Hilfsblatt

Algebra I, Prof. Gabriele Nebe, WS2004/05

Dies ist sowohl eine grobe Zusammenfassung des Vorlesungsinhalts als auch Anleitung zu den wichtigsten Aufgabentypen. Die starke Einschränkung der Seitenränder soll die Seitenzahl minimieren, damit dieses Dokument als Klausurhilfsblatt (je zwei Seiten auf Vorder- und Rückseite eins Blattes) dienen kann. Der Autor[1] erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit seiner Angaben. Kommentare oder Wünsche an Ulrich.Loup@rwth-aachen.de.

Gruppen

- Geg: Präsentation von G bzw. G als freie Gruppe

  Ges: **Isomorphietyp** von G/G' als direktes Produkt zyklischer Gruppen

  Weg:
  1. Bestimme Matrix $A \in \mathbb{Z}^{n\times m}$, n = Anz. Erzeuger von G, m = Anz. Relatoren: Eintrag $a_{i,j}$ von A ergibt sich aus der Summe der Exponenten des i-ten Erzeugers im j-ten Relator (Kommutatoren ergeben 0-Spalten)
  2. A auf Elementarteilergestalt $\bar{A}$ bringen mit $d_i = \bar{a}_{i,i}$ den Elementarteilern
  3. *Dann:* $G/G' \cong \mathbb{Z}^n/_{\mathrm{SR}\ A} \cong \mathbb{Z}^n/_{d_1\mathbb{Z}} \times \cdots \times \mathbb{Z}^n/_{d_k\mathbb{Z}} \cong \mathrm{C}_{d_1} \times \cdots \times \mathrm{C}_{d_k}$ ($\mathbb{Z}/_{(1)}$ kann weggelassen werden.).

  Anw: G unendlich, falls ein $d_i = 0$, da $\mathbb{Z}/_{(0)} \cong \mathbb{Z}$. (Ist G/G' unendlich so auch G unendlich.)

- Geg: Gruppe $G = \langle a_1, \ldots, a_n\rangle$

  Ges: **Präsentation** von G unter Verwendung der Erzeuger $a_1, \ldots, a_n$

  Weg:
  1. Setze $F := \mathrm{Fr}(g_1, \ldots, g_n)$ und $\varphi : F \to G$ vermöge $g_i \mapsto a_i$ für $i = 1, \ldots, n$ und $R := \mathrm{Kern}(\varphi)$.

  $\Rightarrow$ $G \cong F/R$, wobei $R = \mathrm{Kern}(\varphi) = \mathrm{Stab}_F(1_G)$

  2. Berechne Erzeuger $r_1, \ldots, r_k$ von $\mathrm{Stab}_F(1_G)$ unter der treuen Operation (LM) von F auf G vermöge φ.

  $\Rightarrow$ $G \cong \widetilde{G} = \langle g_1, \ldots, g_n \mid r_1, \ldots, r_k\rangle$ ist Präsentation, d.h., $r_1, \ldots, r_k$ sind die Relatoren.

- Geg: Gruppe $G = \langle a_1, \ldots, a_n\rangle$, G-Menge M

  Ges: **base & strong generators**

  Weg:
  1. Wähle treue Operation OP auf M ($\mathcal{S}_n$ auf $[1,n]$ via LM, $\mathrm{GL}_n(K)$ auf K^n via LM, G auf $\mathrm{Z}(G)$ via Konj.)
  2. Wähle $m_i \in M$, welches nicht fix unter OP und bestimme Bahnen $G^{(i-1)}m_i$, wobei $G^{(0)} = G$, $G^{(i)} = \mathrm{Stab}_{G^{(i-1)}}(m_i) = \mathrm{Stab}_G(m_1, \ldots, m_i)$. Dabei sei $w_i(x)$ der Weg von m_i zu $x \in M$ (unter Beachtung der Multiplikations-Reihenfolge). Ist bei OP = LM z.B. $g_j g_{j-1} \cdots g_1\ m_i = x$, so ist $w_i(x) = g_j g_{j-1} \cdots g_1$.
  3. $(m_1, \ldots, m_k)$ heißt *base*. Die $w_i(x)$ für jedes $x \in G^{(i-1)}m_i$ und $i = 1, \ldots, k$ heißen *strong generators*.

  Frg: Ist $g \in G$ (für gegebenes g)?

  Weg: Berechne $g \cdot m_1 =: x_1$, so ist $g \in G \Leftrightarrow w_1(x_1)^{-1}g =: y_1 \in \mathrm{Stab}_G(m_1)$. Berechne weiter $y_1 m_2 =: x_2$ also $y_1 \in \mathrm{Stab}_G(m_1) \Leftrightarrow w_2(x_2)^{-1}y_1 =: y_2 \in \mathrm{Stab}_G(m_1, m_2)$ usw. bis $\mathrm{Stab}_G(m_1, \ldots, m_k) = \{1\}$. Ist für ein x_i das Produkt $y_i x_i \notin \mathrm{Stab}_G(m_1, \ldots, m_i)$ so ist $g \notin G$. Ansonsten stellt sich g dar als $g = w_k(x_k) \cdots w_1(x_1)$.

