschlossen. Zeigen Äquivalenzen für $E:K$ Galois.

Lemma 4.10: E Zwischenkörper von $F:K$. Wenn $F:K$ Galois und E stabil unter $\operatorname{Aut}_K F$, dann $E:K$ Galois.

Beweis. $K'' = K \;\Rightarrow\; \forall\, e \in E \setminus K : \exists\,\sigma \in \operatorname{Aut}_K F$ mit $\sigma(e) \neq e$, wegen Stabilität von E unter $\operatorname{Aut}_K F$ kann man σ einschränken auf $\sigma\big|_E \in \operatorname{Aut}_K E$, also $\exists\,\sigma \in \operatorname{Aut}_K E$ mit $\sigma(e) \neq e$. □

Lemma 4.11: E Zwischenkörper von $F:K$, $F:K$ Galois. Wenn $E:K$ algebraisch und Galois, dann E stabil unter $\operatorname{Aut}_K F$.

Beweis. Sei $e \in E$. Zu zeigen: $\forall \sigma \in \operatorname{Aut}_K F$ gilt $\sigma(e) \in E$. Sei $f \in K[x]$ Minimalpolynom von e über K (E algebraisch über K), $\deg f = n$. Seien $e = e_1, e_2, \dots, e_r$ alle Nullstellen (mit Vielfachheiten) von f in E. Betrachten $g = (x - e_1)(x - e_2) \cdots (x - e_r) \in E[x]$. Jedes $\sigma \in \operatorname{Aut}_K F$ permutiert die Nullstellen von f in F, da $\sigma(E) = E$, permutiert σ auch die Nullstellen von f in E. σ permutiert $e_1, \dots, e_r \Rightarrow$ für alle Koeffizienten a_k von g gilt $\sigma(a_k) = a_k$ (Koeffizienten sind elementarsymmetrische Funktionen in den Nullstellen $e_1, e_2, \dots, e_r$). Koeffizienten von g in $(\operatorname{Aut}_K F)' = K$, $g \in K[x]$ mit $\deg g \le \deg f$ und $g(e) = 0 \Rightarrow f \bigm| g$ und daher $f = g$ (beide normiert). Alle Nullstellen von f in F sind schon in E, insbesondere ist für jedes $\sigma \in \operatorname{Aut}_K F$ $\sigma(e) \in E$ (σ permutiert die Nullstellen von f). $\square$

Hauptsatz der Galois-Theorie, Teil 2

Bereits bewiesen: Wenn $F : K$ algebraisch, dann gilt für Zwischenkörper E: $E : K$ Galois genau dann, wenn E stabil unter $\operatorname{Aut}_K F$ (dh. $\sigma(E) = E$ für $\sigma \in \operatorname{Aut}_K F$). E stabil $\Rightarrow E' \trianglelefteq \operatorname{Aut}_K F$; H' stabil $\Leftarrow H \trianglelefteq \operatorname{Aut}_K F$.

Lemma 4.12: Wenn $F : K$ algebraische Körpererweiterung, E stabiler Zwischenkörper; dann ist ${}^{\operatorname{Aut}_K F}\!/_{E'}$ isomorph zur Untergruppe von $\operatorname{Aut}_K E$ bestehend aus jenen Automorphismen von E, die auf F fortsetzbar sind; im Spezialfall $[F : K]$ endlichdimensionale Galois-Erweiterung gilt $\operatorname{Aut}_K E \simeq {}^{\operatorname{Aut}_K F}\!/_{E'}$.

Beweis. E stabil $\Rightarrow E' \trianglelefteq \operatorname{Aut}_K F$, $E : K$ Galois, $\varphi : \operatorname{Aut}_K F \to \operatorname{Aut}_K E$ mit $\varphi(\sigma) = \sigma\big|_E$ (wohldefiniert, weil $\forall \sigma \in \operatorname{Aut}_K F : \sigma(E) = E$, also $\sigma\big|_E : E \to E$ Automorphismus). φ Gruppenhomomorphismus,

$$\begin{aligned} \ker \varphi &= \operatorname{Aut}_K E \\ \operatorname{Im} \varphi &= \{\pi \in \operatorname{Aut}_K E : \exists \sigma \in \operatorname{Aut}_K F : \sigma\big|_K = \pi\}, \end{aligned}$$

das ist {alle K-Automorphismen von E, die auf F fortsetzbar sind}. Für $[F : K]$ endlichdimensional und Galois:

$$|\operatorname{Aut}_K F| = [F : K], \quad E' = [E' : \{\mathrm{id}\}] = [F : E]$$

also

$$|{}^{\operatorname{Aut}_K F}\!/_{E'}| = {}^{[F:K]}\!/_{[F:E]} = [E : K] = [\operatorname{Aut}_K E]$$

Daher $\operatorname{Im} \varphi$ Untergruppe von $\operatorname{Aut}_K E$, gleichmächtig wie $\operatorname{Aut}_K E$ also $\operatorname{Im} \varphi = \operatorname{Aut}_K E$. $\square$

Satz 4.13: $F : K$ algebraische Körpererweiterung, $F : K$ Galois $\Leftrightarrow$ $F : K$ separabel und normal, bzw. $F : K$ Galois $\Leftrightarrow$ $F : K$ separabel und F Zerfällungskörper über K, einer Menge von Polynomen $\in K[x]$.

Anmerkung: Wissen bereits: $F : K$ algebraisch $\Rightarrow$ ($F : K$ normal $\Leftrightarrow$ $F : K$ Zerfällungskörper).

