Mathematik Mitschriften: Algebra II

Wintersemester 2003/04 bei Prof. Dr. Wiland Schmale

Nur für den persönlichen Gebrauch

Felix Fontein

14. April 2007

Inhaltsverzeichnis

Kapitel 1

Algebraische Gleichungen in einer Variablen

1.0 Vorbemerkungen

Die Algebra ist ein riesiges Gebiet:

- Gruppentheorie (Lie-Gruppen, allgemeine Gruppentheorie, etc.),
- Ringtheorie,
- Idealtheorie,
- Algebren,
- Körpertheorie (Galoistheorie),
- Garbentheorie,
- (Kategorientheorie, Modelltheorie),
- Homologie-/Kohomologietheorie,
- universelle Algebra,
- multilineare Algebra → Grassmannalgebra,
- Differnentialalgebra,

etc.

- algebraische Geometrie,
- kommutative Algebra,
- (zu diesen beiden gehören auch Gröbnerbasen),
- Zahlentheorie,
- Darstellungstheorie,

etc.

Seid ca. 1975: berechnende Algebra (computational algebra), Computeralgebra, symbolisches Rechnen; wirkt in alle Gebiete rein.

Vorbemerkungen: Algebraische Gleichung in einer Variable:

$$f(t) := \sum_{i=0}^{n} a_i t^i = 0,$$

gesucht ist t.

- $n = 1$: trivial,
- $n = 2$: Schule,
- $n = 3, 4$: → Jacobson, Basic Algebra I,
- $n \geq 5$: ?
- Bis $n = 4$: Lösungstyp $\frac{\sqrt[n_3]{\sqrt[n_1]{q_1} + \sqrt[n_2]{q_2} + \ldots}}{\ldots}$.

Bei der Betrachtung der Gleichung $f(t) = 0$ gibt es zwei Standpunkte:

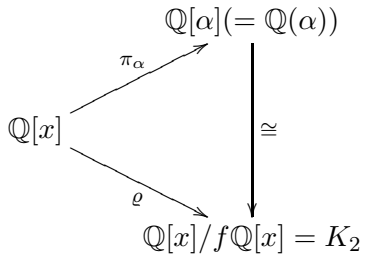
(A) Körper K, $f \in K[x]$. Zeige: Es gibt eine algebraisch abgeschlossene Körpererweiterung $L : K$ (i. A. Mengentheorie, etwa Lang: Algebra). Betrachte dann $K(\alpha_1, \ldots, \alpha_r)$, wobei α_i Nullstellen von f in L sind.

Insbesondere $K(\alpha_1, \ldots, \alpha_r) \subseteq L$. Zum Beispiel $K = \mathbb{Q}$, $L = \mathbb{C}$ oder $L = \mathbb{A}$.

(B) $f \in K[x] \setminus K$ gegeben, f unzerlegbar. Konstruktion eines Zerfällungskörpers L von f über K.

Schritt für Schritt: $K[x]/fK[x] =: K_2$; f hat in K_2 mindestens eine Nullstelle (Kronecker-Konstruktion). Wenn f über K_2 nicht in Linearfaktoren zerfällt, dann $K_2[x]/f_2K_2[x] =: K_2$, wobei f_2 unzerlegbarer Teiler von $f \in K_2[x]$ ist mit Grad größer 1. Ohne Einschränkung sei $K \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq L$.

Beispiel 1.0.0.1. $f = X^6 - 2$, $K = \mathbb{Q}$. f ist über K unzerlegbar nach Eisenstein. $\alpha := \sqrt[6]{2} \in \mathbb{R}$.
$K_2 := \mathbb{Q}[x]/f\mathbb{Q}[x]$, $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$.
Zusammenhang zwischen K_2 und $\mathbb{Q}(\alpha)$:



Es ist $\varrho : g \mapsto g + f\mathbb{Q}[x]$, sowohl ϱ als auch π_α sind surjektiv, und $\ker \varrho = f\mathbb{Q}[x] = \ker \pi_\alpha$, womit K_2 und $\mathbb{Q}(\alpha)$ nach dem Homomorphiesatz isomorph sind.