  Anw:
  - $|G| = \prod_{i=1}^k |G^{(i-1)}m_i|$
  - $|\mathrm{Z}(G)|$: Bestimme $\mathrm{Z}(G) = \mathrm{C}_G(a_1, \ldots, a_n)$ via Bahnenalgorithmus mit OP = Konjugation.

- Geg: **simultane Kongruenzen** $\{x \equiv_{z_i} a_i\}_{i=1}^n$, wobei $z_i \in \mathbb{Z}$ vorgegeben und $a_i \in \mathbb{Z}$ beliebig.

  Ges: alle solche x

  Weg:
  1. Berechne $k := \mathrm{kgV}(z_i)_{i=1}^n = \prod_{j=1}^m p_j$ für p_j p.v. Primzahlen.
  2. Chin. Restsatz liefert $f : \mathbb{Z} \to \mathbb{Z}/_{p_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_m\mathbb{Z}} \cong \mathbb{Z}/_{k\mathbb{Z}}$, $z \mapsto (\bar{z}, \ldots, \bar{z})$ mit $\mathrm{Kern}(f) = k\mathbb{Z}$.
  3. Bestimme Urbilder von $(1,0,\ldots), (0,1,0,\ldots), \ldots, (0,\ldots,1)$ durch XEA:
     (a) Bestimme für alle $i \in [1,m]$ $Z_i := \prod_{j\in[1,m]\setminus\{i\}} p_j$
     (b) Bestimme für alle $i \in [1,m]$ α, β_i mit $1 = \mathrm{ggT}(z_i, Z_i) = \alpha \cdot z_i + \beta_i \cdot Z_i$ mit XEA.

     $\Rightarrow$ (mit $\alpha \cdot z_i \equiv_{z_i} 0$) $\beta_i \cdot Z_i \equiv_{z_i} 1$ also $\beta_i \cdot Z_i$ Urbild von $(\ldots, 0, 1, 0, \ldots)$ (1 an i-ter Stelle) unter f.
  4. $\{x \in \mathbb{Z} \mid \{x \equiv_{z_i} a_i\}_{i=1}^m\} = \sum_{i=1}^m \beta_i Z_i + k\mathbb{Z}$ ist f-Urbild von $a_1 \cdot (1,0,\ldots) + \ldots + a_m \cdot (0,\ldots,1) = (a_1 \ldots, a_m)$.

- Geg: Gruppe G, G-Menge M und Operation OP

  Ges: **Anzahl der Bahnen** von G auf M unter OP

  Weg:
  1. Bestimme für jedes $g \in G$, welches Vertreter einer Konjugiertenklasse ${}^G g$ ist, die Anzahl der Fixpunkte $|fix_M(g)|$ und die Mächtigkeit $|{}^G g|$, erfasse Ergebnis tabellarisch.
  2. Bahnenanzahl ist nach *Burnside* die mittlere Fixpunktzahl (Fixpunkte jeweils $|fix_M(g)| \cdot |{}^G g|$).

  Bsp: Bestimme Anzahl der Bahnen von $\mathcal{S}_n$ auf $[1,m]^{[1,n]} =: A$, $|A| = m^n$.
  1. Vertr. versch. Konj.-klassen haben versch. Zykeltypen: $(n), (n-1,1), (n-2,2), (n-2,1,1) \ldots, (1,\ldots,1)$

  $\Rightarrow$ $P^n := \sum_{i=0}^n P_k^n$ Vertreter (Anz. ungeord. Zahlpart.), z.B. $(n, P^n) \in \{(4,5), (5,7), (6,11), (7,15), (8,22), (9,30)\}$
  2. Für ein $\sigma \in \mathcal{S}_n$ ist $|fix_M(\sigma)| = m^{\mathrm{z}(\sigma)}$ mit $\mathrm{z}(\sigma)$ = Zykelzähler von σ (Anz. Zykel inkl. Einerzykel).