Beweis. $F : K$ Galois, sei $u \in F$ mit $f \in K[x]$ Minimalpolynom von u über K, seien $u_1, \dots, u_k$ die verschiedenen Nullstellen von f in F (je einmal), $g = (x - u_1) \cdots (x - u_k)$. Die Koeffizienten von g sind elementarsymmetrische Polynome in $u_1, \dots, u_k$, als unter Permutation der u_i invariant, daher unter allen $\sigma \in \operatorname{Aut}_k F$ invariant (jedes $\sigma \in \operatorname{Aut}_K F$ permutiert $u_1, \dots, u_k$). Da $F : K$ Galois, gilt $K'' = K$, also sind die Koeffizienten von g in K; außerdem $g(u) = 0$, daher $f \mid g$ in $K[x]$, $\deg g \leq \deg f$, also $f = g$ (beide normiert). f zerfällt über F in Linearfaktoren, $\deg f$ viele verschiedene Nullstellen, f separabel und f zerfällt über F (f beliebig irreduzibel in $K[x]$ mit Nullstellen in F $\Rightarrow f$ separabel, f zerfällt über F), also $F : K$ normal, separabel. $\square$

Lemma 4.14: $F : K$ algebraische Körpererweiterung. $F : K$ Galois $\Leftrightarrow$ F Zerfällungskörper einer Menge von separablen irreduziblen Polynomen $\in K[x]$

Beweis.

"$\Rightarrow$" schon im vorigen Satz

"$\Leftarrow$" $u \in F \setminus K$, dann $u \in L = K(v_1, \dots, v_k)$, $v_1, \dots, v_k$ Nullstellen von $f_1, \dots, f_k \in K[x]$ separabel, seien $u_1, \dots, u_r$ alle Nullstellen von $f_1, \dots, f_k \in F$, $E = K(u_1, \dots, u_r)$. $E : K$ Zerfällungskörper separabler Polynome, $E : K$ endlichdimensional. Angenommen, Behauptung stimmt für endlichdimensionale Erweiterungen, dann folgt $E : K$ Galois dh. $\exists\, \sigma \in \operatorname{Aut}_K E$ mit $\sigma(u) \neq u$ und σ fortsetzbar zu $\pi \in \operatorname{Aut}_K F$, da F Zerfällungskörper über E (von demselben Polynom wie über K).

Zeigen jetzt Behauptung für $[F : K]$ endlich mittels Induktion nach $n = [F : K]$: $[F : K] = 1$ ✓;
Sei $u \in F \setminus K$, $K[u]$ Zwischenkörper mit $[K[u] : K] = s = \deg f$ mit $f \in K[x]$ Minimalpolynom von u über K. Wissen, dass $|\operatorname{Aut}_K F| \leq [F : K]$, nämlich

$$|\operatorname{Aut}_K F| = |\operatorname{Aut}_{K''} F| = [F : K'']$$

Für $F : K$ Galois genügt es, zu zeigen $[F : K''] = [F : K]$ (da $K'' = K$ folgt) also genügt es, zu zeigen $|\operatorname{Aut}_K F| = [F : K]$

$$\begin{array}{cc}
F & \{\mathrm{id}\} \\
 & \\
K[u] & K[u]' = \operatorname{Aut}_{K[u]} F \\
|s & |s \\
K & \operatorname{Aut}_K F
\end{array}$$

Bijektion zwischen Links-Nebenklassen von $K[u]'$ in $\operatorname{Aut}_{K[u]} F$ und $u_1, \dots, u_s$, den verschiedenen Nullstellen von f in F gegeben durch

$$\sigma(K[u]) \mapsto \sigma(u)$$

Also

$$[K[u] : K] = s = [\operatorname{Aut}_K F : \operatorname{Aut}_{K[u]} F]$$

außerdem $F : K[u]$ Zerfällungskörper von separablem Polynom $\in K[x]$ mit $[F : K[u]] < [F : K]$. Nach Induktionsvoraussetzung $F : K[u]$ Galois,

$$[F : K[u]] = \left|\operatorname{Aut}_{K[u]} F\right|$$

insgesamt

$$[F : K] = [F : K[u]] \cdot [K[u] : K] = \left|\operatorname{Aut}_{K[u]} F\right| \cdot s = (K[u]')[\operatorname{Aut}_K F : K[u]'] = |\operatorname{Aut}_K F|$$

Haben also

$$[F:K] = |\mathrm{Aut}_K F| = |\mathrm{Aut}_{K''} F| = [F:K'']$$

Wegen $K \subseteq K''$ und endlichdimensional folgt $K = K''$, $F:K$ Galois.

$\square$

Satz 4.15: $F:K$ algebraische Körpererweiterung, Galois (dh. $K'' = K$), dann ist durch die Galois-Korrespondenz eine Bijektion zwischen allen Zwischenkörpern und den Galois-abgeschlossenen Untergruppen von $\mathrm{Aut}_K F$ gegeben; insbesondere $F:E$ Galois für jeden Zwischenkörper E. Außerdem $E:K$ Galois $\Leftrightarrow$ E stabil unter $\mathrm{Aut}_K F$ und $E:K$ Galois $\Leftrightarrow$ $E' \trianglelefteq \mathrm{Aut}_K F$ und es gilt für stabilen Zwischenkörper E:

$$\mathrm{Aut}_K E \simeq {}^{\mathrm{Aut}_K F}/_{E'} \; (= {}^{\mathrm{Aut}_K F}/_{\mathrm{Aut}_E F})$$

Beweis. Bijektion zwischen Galois-abgeschlossenen Zwischenkörpern und Galois-abgeschlossenen Untergruppen sowieso. $F:K$ Galois $\Rightarrow$ $F:K$ Zerfällungskörper einer Menge separabler Polynome über K, daher $F:E$ Zerfällungskörper derselben Menge von Polynomen über E, deren irreduzible Faktoren in $E[x]$ wieder separabel, also $F:E$ Galois, dh. $E'' = E$, E Galois-abgeschlossen.