(A) und (B) vermischen sich oft, insbesondere wenn es um das Rechnen geht.

1.1 Wiederholung, Körpertheorie

Eine Gleichung der Form

$$\sum_{i=0}^{n} a_i t^i = 0$$

heißt *algebraische Gleichung in einer Variablen* t. Dabei sind $a_i \in R$, $0 \leq i \leq n$ und R ein kommutativer Ring mit Eins vorgegeben, und gesucht ist ein Oberring S von R und ein $t \in S$, welches diese Gleichung löst.

1.1.0.0.1 Zusammenhang mit Anwendbarkeit (u. A.)

- klassische Probleme der konstruierenden Geometrie;
- Lösung duch Wurzelziehen (Radikale);
- Existenz allgemeiner Lösungsformeln?
- Theorie endlicher Körper;
- Theorie der Zahlen, Einheitswurzeln;
- theoretische Informatik, Codierung, Kryptographie;
- Computeralgebra, symbolische Analysis, Termvereinfachung.

1.1.1 Einsetzen in Polynome und Nullstellen

Im folgenden sei R ein kommutativer Unterring des Ringes R'.

1.1.1.0.2 Einsetzen in Polynome

Definition 1.1.1.1. *Seien $\alpha \in R'$ und $p \in R[x]$.*

(a) *α heißt* einsetzbar *(in Polynome aus $R[x]$)* $:\Leftrightarrow \forall r \in R : \alpha r = r\alpha$;

(b) *α heißt* Nullstelle *(aus R' von p)* $:\Leftrightarrow \alpha$ *einsetzbar und* $p(\alpha) = 0$.

Beobachtung 1.1.1.2. Wenn α einsetzbar ist, dann ist $\pi_\alpha : R[x] \to R'$ mit $p \mapsto p(\alpha)$ ein Ringhomomorphismus.

Definition 1.1.1.3. *π_α heißt* Einsetzungshomomorphismus. $R[\alpha] := \operatorname{Bild} \pi_\alpha$.

Beobachtungen 1.1.1.4. Es ist $R[\alpha] = \{\sum_{i=0}^{n} a_i \alpha^i \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R\}$ der kleinste Unterring von R', der R und α enthält. $R[\alpha]$ ist als homomorphes Bild von $R[x]$ stets kommutativ. Aufgrund des Homomorphiesatzes gilt

$$R[\alpha] \cong R[x]/\ker \pi_\alpha.$$

Die Struktur von $R[\alpha]$ wird daher weitgehend von $\ker \pi_\alpha$ bestimmt. Ist insbesondere $R = K$ ein *Körper*, dann ist $K[x]$ ein Hauptidealbereich und $\ker \pi_\alpha = pK[x]$ mit einem $p \in K[x] \setminus K$ oder $p = 0$. Der uns hier interessierende Fall ist $p \in K[x] \setminus K$. Für alle $k \in K \setminus \{0\}$ gilt $pK[x] = kpK[x]$. Deswegen werden wir gegebenenfalls ohne Einschränkung annehmen, der höchste Koeffizient von p sei 1.

Definition 1.1.1.5. *Ist $\{0\} \neq \ker \pi_\alpha = pR[x]$, und hat p als höchsten Koeffizienten* 1*, dann heißt p* Minimalpolynom von α. *Man sagt in diesem Fall auch: α besitzt ein Minimalpolynom.*

Beobachtungen 1.1.1.6. Wie schon oben festgestellt, ist $p = 1$ unmöglich für ein Minimalpolynom. Außerdem kann α höchstens *ein* Minimalpolynom besitzen. Besitzt α ein Minimalpolynom p und ist $\deg p = n$, dann ist

$$R[\alpha] = \left\{ \sum_{i=0}^{n-1} r_i \alpha^i \,\middle|\, r_0, \ldots, r_{n-1} \in R \right\}$$

und $1, \alpha, \ldots, \alpha^{n-1}$ sind R-linear unabhängig. Kurz: $R[\alpha]$ ist ein freier R-Modul der Dimension n. Im Allgemeinen ist allerdings nicht garantiert, dass α überhaupt ein Minimalpolynom besitzt. Ist $q \in R[x]$ und $q(\alpha) = 0$, dann ist lediglich gesichert, dass $qR[x] \subset \ker \pi_\alpha$ ist.