[1] Ulli :)

3. Für ein $\sigma \in \mathcal{S}_n$ ist $|^{\mathcal{S}_n}\sigma| = \{g\sigma g^{-1} \mid g \in \mathcal{S}_n\}$ (Inverse und z.B. (1234) = (4123) beachten). Beispiele: $(\sigma, |^{\mathcal{S}_5}\sigma|) \in \{((12345), 24), ((1234)(5), 30), ((123)(45), 20), ((123)(4)(5), 20), ((12)(34)(5), 15), ((12)(3)(4)(5), 10)\}$ oder $(\sigma, |^{\mathcal{S}_4}\sigma|) \in \{((1234), 6), ((123)(4), 8), ((12)(34), 3), ((12)(3)(4), 6)\}$

- Geg: Gruppe G und Gruppenordnung $|G| =: n$, p^α Primpotenzteiler von n

  Ges: **Anzahl a_p der p-Sylowgruppen** mit $a_p := |\mathrm{Syl}_p(G)|$

  Tip:
  - $a_p \equiv_p 1$ und $a_p \mid |\frac{n}{p^\alpha}|$ und $\bigcap_{P \in \mathrm{Syl}_p(G)} P \trianglelefteq G$.
  - $\mathrm{Syl}_p(G)$ ist transitive G-Menge, liefert nicht-trivialen Gruppenmorphismus $\varphi : G \to \mathcal{S}_{\mathrm{Syl}_p(G)} \cong \mathcal{S}_{|\mathrm{Syl}_p(G)|}$, es ist $\mathrm{Kern}(\varphi) \trianglelefteq G$ und wegen der Nicht-Trivialität von φ $\mathrm{Kern}(\varphi) \neq G$.
  - Ist $a_p = m$ und $\alpha = 1$ folgt (wegen $P \in \mathrm{Syl}_p(G)$ zyklisch) $m \cdot (p-1)$ Elem. der Ord. p in G.

- Geg: Gruppenordnung $|G| =: n < \infty$

  Ges: **Konstruktion aller Gruppen** G bis auf Isomorphie

  Weg:
  1. Bestimme Normalteiler $N \trianglelefteq G$ und Komplemente $U \leq G$ mittels Sylowgruppen, so dass $N \cap U = \{1\}$ und $|N||U| = n \quad \Rightarrow \quad$ *Aussehen* der Gruppe: $G \cong N \rtimes U$
  2. Ist sowohl $N \trianglelefteq G$ als auch $U \trianglelefteq G \quad \Rightarrow \quad G \cong N \times U$, G ist *abelsch*.
  3. Bestimme Bilder der Ordnung $|U|$ unter dem *nicht-trivialen* Morphismus $f : U \to \mathrm{Aut}\ N$, wobei $\alpha \in \mathrm{Aut}\ N$ gegeben durch $\alpha : g \mapsto g^k$ mit $k \in \mathbb{Z}/_{|N|\mathbb{Z}} \setminus \{0\}$.

- Geg: $f(X) \in \mathbb{Z}[X]$, $R := \mathbb{Z}[X]/_{f(X)}$, Primzahl p.

  Ges: Zerlegung von $R/_{(p)}$ in **ringdirektes Produkt von Körpern**, **nichttriviales nilpotentes Element** in $R/_{(p)}$.

  Weg: Es ist $R/_{(p)} \cong \mathbb{Z}/_{(f(X),p)} \cong \mathbb{F}_p[X]/_{(f(X))}$. Zerlege $f(X)$ irreduzible Faktoren $f_1(X), \ldots, f_k(X)$ mit $f(X) = f_1(X) \cdots f_k(X)$. $\Rightarrow \mathbb{F}_p[X]/_{(f(X))} \cong \mathbb{F}_p[X]/_{(f_1(X),\ldots,f_k(X))} \cong \mathbb{F}_p[X]/_{(f_1(X))} \times \cdots \times \mathbb{F}_p[X]/_{(f_k(X))} =: F$. Ist F Ring und $p \mid \mathrm{grad}(f_i(X))$, so ist die Restklasse $f_i(X)$ nilpotentes Element in F und wegen der Isomorphie auch in $R/_{(p)}$.

- **Gruppe G ist auflösbar**
  - $\Leftrightarrow \exists \quad G \trianglelefteq G^{(1)} \trianglelefteq \cdots \trianglelefteq G^{(k)}$ mit abelschen $G^{(i)}, \quad G^{(i)}/_{G^{(i+1)}}$
  - $\Leftrightarrow |G| \in \{p^\alpha, p^2q, p^2q^2 \mid p, q$ Primzahlen mit $p \neq q,\ \alpha \in \mathbb{N}\}$
  - $\Leftrightarrow N \trianglelefteq G$ auflösbar und $G/_N$ auflösbar
  - $\Rightarrow$ alle $U \leq G$ sind auflösbar

- **Gruppe G ist abelsch**
  - $\Leftrightarrow G = \mathrm{Z}(G)$, $\mathrm{Inn}(G) = \{\alpha_g \in \mathrm{Aut}\ G \mid \alpha_g(x) = gxg^{-1}$ Konjugation mit $g\} = \{1\}$
  - $\Leftrightarrow G' = \langle [a,b] \mid a, b \in G \rangle = \{1\}$ (G' char G, $G/_{G'}$ ist abelsch)
  - $\Leftrightarrow xy = yx\ \forall\ x, y \in G$
  - $\Leftrightarrow$ für alle $U \leq G$ gilt $U \trianglelefteq G$
  - $\Rightarrow G$ auflösbar
  - $\Leftarrow G/_{\mathrm{Z}(G)}$ zyklisch