Schon gezeigt $E:K$ Galois $\Leftrightarrow$ E stabil unter $\mathrm{Aut}_K F$ und für E mit $E'' = E$ $E:K$ Galois $\Leftrightarrow$ $E' \trianglelefteq \mathrm{Aut}_K F$.

Für

$$\mathrm{Aut}_K E \simeq {}^{\mathrm{Aut}_K F}/_{\mathrm{Aut}_E F}$$

brauchen wir nur mehr, dass jedes $\sigma \in \mathrm{Aut}_K E$ zu $\pi \in \mathrm{Aut}\, F$ fortsetzbar ist. $\sigma \in \mathrm{Aut}\, E$ ist zu $\sigma \in \mathrm{Aut}\, F$ fortsetzbar, weil F Zerfällungskörper über E. $\square$

Beispiel: F, K endliche Körper $\Rightarrow$ $F:K$ Galois, da K perfekt, also jede Erweiterung separabel und F Zerfällungskörper von $x^q - x$ über K, $q = |K|$. $\mathrm{Aut}_K F = \langle\psi\rangle$, $\psi(x) = x^q$, $|\langle\psi\rangle| = n$ wenn $|F| = q^n = [F:K]$. Für $\ell \mid n$ ist der Fixkörper von $\langle\psi^\ell\rangle = \{u \in F \mid u^{q^\ell} - u = 0\}$ der eindeutig bestimmte Unterkörper von F mit q^ℓ Elementen.

Beispiel: A der algebraische Abschluss von $\mathbb{Z}_p$, $A:\mathbb{Z}_p$ algebraische Erweiterung, nicht endlichdimensional. A normal und separabel über $\mathbb{Z}_p$, also $A:\mathbb{Z}_p$ Galois. Die von $\psi : A \to A$, $\psi(x) = x^p$ (Frobenius-Homomorphismus) erzeugte Untergruppe von $\mathrm{Aut}_{\mathbb{Z}_p} A$ hält nur die Elemente von $\mathbb{Z}_p$ punktweise fest, ist aber nicht ganz $\mathrm{Aut}_{\mathbb{Z}_p} A$, dh. $\langle\psi\rangle'' = \mathbb{Z}_p' = \mathrm{Aut}_{\mathbb{Z}_p} A \neq \langle\psi\rangle$, $\langle\psi\rangle$ nicht-Galois-abgeschlossene Untergruppe $\leq \mathrm{Aut}_{\mathbb{Z}_p} A$.

5 Norm, Spur und Basis

5.1 Norm und Spur

Definition 5.1: Im Spezialfall $F : K$ endlichdimensionale Galois-Erweiterung: *Norm* $N_K^F : F \to K$, *Spur* $T_K^F : F \to K$ definiert durch

$$\begin{aligned} N_K^F(u) &= \sigma_1(u) \cdot \sigma_2(u) \cdots \sigma_n(u) \\ T_K^F(u) &= \sigma_1(u) + \sigma_2(u) + \ldots + \sigma_n(u) \end{aligned}$$

wobei $\{\sigma_1, \ldots, \sigma_n\} = \operatorname{Aut}_K F$ $(n = [F : K])$.

Anmerkung: Abkürzende Schreibweise: N, T für N_K^F, T_K^F.

Lemma 5.1: $F : K$ endlichdimensional-Galois, dann

1. $\forall\, u \in F : N_K^F(u) \in K, T_K^F(u) \in K$ (daher $N_K^F, T_K^F : F \to K$ wohldefinierte Funktionen)
2. $N(u) \cdot N(v) = N(u \cdot v)$, $T(u) + T(v) = T(u + v)$.
3. Für $u \in K$:

$$\begin{aligned} N(u) &= u^{[F : K]} \\ T(u) &= [F : K] \cdot u \end{aligned}$$

4. wenn $F = K[u]$ und $f = x^n + an_{n-1}x^{n-1} + \ldots + a_1x + a_0$ das Minimalpolynom in $K[x]$ von u, dann

$$\begin{aligned} N(u) &= (-1)^n a_0 \\ T(u) &= -a_{n-1} \end{aligned}$$

Allgemein, wenn $u \in F$ mit Minimalpolynom wie oben, dann

$$\begin{aligned} N(u) &= ((-1)^n a_0)^{[F : K[u]]} \\ T(u) &= -[F : K[u]] \cdot a_{n-1} \end{aligned}$$

5. $K \subseteq E \subseteq F$, dann

$$\begin{aligned} N_K^E \circ N_E^F &= N_K^F \\ T_K^E \circ T_E^F &= T_K^F \end{aligned}$$

Definition 5.2: Für $F : K$ endlichdimensionale Körpererweiterung, $\overline{K}$ sei algebraischer Abschluss von K, $\overline{K} \supseteq F \supseteq K$, für $u \in F$ ist

$$\begin{aligned} N_K^F(u) &= \sigma_1(u) \cdots \sigma_n(u) \\ T_K^F(u) &= \sigma_1(u) + \ldots + \sigma_n(u) \end{aligned}$$

wobei $\sigma_1, \ldots, \sigma_n$ alle injektiven Einbettungen von F in $\overline{K}$, die K punktweise gleich lassen, durchläuft.

Definition 5.3: $F:K$ separable algebraische Erweiterung, endlich-dimensional mit $[F:K] = n$. Definiere

$$N = N_K^F : \; F \to K,$$
$$T = T_K^F : \; F \to K$$

mit

$$N(u) = \sigma_1(u) \cdot \sigma_2(u) \cdots \sigma_n(u)$$
$$T(u) = \sigma_1(u) + \sigma_2(u) + \ldots + \sigma_n(u)$$

wobei $\sigma_1, \ldots, \sigma_n$ alle verschiedenen K-Einbettungen von F in $\overline{K}$ ($\overline{K}$ algebraischer Abschluss von K, der F enthält) durchläuft.