Wenn allerdings $R = K$ ein Körper ist, dann ist $\ker \pi_\alpha$ stets ein Hauptideal. Falls dann $\ker \pi_\alpha \neq 0$ ist gibt es ein Polynom $p \neq 0$ mit höchstem Koeffizienten 1 und $\deg p \geq 1$ so, dass $\ker \pi_\alpha = pK[x]$.

Definition 1.1.1.7. *Sei α einsetzbar. Dann heißt α*

(a) algebraisch über $R :\Leftrightarrow \ker \pi_\alpha \neq \{0\}$*;*

(b) transzendent über $R :\Leftrightarrow \ker \pi_\alpha = \{0\}$.

1.1.1.0.3 Nullstellen und lineare Faktoren

Satz 1.1.1.8.

(a) *α Nullstelle aus R' von $p \Leftrightarrow (x - \alpha) \mid p$ in $(R[\alpha])[x]$;*

(b) *R' kommutativer Bereich, $p \neq 0$, dann hat p höchstens $\deg p$ Nullstellen in R'.*

Beispiele 1.1.1.9.

1. $R = \mathbb{Z}$, $R' = \mathbb{Q}$;
2. $R = R' = \mathbb{Z}_6$, $p = x^3 - x$.

Eine wichtige Folgerung aus Satz 8 ist z. B., das nichtlineare unzerlegbare Polynome aus $R[x]$ keine Nullstellen in R besitzen können.

1.1.2 Algebraische Elemente und ihre Konstruktion (Vorüberlegungen)

1.1.2.0.4 Zunächst der Fall $R = \mathbb{Q}$, $R' = \mathbb{C}$ Wegen der Nullteilerfreiheit von $\mathbb{Q}[x]$ genügt es, Nullstellen für unzerlegbare Polynome zu untersuchen.

Sei also $p \in \mathbb{Q}[x]$ unzerlegbar (per Definition ist dann $p \neq 0$ und $\deg p \geq 1$) und $\alpha \in \mathbb{C}$ eine Nullstelle von p. $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/p\mathbb{Q}[x]$ ist dann ein Körper. Bezeichnung in diesem Fall: $\mathbb{Q}(\alpha) := \mathbb{Q}[\alpha]$. Natürlich gilt $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{C}$. $\mathbb{Q}(\alpha)$ ist ein $\mathbb{Q}$-Vektorraum der Dimension $\deg p$.

Die Frage nach Lösungen algebraischer Gleichungen über $\mathbb{Q}$ hängt somit eng zusammen mit dem Studium von Körpern "zwischen" $\mathbb{Q}$ und $\mathbb{C}$ mit endlicher $\mathbb{Q}$-Dimension.

1.1.2.0.5 Allgemeine Konstruktion von Nullstellen bzw. algebraischer Elemente Sei $p \in R[x] \setminus R$, $\deg p = n \geq 1$ und $p = \sum_{i=0}^{n} a_i x^i$ mit $a_n = 1$. Wir betrachten $R[x]/pR[x] =: \overline{R}$ und fassen R als Unterring von $\overline{R}$ auf vermöge der Einbettung $r \mapsto r + pR[x] =: \overline{r}$. Sei $\overline{x} = x + pR[x]$, dann gilt $p(\overline{x}) = \sum_{i=0}^{n} a_i \overline{x}^i = \sum_{i=0}^{n} a_i (x + pR[x])^i = (\sum_{i=0}^{n} a_i x^i) + pR[x] = pR[x] = \overline{0}$.