- **Beispiele für Gruppen:**

  $\mathcal{S}_3 = \langle (123), (12) \rangle$, $\mathrm{C}_3 \cong \langle (123) \rangle \trianglelefteq \mathcal{S}_3$

  $\mathcal{S}_4 = \langle (1234), (12) \rangle$, $V_4 \cong \langle (12)(34), (13)(24) \rangle \trianglelefteq \mathcal{S}_4$, $A_4 = \{\pi \in \mathcal{S}_4 \mid \mathrm{sgn}(\pi) = +1\} \trianglelefteq \mathcal{S}_4$, $D_8 \cong \langle (1234), (12)(34) \rangle \leq \mathcal{S}_4$

  $Q_8 \cong \langle (1234)(5678), (1537)(2846) \rangle$ oder $Q_8 \cong \langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$ die Quaternionengruppe

- **Begriffe:** Sei G Gruppe, $U \leq G$:
  - Normalisator: $\mathrm{N}_G(U) = \{g \in G \mid gug^{-1} \in U$ für $u \in U\}$, Zentralisator: $\mathrm{C}_G(x) = \{g \in G \mid gxg^{-1} = x\}$
  - Zentrum: $\mathrm{Z}(G) = \{g \in G \mid gxg^{-1} = x \quad \forall\ x \in G\}$
  - charakteristische Untergruppe: U char $G \ \Leftrightarrow\ \alpha(U) = U \quad \forall \alpha \in \mathrm{Aut}(G) \ \Rightarrow\ U \trianglelefteq G\ (\forall u \in U :\ gug^{-1} \in U\ \forall g \in G)$

Ringe/Körper

- Geg: Körper K, $f(X) \in K[X]$.

  Ges: geeignete **Einbettung der Galoisgruppe** $G := \mathrm{Gal}(E|K) \hookrightarrow \mathcal{S}_n$ für $E := \mathrm{Zerf}_K(f)$ und Erzeuger in $\mathcal{S}_n$

  Weg:
  1. Bestimme Zerfällungskörper $E = \mathrm{Zerf}_K(f)$. (Setze $f^{(0)} = f$, $K_0 := K$, $j := 0$.)
     (a) Zerlege $f^{(j)}$ (mit Eisenstein oder bei $\mathrm{grad}(f^{(j)}) \leq 3$ über Nullstellen) in irreduzible Faktoren $f_i^{(j)}$.
     (b) Falls $f^{(j)} \in K_j[X]$ noch nicht in Linearfaktoren zerfällt, setze $j := j+1$ und gehe zu (c). Sonst $E = K_j$.

(c) Bestimme für ein $f_i^{(j-1)} =: f_i$ Nullstelle α_j (etwa durch die Umstellung $\alpha_j^r = -f_i(\alpha_j) + \alpha_j^r$ für $\mathrm{grad}(f_i) = r$) und adjungiere sie an $K_{j-1} \rightsquigarrow K_j := K_{j-1}(\alpha_j) = K_{j-1}[T_j] \,/_{(f_i(T))}$, d.h., $\alpha_j = \bar{T}$ Restklasse von T.

$\Rightarrow$ $E = \mathrm{Zerf}_K(f)$, $E[X] \ni f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$, wobei hier $\alpha_1, \ldots, \alpha_k$ adjungiert seien.

2. Es ist $\mathrm{Aut}_K(E) = \mathrm{Gal}(E|K) = G$. Ein Automorphismus von $E|K$ hat die Form $\sigma : (\alpha_1, \ldots, \alpha_k) \mapsto (\beta_1, \ldots, \beta_k)$, wobei $(\beta_1, \ldots, \beta_k) \in \{(\alpha_{\pi(1)}, \ldots, \alpha_{\pi(k)}) \mid \pi \in U \leq \mathcal{S}_{\{\alpha_1, \ldots, \alpha_n\}}\}$.
3. Betrachte $G \hookrightarrow U \leq \mathcal{S}_{\{\alpha_1, \ldots, \alpha_n\}} \cong \mathcal{S}_n$, $|G|$ liefert Idee für die Identifikation in $\mathcal{S}_n$. Für $\beta_j \notin \{\alpha_1, \ldots, \alpha_k\}$ muss durch Nachrechnen die Korrektheit der gewählten Erzeuger von U verifiziert werden.

Prb: Verifiziere $|\mathrm{Gal}(E|K)| = [E : K]$ (dann und nur dann heißt $E|K$ galoisch).