Statt $\overline{K}$ kann man in der Definition auch N, den normalen Abschluss der Erweiterung $F:K$ verwenden; N ist der eindeutig bestimmte kleinste Körper mit $\overline{K} \supseteq N \supseteq F \supseteq K$, sodass $N:K$ normal; man erhält N, indem man den Zerfällungskörper über F aller Polynome in $K[x]$, die eine Nullstelle haben, bildet. Ohne Beweis:

$$\begin{aligned}[F:K] &= \big|\{\sigma : F \to N \;\big|\; \sigma\ K\text{-Monomorphismus}\}\big| \\ &= \big|\{\sigma : F \to \overline{K} \;\big|\; \sigma\ K\text{-Monomorphismus}\}\big|\end{aligned}$$

Letzteres gilt, weil K-Monomorphismus Nullstellen eines Polynoms $f \in K[x]$ permutiert, also $\sigma(F) \subseteq F$.

Es gilt

1. $\forall\, u \in F : \; N_K^F(u), T_K^F(u) \in K$
2. $N_K^F(uv) = N_K^F(u) \cdot N_K^F(v)$
3. $T_K^F(u+v) = T_K^F(u) + T_K^F(v)$, $T_K^F(ku) = kT_K^F(u)$ (dh. $T : \; F \to K$ ist K-linear)
4. für $u \in F$ sei $a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + x^m$ das Minimalpolynom von u über K. dann

   $$T_K^F(u) = -[F:K[u]] \cdot a_{n-1}$$
   $$N_K^F(u) = ((-1)^m a_0)^{[F:K[u]]}$$

5. $F \supseteq E \supseteq K$, dann

   $$N_K^E \circ N_E^F = N_K^F$$
   $$T_K^E \circ T_E^F = T_K^F$$

   Im Spezialfall $F:K$ endlichdimensional Galois ist $N = F$ und $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Aut}_K\, F$
6. Für $k \in K$ ist

   $$N_K^F(k) = k^{[F:K]}$$
   $$T_K^F(k) = [F:K] \cdot k$$

Lemma 5.2 (Artin-Lemma)**:** F Körper, $\varphi_1, \ldots, \varphi_n : (G_i) \to (F^*, \cdot)$ verschiedene Gruppenhomomorphismen, dann sind $\varphi_1, \ldots, \varphi_n$ F-linear unabhängig, dh. wenn für $a_1, \ldots, a_n \in F$ gilt $a_1\varphi_1 + \ldots + a_n\varphi_n = 0$ (die Funktion konstant 0), dann folgt $a_1 = a_2 = \ldots = 0$ (dh. im F-Vektorraum F^G aller Funktionen $G \to F$ mit elementweisen Operationen).

Beweis. Induktion nach n.

Für $n = 1$: $\varphi(e_G) = 1 \neq 0$, daher auch kein Vielfaches, außer $a = 0$.

$n - 1 \to n$: Sei $a_1\varphi_1(x) + \ldots + a_n\varphi_n(x) = 0 \diamondsuit$. OBdA alle $a_i \neq 0$ sonst folgt Behauptung aus Induktionsvoraussetzung; $\varphi_1, \ldots, \varphi_n$ verschieden, sei $g \in G$, sodass $\varphi_1(g) \neq \varphi_n(g)$. In $\diamondsuit$ gx für x einsetzen und mit $\varphi_n(g)^{-1}$ multiplizieren. Dann $a_1\varphi_n(g)^{-1}\psi_1(g)\varphi_1(x) + \ldots + a_n\varphi_n(g)^{-1}\varphi_n(g)\varphi_n(x) = 0 \heartsuit$. Subtraktion $\heartsuit - \diamondsuit$ liefert Gleichung $b_1\varphi_1(x) + \ldots + b_{n-1}\varphi_{n-1}(x) = 0$, dh. $b_1 = a_1 - a_1(\varphi_n(g)^{-1}\varphi_1(g)) \neq 0$, Widerspruch zur Induktionsvoraussetzung, dass $\varphi_1, \ldots, \varphi_{n-1}$ F-linear unabhängig. $\square$

Korollar 5.3: Verschiedene Automorphismen eines Körpers F sind F-linear unabhängig. ($\varphi \in \operatorname{Aut} F \to \varphi(0) = 0$, φ bijektiv, also $\varphi\big|_{F^*} : F^* \to F^*$ Automorphismus von $(F^*, \cdot)$), insbesondere sind die in Definition von N, T vorhandenen $\sigma_1, \ldots, \sigma_n$ F-linear unabhängig.

Korollar 5.4: $T_K^F : F \to K$ surjektive K-lineare Funktionale. $\operatorname{Im} T$ ist K-Unterraum von K, also K oder (0), nicht (0), weil $T = \sigma_1 + \sigma_2 + \ldots + \sigma_n$ nichttriviale F-Linearkombination verschiedener Automorphismen von F ist.

Anmerkung: $F : K$ endlicher Körper, dann sind die K-linearen Funktionale $F : F \to K$ genau die Abbildungen $L_\beta : F \to K$ für $\beta \in F$ definiert durch

$$L_\beta(x) = T_K^F(\beta x)$$

(und für verschiedene β, γ ist $L_\beta \neq L_\gamma$).