$\overline{R}$ ist demnach ein Oberring zu R, der eine neue Nullstelle von p enthält, und zwar unabhängig davon, ob R schon Nullstellen von p enthält oder nicht. Da $R \subset \overline{R}$ ist auch $R[x] \subset \overline{R}[x]$, also $p \in \overline{R}[x]$. Mit der gleichen Konstruktion könnte eine weitere Nullstelle von p erzeugt werden und so fort.

Anstelle des Faktorrings $\overline{R}$ können natürlich auch dazu isomorphe Ringe betrachtet werden (Matrizenmodelle, kanonische Modelle).

Beispiel 1.1.2.0A (Matrizenmodell, Spezialfall). $R = \mathbb{C}$, $p = x^2 + 1$, $c = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\mathbb{C}[c] \subset \mathbb{C}^{2\times 2}$.

$R' := \mathbb{C}[c] \cong \mathbb{C}[x]/(x^2+1)\mathbb{C}[x]$. Die Matrix c ist eine weitere Nullstelle von x^2+1 aus R'. p ist schon zerlegbar über $\mathbb{C}$, denn es ist $p = (x+\mathbf{i})(x-\mathbf{i})$ in $\mathbb{C}[x]$. Es ist aber auch $p = (x+c)(x-c) = x^2+1$. Nach Identifizierung von $\mathbb{C}$ mit $\{z + (x^2+1)\mathbb{C}[x] \mid z \in \mathbb{C}\}$ gilt $R = \mathbb{C} \subset R'$.

Betrachte $\pi_c : \mathbb{R}[x] \to R'$ und $\pi_c' : \mathbb{C}[x] \to R'$. Man erhält $\ker \pi_c = (x^2+1)\mathbb{R}[x]$, $\ker \pi_c' = (x^2+1)\mathbb{C}[x]$ und $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ ist ein Körper, während $R' = \mathbb{C}[c]$ Nullteiler enthält: $(\mathbf{i}-c)(\mathbf{i}+c) = 0$.

Beispiel 1.1.2.0B (Kanonisches Modell). Sei $f \in K[x] \setminus K$, $\deg f = n$. $E := \{\sum_{i=0}^{n-1} k_i x^i \mid k_0, \ldots, k_{n-1} \in K\} \subseteq K[x]$. E ist n-dimensionaler K-Vektorraum mit der kanonischen Basis 1, x, …, x^{n-1}.

Definiere für $u, v \in E$: $u \bullet v :=$ Rest von $uv \in K[x]$ bei Division mit $f =: \varrho_f(uv)$.

Behauptung: E ist Ring bzgl. $+$ von $K[x]$ und $\bullet$.

Behauptung: E als Ring ist isomorph zu $K[x]/fK[x]$ mit einem K-linearen Isomorphismus.

Zum Beweis: $\varrho_f : K[x] \to E$, $g \mapsto \varrho_f(g) =$ Rest von g bei Division durch f, $LK(f) = 1$. Nachrechnen: ϱ_f ist K-linearer surjektiver Ringhomomorphismus.

Beachte: $\varrho_f|_E$ ist die identische Abbildung, also insbesondere bijektiv und K-linear.

Übung: Zeige $\varrho_f(gh) = \varrho_f(g) \bullet \varrho_f(h)$.

Vorsicht: In E ist x keine Unbestimmte über K! Denn es gilt in E: $x^n = \varrho_f(x^n) = -\sum_{i=0}^{n-1} a_i x^i$, wenn $f = \sum_{i=0}^{n-1} a_i x^i + x^n$ ist.

Daher besser Umtaufen: $x \to \alpha$.