Ges: **Erzeuger der echten Zwischenkörper** $K \subset F \subset E$

Weg: Sei $G := \mathrm{Gal}(E|K)$, $\Phi : \mathcal{U}(G) \to \mathcal{T}(E, K)$ inklusionsumkehrende Bijektion mit $\Phi(U) = \mathrm{Fix}_U(E) := \{a \in E \mid g(a) = a \ \forall g \in U\}$ und $\mathrm{S}_{F|K}(a) = \sum_{g \in U} g(a)$ mit $U = \Phi^{-1}(F)$ die Spur von $a \in F \leq E$.

1. Ermittle nicht-triviale Untergruppen $U_i < G$ identifiziert durch Elemente in $\mathcal{S}_n$ ($|\mathcal{U}(G)| =: z$ viele).
2. Die Zwischenkörper sind $F_i = \mathrm{Fix}_{U_i}(E)$ für $i \in [1, z]$. Ermittle Erzeuger via $\mathrm{S}_{F_i|K}(a)$ für jeweils geeignete $a \in E$. Ist $|U_i|$ prim, genügt es, *einen* Erzeuger anzugeben, der nicht in K liegt. Es ist $[G : U_i] = |\mathrm{Gal}(F_i|K)| = [F_i : K]$.

Bem.: Spur ist surjektiv und somit ist für $(b_i)_{i=1}^z$ Basis von $E|K$ $(\mathrm{S}_{F_i|K}(b_1), \ldots, \mathrm{S}_{F_i|K}(b_z))$ Basis von $F_i|K$.

Bem.: Jeder Teilkörper von $\mathbb{F}_{p^n}$ ist isomorph zu $\mathbb{F}_{p^d}$ mit $d \mid n$. Es ist $\mathbb{F}_{p^d} = \mathrm{Fix}_{\langle \mathrm{Frob}^d \rangle}(\mathbb{F}_{p^n})$.

Frg: Welche der echten Zwischnekörper F_i sind galoisch?

Weg: $F_i|K$ ist galoisch $\Leftrightarrow$ $U_i \trianglelefteq \mathrm{Gal}(E|K)$ ist (da dann $\mathrm{Gal}(E|K) \,/_{U_i} \cong \mathrm{Gal}(F_i|K)$ Gruppe).

Ges: **Normalbasis** für einen Zwischenkörper $K \subset L \subset E$.

Weg: Rate $c \in L$ mit $(\sigma_1(c), \ldots, \sigma_k(c))$ mit $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_k\}$.

• Geg: R HIB, $(X \xrightarrow{u} Y)$ als R-Modulhom. repr. durch $(u) \in R^{n \times m}$ mit $X = \bigoplus_{i=1}^n R \,/_{(a_i)}$, $Y = \bigoplus_{j=1}^m R \,/_{(b_j)}$

Ges: $\mathrm{Kern}(u), \mathrm{Bild}(u), \mathrm{Cokern}(u)$ als **direkte Summe zyklischer** R**-Moduln**

Weg: Für $(p) = \mathrm{diag}(a_1, \ldots, a_n)$, $(q) = \mathrm{diag}(b_1, \ldots, b_m)$, $(\hat{u}) = (u)$ lässt sich die Situation wie folgt darstellen:

$$\begin{array}{ccccc} R^n & \xrightarrow{p} & R^n & \xrightarrow{id} & X \\ & & \downarrow{\scriptstyle \hat{u}} & & \downarrow{\scriptstyle u} \\ R^m & \xrightarrow[q]{} & R^m & \xrightarrow[id]{} & Y \end{array}$$

(Beachte im folgenden, dass $R \,/_{(1)} = \{0\}$ weggelassen werden kann und $R \,/_{(0)} \cong R$.)

1. Berechne $\left(\frac{(\hat{u}q)}{(id)}\right) \rightsquigarrow \left(\frac{(\hat{u}q)^*}{(id)^*}\right)$, wobei $\begin{array}{ll} (\hat{u}q)^* & \text{Elementarteilerform von } (\hat{u}q) \\ (id)^* & \text{nur entspr. Spaltenumformungen auf } (id) = \mathrm{E}_{n+m} \end{array}$
2. Seien $u_1, \ldots, u_k$ die Elementarteiler von $(\hat{u}q)$ und $(id)_0^*$ die Spalten unter den 0-Spalten von $(\hat{u}q)^*$

$\Rightarrow$ $\mathbf{Cokern(u)} \cong \mathrm{Cokern}((\hat{u}q)) \cong R \,/_{(u_1)} \oplus \cdots \oplus R \,/_{(u_k)}$.

3. Bezeichne $I := \pi_{R^n}((id)_0^*) = \mathrm{Kern}(u \circ id)$ die Projektion von $(id)_0^*$ auf R^n (d.h. die ersten n Zeilen von $(id)_0^*$).
4. Berechne Elementarteilerform $I^* = \mathrm{diag}(i_1, \ldots, i_s)$.