Beweis. $L(x, y) = T_K^F(xy)$ K-bilinear, $L_\beta(y) = L(\beta, y) = T(\beta y)$ K-linear, $L_\beta : F \to K$ für beliebiges $\beta \in F$, für $\beta \neq \gamma$ ist $L_\beta(x) - L_\gamma(x) = T((\beta - \gamma)x)$ nicht die 0-Funktion, $x \mapsto (\beta - \gamma)x$ bijektiv $F \to F$ und $T : F \to K$ surjektiv. Daher $|F| = |K|^{[F:K]}$ verschiedene L_β. Das sind alle K-linearen Funktionale $F \to K$. $\square$

Definition 5.4: Eine *zyklische* Körpererweiterung $F : K$ ist eine Galois-Erweiterung mit zyklischer Galoisgruppe $\operatorname{Aut}_K F$.

Analog heißt "soundso" Körpererweiterung (wobei "soundso" ein Adjektiv ist, das einer Gruppe zukommt), dass die Galois-Erweiterung mit "soundso" Galois-Gruppe gemeint ist; zB zyklische, Abelsche, auflösbare, etc Erweiterung.

Proposition 5.5: $F : K$ endlichdimensional zyklisch, $\operatorname{Aut}_K F = \langle\sigma\rangle$, dann gilt für $u \in F$

$$T_K^F(u) = 0 \Leftrightarrow \exists\, v \in F : u = v - \sigma(v)$$

Beweis 1. "$\Leftarrow$" Klar, sogar für beliebige Körpererweiterungen, $\sigma \in \operatorname{Aut}_K F$

$$T(v - \sigma(v)) = T(v) - T(\sigma(v)) = T(v) - T(v) = 0$$

"$\Rightarrow$" Weil $T : F \to K$ surjektiv, $\exists w \in F$ mit $T(w) = 1$. Für ein solches w und ein $u \in F$ mit $T(u) = 0$ sei

$$v = uw + (u + \sigma(u))\sigma(w) + (u + \sigma(u) + \sigma^2(u))\sigma^2(w) + \ldots + (u + \sigma(u) + \sigma^2(u) + \ldots + \sigma^{n-2}(u))\sigma^{n-2}(w)$$

dann (Übung) $v - \sigma(v) = uT(w)$, dh. für w mit $T(w) = 1$ gilt $v - \sigma(v) = u$.

□

Beweis 2. Einfacher Beweis für den Spezialfall $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$: Sei $\alpha \in F : 0 = T(\alpha)$. Sei β (in Erweiterung von F) Nullstelle von $x^q + x - \alpha = 0$. Zeigen: $\beta \in F$, dann $\alpha = \beta^q - \beta = \sigma(\beta) - \beta$, $\operatorname{Aut}_K F = \langle\sigma\rangle$.

$$\begin{aligned} 0 = T(\alpha) &= \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + (\beta^q - \beta)^{q^2} + \ldots + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + \beta^{q^2} - \beta^q + \beta^{q^3} - \beta^{q^2} + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta \end{aligned}$$

Daher $\beta \in \mathbb{F}_{q^m} = F$. □

Satz 5.6 (Hilberts Satz 90)**:** $F : K$ endlichdimensionale zyklische Erweiterung, $\operatorname{Aut}_K F = \langle\sigma\rangle$, dann für $u \in F$:

$$N_K^F(u) = 1 \Leftrightarrow \exists\, v \in F : U = v(\sigma(v))^{-1}$$

Beweis. "$\Leftarrow$" Für beliebige Galoiserweiterung und $\sigma \in \operatorname{Aut}_K F$ und $v \in F$ gilt

$$N(v\sigma(v)^{-1}) = N(v)N(\sigma(v))^{-1} = N(v)N(v)^{-1} = 1$$

"$\Rightarrow$" Sei $u \in F$ mit $N(u) = 1$ (insbesondere $u \neq 0$); Dan $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ ($n = [F : K]$) verschieden, sind sie F-linear unabhängig, also gibt es $w \in F$ mit

$$v = uw + (u\sigma(u))\sigma(w) + (u\sigma(u)\sigma^2(u))\sigma^2(w) + \ldots + (u\sigma(u) \cdots \sigma^{n-1}(u))\sigma^{n-1}(w) \neq 0$$

für jedes solche v gilt: $u = v\sigma(v)^{-1}$ (Übung).

□

5.2 Basen

Definition 5.5 (Basen)**:** $F : K$ endlichdimensionale Galois-Erweiterung, $[F : K] = m$, $\alpha_1, \ldots, \alpha_m$ K-Basis von F genau dann, wenn

$$\det \begin{pmatrix} T(\alpha_1\alpha_1) & \cdots & T(\alpha_1\alpha_m) \\ T(\alpha_2\alpha_1) & \cdots & T(\alpha_2\alpha_m) \\ \vdots & & \vdots \\ T(\alpha_m\alpha_1) & \cdots & T(\alpha_m\alpha_m) \end{pmatrix} = \det(T(\alpha_i\alpha_j))_{\substack{1\leq i\leq m \\ 1\leq j\leq m}} \neq 0$$

wobei $T = T_K^F$.

Korollar 5.7: $\alpha_1, \ldots, \alpha_m$ wie oben sind K-Basis von F genau dann, wenn

$$\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_m) \\ \sigma_2(\alpha_1) & \cdots & \sigma_2(\alpha_m) \\ \vdots & & \vdots \\ \sigma_m(\alpha_1) & \cdots & \sigma_m(\alpha_m) \end{pmatrix} = \det(\sigma_i(\alpha_j)) \neq 0$$

wobei $\{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_m\} = \mathrm{Aut}_K F$.

Beweis. Angenommen $T(\alpha_i\alpha_j)$ hat m K-linear unabhängige Zeilen. Sei

$$c_1\alpha_1 + \ldots + c_m\alpha_m = 0$$

dann auch

$$c_1\alpha_1\alpha_k + \ldots + c_m\alpha_m\alpha_k = 0$$

für beliebige α_k. Darauf T anwenden:

$$c_1T(\alpha_1\alpha_k) + c_2T(\alpha_2\alpha_k) + \ldots + c_mT(\alpha_m\alpha_k) = 0$$

für alle $k = 1, \ldots, m$, dh. die entsprechende K-Linearkombination der Zeilen von $(T(\alpha_i\alpha_j))$ ist 0, es folgt für alle c_i, dass $c_i = 0$.