Beispiel 1.1.2.0C (Matrizenmodell). $f = x^n + \sum_{i=0}^{n-1} a_i x^i$,

$$A := C(f) = \begin{pmatrix} 0 & \cdots & 0 & -a_{n-1} \\ 1 & \ddots & \vdots & \vdots \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -a_0 \end{pmatrix}.$$

Es ist $K[A] \subseteq K^{n\times n}$, wobei $K[A] = \{k_0 E_n + k_1 A + \cdots + k_r A^r \mid r \in \mathbb{N}, k_0, \ldots, k_r \in K\}$. $K[A]$ ist kommutativer Unterring von $K^{n\times n}$.

Behauptung: Es ist $K[A] \cong K[x]/fK[x]$ mit einem K-linearen Isomorphismus.

Beweis. $\pi_A : K[x] \to K[A]$, $g \mapsto g(A)$ Einsetzungshomomorphismus, surjektiv und K-linear, $\ker \pi_A = M_A K[x]$, wobei M_A das zu A gehörende Minimalpolynom ist. Es ist bereits $M_A = P_A$ das charakteristische Polynom von A (warum?), also $\ker \pi_A = P_A K[x] = fK[x]$. □

1.1.3 Algebraische Körpererweiterungen

Sei K ein Unterkörper von K'. K' heißt dann *Körpererweiterung von* K.

Definition 1.1.3.1.

(a) K' *heißt* algebraisch über $K :\Leftrightarrow K'$ *heißt* algebraische Körpererweiterung von $K :\Leftrightarrow \forall \alpha \in K' : \alpha$ *algebraisch über* K.

(b) K' *endliche Körpererweiterung* $:\Leftrightarrow \dim_K K'$ *endlich* $:\Leftrightarrow K'$ *endlich über* K.

Beispiel 1.1.3.2. $\dim_{\mathbb{Q}} \mathbb{R}$ ist nicht endlich!

Schreibweise 1.1.3.3. *Es heißt* $[K' : K] := \dim_K K'$ *der* Grad von K' über K.

Satz 1.1.3.4. *K' endlich über $K \Leftrightarrow K'$ algebraisch über K und $[K' : K]$ endlich.*

Satz 1.1.3.5. *Sei $\alpha \in K'$ algebraisch über K. Dann gilt*

(i) *$\{0\} \neq \ker \pi_\alpha = pK[x]$ mit $p \in K[x]$, $\deg p \geq 1$ und 1 als höchstem Koeffizienten von p. Kurz: α besitzt ein Minimalpolynom p.*

(ii) *Das Minimalpolynom p von α ist unzerlegbar.*

(iii) *$K(\alpha) := K[\alpha]$ ist eine algebraische Körpererweiterung von K.*

(iv) *Es ist $[K(\alpha) : K] = \deg p$.*

Satz 1.1.3.6 (Dimensionsformel). *Sei $K \subset K' \subset K''$ ein Körperturm, dann gilt:*

(a) *$[K'' : K]$ endlich $\Leftrightarrow [K'' : K']$ endlich und $[K' : K]$ endlich;*

(b) *im endlichen Fall gilt $[K'' : K] = [K'' : K'][K' : K]$.*

Satz 1.1.3.7. *Sei K Unterkörper von K' und M eine Teilmenge von K'. Definiere*

$$K[M] := \bigcap \{R \subseteq K' \mid R \text{ Unterring von } K' \text{ mit } K \cup M \subset R\}$$

der kleinste Unterring von K', der K und M enthält.

(1) *Es gilt dann:*

   (a) *$K[M] = \{\sum_{i=1}^{m} k_i \alpha_1^{r_{1,i}} \cdots \alpha_n^{r_{n,i}} \mid n, m \in \mathbb{N}, r_{1,i}, \ldots, r_{n,i} \in \mathbb{N}, \alpha_j \in M, k_i \in K\}$,*
   (b) *und falls $N \subset M$ gilt $(K[M \setminus N])[N] = K[M]$.*