$\Rightarrow$ (wegen $\mathrm{Bild}(u) \cong R^n \,/_{\mathrm{Kern}(u \circ id)}$) $\mathbf{Bild(u)} \cong \mathrm{Cokern}(R^n \xrightarrow{I^*} R^n) \cong R \,/_{(i_1)} \oplus \cdots \oplus R \,/_{(i_s)}$.

5. Da $p(R^n) \subseteq \mathrm{Kern}(u \circ id)$ ist $(p) = \mathrm{Kern}((u \circ id) \cdot C$. Berechne $R^{n \times n} \ni C = I^{-1} \cdot (p)$ (Rechn. evtl. in $Quot(R)$).
6. Berechne Elementarteilergestalt C^* von C mit $C^* = \mathrm{diag}(c_1, \ldots, c_t)$.

$\Rightarrow$ $\mathbf{Kern(u)} \cong \mathrm{Cokern}(R^n \xrightarrow{C^*} R^n) \cong R \,/_{(c_1)} \oplus \cdots \oplus R \,/_{(c_t)}$.

Prb: Verifiziere $|X| = |\mathrm{Kern}(u)| \cdot |\mathrm{Bild}(u)|$ und $|Y| = |\mathrm{Bild}(u)| \cdot |\mathrm{Cokern}(u)|$.

• Geg: endlicher Körper $K := \mathbb{F}_m$, Zahl $n \in \mathbb{N}$

Ges: ein **irreduzibles Polynom** $f(X)$ vom Grad n in $\mathbb{F}_m[X]$

Weg:
1. Konstruiere $E := \mathbb{F}_{m^n}$ mittels irreduzibler Polynome kleinen (≤ 3) Grades, so dass Nullstellentest möglich.
2. Wähle primitives Element in $a \in E$ und bestimme Minimalpolynom $\mu_{a,K}(X)$ via Koeffizientenmatrix bzgl. einer Basis von $E|K$. Es ist $\mu_{a,K}(X)$ irreduzibel in K mit Grad n.

• Geg: endlicher Körper $K := \mathbb{F}_m$ mit $m = p^e$, Zahl $n \in \mathbb{N}$

Ges: alle **irreduziblen normierten Polynome** $f(X)$ vom Grad $n \leq 3$ in $\mathbb{F}_m[X]$ (Nullstellentest möglich)

Weg: Es ist $\mathrm{Gal}(\mathbb{F}_{p^z}|\mathbb{F}_p) = \langle \mathrm{Frob} \rangle = \{\mathrm{Frob}^0, \ldots, \mathrm{Frob}^{z-1}\}$ mit $\mathrm{Frob}(a) = a^p \ \forall a \in \mathbb{F}_{p^z}$ und $\mathbb{F}_m = \mathbb{F}_p(\alpha_1, \ldots, \alpha_s)$.

1. Bestimme die $\langle \mathrm{Frob} \rangle$-Bahnen aller $a \in \mathbb{F}_m$, d.h. $\langle \mathrm{Frob} \rangle \backslash \mathbb{F}_m$ (alle $\langle \mathrm{Frob} \rangle$-Bahnen in $\mathbb{F}_m$). Sei $|\langle \mathrm{Frob} \rangle \backslash \mathbb{F}_m| =: k$.
2. Ermittle alle möglichen Polynome der Form $f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0$, wobei die Koeffizienten b_i nur jeweils Vertreter einer der $\langle \mathrm{Frob} \rangle$-Bahnen sein müssen. (Ist von diesen Polynomen eines irreduzibel, so auch alle Polynome, deren Koeffizienten in den selben jeweiligen Bahnen liegen.) Systematisch:
   (a) Konstruiere $\mathbb{F}_m$ ggf. via irreduzibler Polynome. (Nicht etwa $\mathbb{F}_m \cong \mathbb{Z} \,/_{m\mathbb{Z}}$.)
   (b) $b_0 = 0$ ist auszuschließen (sonst $\xi = 0$ Nullstelle).

(c) $X^n + b_0$, $b_0 \neq 0$ ist auszuschließen, falls es ein $u \in \mathbb{F}_m$ mit $u^n = b_0$. Sei dies im Folgenden vorausgesetzt.
(d) Best. Polynome $f_1(X), \ldots, f_{(k-1)\cdot(n-1)}(X)$ mit b_{n_1}, b_{n-2} jeweils Vertr. einer $\langle$Frob$\rangle$-Bahn und $b_0 =: \xi_i$.
(e) Bestimme die Wertemenge W_i der $f_i(X) - b_0$ für $i = 1, \ldots, (k-1)\cdot(n-1)$ durch Einsetzen der Basiselemente.
(f) Wähle ξ_i als Vertreter einer $\langle$Frob$\rangle$-Bahn so, dass $\xi_i \notin W_i$, dann ist $f_i(X)$ auch für die gesamte $\langle$Frob$\rangle$-Bahn irreduzibel (sowie für die $\langle$Frob$\rangle$-Bahnen der anderen Koeffizienten).