Umgekehrt, wenn $\alpha_1, \ldots, \alpha_m$ K-linear unabhängig. Angenommen, K-Linearkombination der Zeilen von $(T(\alpha_i\alpha_j))$ mit Koeffizienten $c_i \in K$ ist 0, dh. für $k = 1, \ldots, m$:

$$c_1T(\alpha_1\alpha_k) + c_2T(\alpha_2\alpha_k) + \ldots + c_mT(\alpha_m\alpha_k) = 0$$

$$T((c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m)\alpha_k) = 0$$

für $k = 1, \ldots, m$, dh. für $\beta = c_1\alpha_1 + \ldots + c_m\alpha_m$ ist $L_\beta = 0$ weil $L_\beta(\alpha_i) = 0$ für $\alpha_1, \ldots, \alpha_m$ eine K-Basis von F; Daraus folgt $\beta = 0$, weiters folgt alle $c_i = 0$, da $\alpha_1, \ldots, \alpha_n$ K-linear unabhängig.

Korollar folgt aus

$$(\sigma_i(\alpha_j))^t \cdot (\sigma_i(\alpha_j)) = (T(\alpha_i\alpha_j))$$

also

$$\det(T(\alpha_i\alpha_j)) = (\det(\sigma_i(\alpha_j)))^2$$

(i,j)-te Eintragung von $(\sigma_i(\alpha_j))^t \cdot (\sigma_i(\alpha_j))$ ist

$$(\sigma_1(\alpha_i), \sigma_2(\alpha_i), \ldots, \sigma_n(\alpha_i)) \cdot \begin{pmatrix} \sigma_1(\alpha_i) \\ \sigma_2(\alpha_j) \\ \vdots \\ \sigma_m(\alpha_j) \end{pmatrix} = \sigma_1(\alpha_i\alpha_j) + \sigma_2(\alpha_i\alpha_j) + \ldots + \sigma_m(\alpha_i\alpha_j) = T(\alpha_i\alpha_j)$$

□

[Beweis]
Satz 5.8: $F:K$, $n = [F:K]$ endlichdimensionale zyklische Körpererweiterung $(\mathrm{Aut}_K F = \langle\sigma\rangle)$. Dann hat F eine K-Basis der Form $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)$ für ein $\alpha \in F$.

Beweis. $\sigma^n = \mathrm{id}$ und $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ verschiedene K-Automorphismen von F, also F-linear unabhängig. Daher σ Nullstelle von $x^n - 1$, aber nicht Nullstelle eines Polynoms in $K[x]$ mit $\deg < n$. Daher $x^n - 1$ Minimalpolynom von σ als K-lineare Abbildung $F \to F$. Da Grad des Minimalpolynoms von σ gleich n (= Grad des charakteristischen Polynoms) ist das Minimalpolynom gleichzeitig das charakteristische Polynom und σ hat bezüglich einer bestimmten K-Basis von F die Form: Gefährtenmatrix des Minimalpolynoms, dh.

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & & & & 1 \\ -a_0 & & \cdots & & -a_{n-1} \end{pmatrix}$$

Wobei $a_0, \ldots, a_{n-1}$ die Koeffizienten des Minimalpolynoms, speziell $x^n - 1$. Dh. wenn α das erste Basiselement, dann hat die Basis die Form $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^n(\alpha)$. □

6 Minimalpolynom eines linearen Operators / einer Matrix, rationale Normalform

Gegeben n-dimensionaler K-Vektorraum V, $\sigma \in \mathrm{End}_K(V) = \{\varphi : V \to V \mid \varphi\ k\text{-linear}\}$, bezüglich Basis B habe σ die Matrix S. Definieren eine von σ induzierte $K[x]$-Modulstruktur auf V. $f(x)v = f(\sigma)v$ sei die Skalarmultiplikation. Nennen diesen $K[x]$-Modul V_σ.

Lemma 6.1: Für K-Unterraum U von V ist äquivalent

1. U ist invariant unter σ, dh. $\sigma(U) \subseteq U$
2. U ist $K[x]$-Untermodul von V_σ

Beweis. Klar, da $U \leq (V, +)$ sowieso und Abgeschlossenheit bezüglich Skalarmultiplikation mit Elementen aus $K[x]$ heißt Abgeschlossenheit bezüglich Multiplikation mit Konstanten aus K und Anwendung von σ. □

Definition 6.1: Sei R kommutativer Ring. Ein R-Modul M heißt *zyklisch*, wenn er von einem Element erzeugbar ist, dh. $M = Rm$ für ein $m \in M$.

Anmerkung: Wenn $M = Rm$ zyklischer R-Modul, dann $M \simeq R/\mathrm{Ann}_R(m)$, wobei $\mathrm{Ann}_R\, m = \{r \in R \mid rm = 0\} \trianglelefteq R$ via $f : R \to Rm$, $f(r) = rm$ und erstem Isomorphiesatz.

Lemma 6.2: Für einen Teilraum U des K-Vektorraums V ist äquivalent:

1. U ist σ-invarianter Teilraum, der eine σ-zyklische K-Basis hat, dh. eine Basis der Form $v, \sigma v, \sigma^2 v, \ldots, \sigma^{k-1} v$ ($k = \dim U$).
2. U ist ein zyklischer $K[x]$-Untermodul von V_σ.