Prb: Nach Übungsaufgabe 58(2) gibt es $(q^{l^r} - q^{l^{r-1}})l^{-r}$ normierte irreduzible Polynome vom Grad $n = l^r$ in $\mathbb{F}_q[X]$.

- Geg: abelsche Gruppe (bzw. $\mathbb{Z}$-Modul) $\mathbb{Z}/_{(s_1)} \oplus \cdots \oplus \mathbb{Z}/_{(s_n)} =: M$
  Ges: $|\mathbf{End\ M}|$
  Weg: $M \cong F/_T = \mathbb{Z}^n/_{s_1\mathbb{Z}\oplus\cdots\oplus s_n\mathbb{Z}}$ und $End\ M \cong \{\varphi \in End\ F \mid \varphi(T) \subseteq T\}/_{\{\varphi \in End\ F \mid \varphi(F) \subseteq T\}}$, wobei $End\ F \cong \mathbb{Z}^{n\times n}$ und $T = \{(s_1\mathbb{Z}, \ldots, s_n\mathbb{Z})\}$
  1. Wähle $\varphi = A \in End\ F$ mit Einträgen a_{ij}, d.h., $\varphi(x) = A \cdot x$ für $x \in \mathbb{Z}^n$.
  2. Es soll $\varphi(T) \subseteq T$ gelten $\Rightarrow$ löse LGS $A(s_1, \ldots, s_n)^T x = (s_1, \ldots, s_n)^T b$ wie folgt:
     Berechne $\varphi(x_j) =: y_j$ für $j = 1, \ldots, n$, wobei $x_j = (\delta_{1j}s_j, \ldots, \delta_{nj}s_j)^T$ mit δ_{ij} Kroneckersymbol. Ist $y_j \notin T$, d.h., $s_i \nmid s_j a_{ij}$, so muss für diese i ein $c_{ij} \in \mathbb{Z}$ so gewählt werden, dass $s_i \mid c_{ij} \cdot s_j a_{ij}$.
  3. Da $\varphi(F) \subseteq T$ gelten soll, löse $Ax = (s_1, \ldots, s_n)^T b$ mit der Matrix $A = (s_i \cdot a_{ij})_{i=1}^n$.

  $$\Rightarrow End\ M \cong \begin{pmatrix} c_{11}\mathbb{Z} & \ldots & c_{11}\mathbb{Z} \\ \vdots & \ddots & \vdots \\ c_{n1}\mathbb{Z} & \ldots & c_{nn}\mathbb{Z} \end{pmatrix} \Big/ \begin{pmatrix} s_1\mathbb{Z} & \ldots & s_1\mathbb{Z} \\ \vdots & \ddots & \vdots \\ s_n\mathbb{Z} & \ldots & s_n\mathbb{Z} \end{pmatrix} \Rightarrow |End\ M| = \prod_{i,j\in[1,n]} \frac{s_i}{c_{ij}} \in \mathbb{Z}$$

- Geg: symmetrisches Polynom $f(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ mit $f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ für alle $\sigma \in \mathcal{S}_n$
  Ges: $f(X_1, \ldots, X_n)$ geschrieben in den elementarsymmetrischen Polynomen s_i
  Weg: Die s_i ergeben sich zu den symmetrischen Polynomen ersten Grades:
  $s_1 = X_1 + X_2 + \cdots + X_n$, $s_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n$, $\ldots$, $s_3 = X_1X_2\cdots X_n$. Verfahren:
  1. Sortiere das Polynom f lexikographisch (höchste Potenz von X_k mit kleinstem Index k vorne).
  2. Stelle den ersten Summanden mit einer führenden X-Potenz als Produkt $P := \prod c_i s_i^{e_i}$ für entsprechende i (eindeutig!) dar. Berechne Summanden von P, ermittle dazu zuerst die einzelnen $s_i^{e_i}$:
     (a) Ermittle jede mögliche Exponentenkonfiguration in $s_i^{e_i}$, wobei $e = i \cdot e_i$ auf die Exponenten der j X-Potenzen mit $i \leq j \leq n$ zu verteilen ist und keiner der Exponenten $\geq e_i$ werden kann.
     (b) Für die Exponentenkonfiguration $(a_1, \ldots, a_r)$ gibt es $\frac{e!}{(a_1\cdots a_r)!}$ $\mathcal{S}_n$-Bahnen von Summandenkonfigurationen (von diesen braucht nur der erste Summand ausgeschrieben zu werden). Die Länge der $\mathcal{S}_n$-Bahnen liefert die Anzahl der Summanden der Konfiguration. *Probe:* Es muss n^{e_i} Summanden insgesamt geben.
  3. Kürze die entstandene Summe sukzessive (nach jedem aufgelösten $s_i^{e_i}$). Fahre gegebenenfalls bei 1. fort.