Bzw genauer, äquivalent ist

1' U ist σ-invarianter Teilraum mit Basis, bezüglich derer $\sigma\big|_U$ eine Matrix der Form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots \\ 0 & 0 & 1 & \cdots & \cdots \\ 0 & 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} \end{pmatrix}$$

2' U zyklischer $K[x]$-Untermodul $U = K[x]v$ mit $\mathrm{Ann}_{K[x]}\, v = f(x)K[x]$ mit $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0$

Beweis.

- $1' \to 2'$: Die ersten $k-1$ Zeilen der Matrix von $\sigma\big|_U$ bedeuten eine Basis der Form $v, \sigma v, \sigma^2 v, \ldots, \sigma^{k-1} v$.
  Letzte Zeile: $\sigma^k v = (a_0 + a_1\sigma + a_2\sigma^2 + \ldots + a_{k-1}\sigma^{k-1})v$. Sei $f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_0$, dann $f(\sigma\big|_U) = 0$ (als lineare Abbildung $U \to U$) und $\sigma\big|_U$ ist nicht Nullstelle eines $g \in K[x]$

mit $\deg g < k = \deg f$ weil $v, \sigma v, \sigma^2 v, \ldots, \sigma^{k-1} v$ K-linear unabhängig und daher $(b_0 + b_1\sigma + \ldots + b_{k-1}\sigma^{k-1} v \neq 0$, für alle $b_0, \ldots, b_{k-1}$ nicht alle 0. Also $\mathrm{Ann}_{K[x]} U = \mathrm{Ann}_{K[x]} v = K[x]f(x)$.

- $2' \to 1'$: $U = K[x]v$ (U zyklischer $K[x]$-Modul) heißt $U = \{g(x)v \mid g(x) \in K[x]\}$, wobei man sich auf $g(x)$ mit $\deg g < \deg f$ beschränken kann, da für $g(x) = g(x)f(x) + r(x)$ gilt, dass $g(\sigma)v = r(\sigma)v$ (da ja $f(\sigma)v = 0$). $U = \{g(\sigma)v \mid g \in K[x], \deg g < k = \deg f\}$ als K-Vektorraum ist U erzeugt von $v, \sigma v, \ldots, \sigma^{k-1} v$ und $v, \sigma v, \ldots, \sigma^{k-1} v$ sind K-linear unabhängig, da $\sigma\big|_U$ kein Polynom von Grad $< k$ erfüllt. Da außerdem $\sigma^k v = (a_{k-1}\sigma^{k-1} + \ldots + a_1\sigma + a_0)v$ hat $\sigma\big|_U$ die Matrix wie in $1'$ (Gefährtenmatrix von f).

$\square$

Da $K[x]$ Euklidischer Ring ist, hat V_σ Darstellung als direkte Summe von zyklischen $K[x]$-Moduln

$$V_\sigma = {}^{K[x]}/_{(m_1)} \oplus \ldots \oplus {}^{K[x]}/_{(m_n)}$$

mit $m_i \in K[x]$, so dass $m_1 \mid m_2 \mid \ldots \mid m_{n-1} \mid m_n$ ($K[x]$ ist endlich erzeugter $K[x]$-Modul, da sogar endlich erzeugter K-Vektorraum; V_σ ist Torsionsmodul, dh. $\forall\, v \in V_\sigma : \exists\, f \neq 0 : f \in \mathrm{Ann}_{K[x]} v$, nämlich ist $\chi_\sigma(x)$ das charakteristische Polynom von σ in $\mathrm{Ann}_{K[x]} v$ für alle $v \in V$). Man bekommt $m_1, \ldots, m_n$, indem man ein Erzeugendensystem von V_σ nimmt, und ein Erzeugendensystem des Kerns des $K[x]$-Modul-Epimorphismus $\varphi : K[x] \times \ldots \times K[x] \to V_\sigma$, $\sigma(e_i) = \rho_i$, zB als Erzeugendensystem eine Basis $v_1, \ldots, v_n$ des K-Vektorraums V und als Relationen

$$xv_i - \sigma v_i = 0$$

Diese Relation mit den Eintragungen der Matrix von σ angeschrieben:

$$xv_i - (s_{i1}v_1 + s_{i2}v_2 + \ldots + s_{in}v_n) = 0$$

Dh. die Zeilen der Relationen-Matrix von $v_1, \ldots, v_n$ also Erzeugendensystem des $K[x]$-Moduls V_σ sind: i-te Zeile:

$$(-s_{i1}, -s_{i2}, \ldots, (x - s_{ii}), -s_{ii+1}, \ldots, -s_{in})$$

Die Relationsmatrix ist also $xI - S = C_\sigma$ (S Matrix von σ bezüglich Basis $v_1, \ldots, v_n$). C_σ durch elementare Zeilen- und Spaltenumformungen (Addition von $f(x)z_i$ zu z_j für $f \in K[x]$ $(i \neq j)$ und analog für Spalten) auf Diagonalform mit Eintragungen $m_1 \mid m_2 \mid \ldots \mid m_n$ bringen. Dann

$$V_\sigma = {}^{K[x]}/_{(m_1)} \times \ldots \times {}^{K[x]}/_{(m_n)}$$

und m_1 erzeugt $\mathrm{Ann}_{K[x]} V_\sigma$, dh.

$$m_1(x)K[x] = \{f(x) \in K[x] \mid f(\sigma) = 0 \text{ als lineare Abbildung } V \to V\}$$

m_1 ist das Minimalpolynom von σ bzw. auch von jeder Matrix von σ bezüglich einer Basis von V.

Aus der Darstellung

$$V_\sigma = {}^{K[x]}/_{(m_1)} \times \ldots \times {}^{K[x]}/_{(m_n)}$$

bekommt man eine Darstellung von V als direkte Summe von σ-zyklischen Teilräumen $V_\sigma = U_1 \times \ldots \times U_n$, so dass $\sigma\big|_{U_i}$ einer Basis der Matrix G_{m_i} (Gefährtenmatrix von m_i, wie in $1'$) hat. Bezüglich einer gemeinsamen Basis von V hat also σ die Matrix

$$R_\sigma = \begin{pmatrix} G_{m_1} & & & \\ & G_{m_2} & & \\ & & \ddots & \\ & & & G_{m_n} \end{pmatrix}$$

Blockdiagonalmatrix mit i-tem Block

$$G_{m_i} = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots \\ 0 & 0 & 1 & \cdots & \cdots \\ 0 & 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{k-1} \end{pmatrix}$$

wenn

$$m_i(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0$$

Diese Matrix R_σ von σ bezüglich einer Basis von V, der Form: Blockdiagonalmatrix mit Blöcken $G_{m_1}, \ldots, G_{m_n}$ (G_{m_i} Gefährtenmatrix von $m_i \in K[x]$) mit $m_1 \mid m_2 \mid \ldots \mid m_n$ heißt *rationale kanonische Form* von σ bzw. der Matrix von σ (Version mit invarianten Faktoren).

Da man $\operatorname{diag}(m_1, \ldots, m_n)$ aus $xI - S$ (S Matrix von σ bezüglich $v_1, \ldots, v_n$) durch elementare Zeilen- und Spaltenumformungen, die an Determinante nichts ändern, bekommt, ist

$$\begin{aligned} \chi_\sigma &= \det(xI - S) = \det(\operatorname{diag}(m_1, \ldots, m_n)) \\ &= m_1(x) \cdot m_2(x) \cdots m_n(x) \end{aligned}$$

Das ist auch die Determinante von $x - R_\sigma$, R_σ die rationale kanonische Form von σ. Das Minimalpolynom eines jeden Blocks G_{m_i} ist jeweils m_i (im Zusammenhang mit dem Satz von McCoy) das Minimalpolynom einer Blockdiagonalmatrix ist das kgV der Minimalpolynome, also ist das Minimalpolynom von R_σ gleich $\operatorname{kgV}(m_1, m_2, \ldots, m_n) = m_n$. R_σ ähnlich zu jeder Matrix von $\sigma \Rightarrow m_1$ Minimalpolynom von σ, $m_1 \cdots m_n$ charakteristisches Polynom von σ.

Offensichtlich haben σ, τ dieselbe rationale Form genau dann, wenn $V_\sigma \simeq V_\tau$ als $K[x]$-Modul (da die invarianten Faktoren eindeutig mit einer Isomorphieklasse von $K[x]$-Modulen korrespondieren).
Lemma 6.3: $\sigma, \tau \in \operatorname{End}_K(V)$, dann $V_\sigma \simeq V_\tau$ (als $K[x]$-Moduln) genau dann, wenn $\exists \varphi \in \operatorname{Aut}_K(V)$: $\sigma = \varphi^{-1} \circ \tau \circ \varphi$

Beweis.

"$\Rightarrow$" $\varphi : V_\sigma \to V_\tau$ $K[x]$-Modul-Isomorphismus, dh. φ bijektiv, $\varphi(v+w) = \varphi(v)+\varphi(w)$, $\varphi(f(x)v) = f(x)\varphi(v)$, dh. $\varphi(f(\sigma)v) = f(\tau)\varphi(v)$, φ K-linear, da insbesondere $\varphi(kv) = k\varphi(v)$ und $\varphi(\sigma v) = \tau\varphi(v)$, also $\sigma = \varphi^{-1}\tau\varphi$.

“$\Leftarrow$” Wenn $\varphi \in \operatorname{Aut}_K V$ mit $\sigma = \varphi^{-1} \circ \tau \circ \varphi$, dann $\forall v \in V_\sigma :\ \varphi(\sigma v) = \tau(\varphi(v))$ und $\forall k \in K :$ $\varphi(kv) = k\varphi(v)$, daher $\forall f \in K[x]\ \varphi(f(\sigma)v) = f(\tau)\varphi(v)$, φ ist $K[x]$-Modul-Homomorphismus $V_\sigma \to V_\tau$, bijektiv nach Voraussetzung, also $K[x]$-Modul-Isomorphismus.

□

Zwei lineare Abbildungen $\sigma, \tau : V \to V$ haben also dieselbe rationale kanonische Form genau dann, wenn $\exists\, \varphi : V \to V$ bijektiv, K-linear, mit $\sigma = \varphi^{-1} \circ \tau \circ \varphi$; analog haben zwei Matrizen $\in M_n(K)$ dieselbe rationale kanonische Form genau dann, wenn sie ähnlich sind.

Damit ist jetzt die Aussage aus dem vorigen Kapitel: $F : K$ endlichdimensionale Galois-Erweiterung mit zyklischer Galoisgruppe $\operatorname{Aut}_K F = \langle \sigma \rangle$, dann hat F eine K-Basis der Form $v, \sigma v, \sigma^2 v, \ldots, \sigma^{n-1} v$ ($n = [F : K]$), weil wir gezeigt haben: Minimalpolynom von σ ist $x^n - 1$ und ist da deg = deg des charakteristischen Polynoms auch gleich dem charakteristischen Polynom χ_σ, daher ist die rationale kanonische Form der Matrix von σ die Gefährtenmatrix von $x^n - 1$, bzw hat F eine σ-zyklische Basis. Insbesondere für Erweiterung von endlichen Körpern $\mathbb{F}_{q^n} : \mathbb{F}_q$ gilt: $\mathbb{F}_{q^n}$ hat $\mathbb{F}_q$-Basis der Form $v, v^q, v^{q^2}, \ldots, v^{q^{n-1}}$ (normale Basis).