- **einige Körperkonstruktionen**
  - Sei $\Phi_n(X) = \dfrac{X^n - 1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d(X)} \in \mathbb{Z}[X]$, $\Phi_1(X) = X - 1$ das n-te Kreisteilungspolynom mit den Eigenschaften
    - $\mathrm{grad}(\Phi_n) = \varphi(n) = n \cdot \prod_{\substack{p|n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right) = |\{m \in [1, n] \mid \mathrm{ggT}(n, m) = 1\}|$
    - $\Phi_n(X) \in \mathbb{Q}[X]$ ist irreduzibel, Nullstellen sind die *primitiven n-ten Einheitswurzeln* ζ_n mit $\zeta_n^n = 1$ und $\Phi_n(X) = \prod_{\substack{m\in[1,n] \\ \mathrm{ggT}(m,n)=1}} (X - \zeta_n^m) \in \mathbb{Q}[\zeta_n][X] \Rightarrow \quad \Phi_n(\zeta_n^m) = 0 \Leftrightarrow \mathrm{ggT}(m, n) = 1$
    - $\Phi_3(X) = X^2 + X + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $\Phi_7(X) = X^6 + \cdots + X + 1$, $\Phi_8(X) = X^4 + 1$

    $\mathbb{Q}[\zeta_n] = \mathrm{Zerf}_{\mathbb{Q}}(\Phi_n)$ ist der n-te *Kreisteilungskörper* und $\mathrm{Gal}(\mathbb{Q}[\zeta_n]|\mathbb{Q}) \cong (\mathbb{Z}/_{n\mathbb{Z}})^*$ vermöge $\zeta_n \mapsto \zeta_n^a$ für $a \in (\mathbb{Z}/_{n\mathbb{Z}})^*$.
  - Es gibt bis auf Isomorphie genau einen Körper K mit $|K| = p^n$, $K := \mathbb{F}_{p^n}$. Es ist $(\mathbb{F}_{p^n})^* \cong \mathrm{C}_{p^n-1}$ zyklisch, Erzeuger von $(\mathbb{F}_{p^n})^*$ heißen *Primitivwurzeln.* Es ist $\mathbb{F}_{p^n}|\mathbb{F}_p$ galoisch und $\langle \mathrm{Frob}_p \rangle = \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) \cong \mathrm{C}_n$. Konstruktion über irreduzible Polynome, z.B.: $\mathbb{F}_8 \cong \mathbb{F}_2[X]/_{X^3+X^2+1} \cong \mathbb{F}_2[X]/_{X^3+X+1}$.

- **Begriffe/Lemmata:** Sei R Ring, $E|K$ Körpererweiterung.
  - *Eisensteinkriterium:* R faktoriell, $K = Quot(R)$, $R[X] \ni f(X) = \sum_{i=0}^n a_i x^i$, $p \in R$ mit $p \nmid a_n$, $p \mid a_i \forall i = 0, \ldots, n-1$ und $p^2 \nmid a_0 \quad \Rightarrow \quad f \in K[X]$ **irreduzibel**.
  - $a \in K$ heißt **separabel**, falls $\mu_{a,K}(X)$ separabel ($E|K$ separabel, falls alle $a \in E$ separabel). Sei $f(X) \in K[X]$. $f(X)$ irreduzibel, $f'(X) \neq 0 \Rightarrow f(X)$ separabel. $f(X)$ separabel $\Leftrightarrow \mathrm{ggT}(f(X), f'(X)) = 1$ mit f' Ableitung von f.
  - $a \in R$ heißt *prim*, falls $(a) \supseteq (x)(y) \Rightarrow (a) \supseteq (x)$ oder $(a) \supseteq (y)$
  - $R^* := \{a \in R \mid \exists a' \in R : aa' = a'a = 1\}$ heißt die *Einheitengruppe* von R, z.B. $\mathbb{Z}^* = \{1, -1\}$
  - $\mathcal{U}(G) = \{U \leq G\}$, $\mathcal{T}(E, K) := \{F \text{ Körper} \mid k \leq F \leq E\}$, $\mathcal{T}(\mathbb{F}_{p^n}, \mathbb{F}_p) := \{\mathbb{F}_{p^m} \mid m \mid n\}$
  - $K[\alpha]$: kleinster *Ring*, der K und α enthält, $K(\alpha) = Quot(K[\alpha])$: kleinster *Körper*, der K und α enthält
  - Ein R-Modul M ist eine Menge, die mit dem Ring eine sinnvolle Linksmultiplikation $\begin{matrix} R \times M & \to & M \\ (r, m) & \mapsto & rm \end{matrix}$ auf sich definieren lässt. ${}_RR$ heißt der *reguläre* R-Modul und die Ideale $I \trianglelefteq {}_RR$ heißen *Linksideale.*