(2) *Sind außerdem alle $\alpha \in M$ algebraisch über K, dann gilt noch:*

   (a) *$K(M) := K[M]$ ist Unterkörper von K';*
   (b) *$K(M)$ ist algebraisch über K;*
   (c) *falls $[K(M) : K]$ endlich ist und N Teilmenge von M, dann gilt $[K(M) : K] = [K(N) : K][K(M) : K(N)]$ und weiterhin $[K(M) : K] \leq [K(M \setminus N) : K][K(N) : K]$.*
   (d) *Es gilt $[K(M) : K]$ endlich $\Leftrightarrow \exists$ endliche Teilmenge $N \subset M : K(M) = K(N)$.*

Satz 1.1.3.8 (Transitivität algebraischer Erweiterungen). *Sei $K \subset K' \subset K''$ ein Körperturm.*

1. *K'' algebraisch über $K \Rightarrow K''$ algebraisch über K' (die Rückrichtung gilt i. A. nicht);*

2. *K'' algebraisch über K' und K' algebraisch über $K \Leftrightarrow K''$ algebraisch über K.*

Beispiel 1.1.3.9. Zu (1): $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

1.1.3.0.6 Relativer algebraischer Abschluss

Definition 1.1.3.10. *Sei K' eine Körpererweiterung von K. Dann heißt $\overline{K}^{K'} := \{\alpha \in K' \mid \alpha$ algebraisch über $K\}$ der* relative algebraische Abschluss von K in K'.

Der relative algebraische Abschluss ist immer ein Körper und damit eine algebraische Körpererweiterung.

Beobachtung 1.1.3.11. $\overline{K}^{K'}$ ist eine algebraische Körpererweiterung von K.

Beweis. Beachte dazu, dass wenn $\alpha, \beta \in K'$ algebraisch über K sind, die endliche Körpererweiterung $K[\alpha, \beta]$ algebraisch ist und somit $\alpha + \beta$, $\alpha\beta$ und α^{-1} falls $\alpha \neq 0$ ebenfalls algebraisch über K sind. □

Beispiel 1.1.3.12. *$K = \mathbb{Q}$, $K' = \mathbb{C}$. $\mathbb{A} := \overline{\mathbb{Q}}^{\mathbb{C}} =:$ Körper der algebraischen Zahlen.*

Satz 1.1.3.13. *$\mathbb{A}$ ist abzählbar.*

Beweis. Es ist $\mathbb{Q}[x]$ abzählbar. Sei zu $f \in \mathbb{Q}[x]$ N_f die Nullstellenmenge von f in $\mathbb{C}$. Dann ist $\mathbb{A} = \bigcup_{f \in \mathbb{Q}[x] \setminus \mathbb{Q}} N_f$ als abzählbare Vereinigung endlicher Mengen wieder abzählbar (Cantorsches Diagonalverfahren). □

1.1.3.0.7 Algebraisch abgeschlossene Körper

Definition 1.1.3.14. *Sei K ein Körper.* K algebraisch abgeschlossen $:\Leftrightarrow$ *In jeder Körpererweiterung K' von K gilt $\overline{K}^{K'} = K$.*

Satz 1.1.3.15. *Sei K' eine Körpererweiterung von K. Ist K' algebraisch abgeschlossen, so auch $\overline{K}^{K'}$.*

Beispiel 1.1.3.16. $K = \mathbb{A}$, $K' = \mathbb{C}$.
Weiterhin ist $\mathbb{A}$ die kleinste algebraisch abgeschlossene Körpererweiterung von $\mathbb{Q}$.

1.1.4 Zerfällungskörper

Definition 1.1.4.1. *Sei K ein Körper und $f \in K[x] \setminus K$.*

(1) *Zunächst sei* 1 *der höchste Koeffizient von f. Eine Körpererweiterung K' von K heißt* Zerfällungskörper von f über K, *wenn gilt $\exists \alpha_1, \ldots, \alpha_n \in K'$, so dass*

   (a) $f = (x - \alpha_1) \cdots (x - \alpha_1) \in K'[x]$ *(insbesondere sind dann die α_i algebraisch über K!),*

   (b) $K' = K(\alpha_1, \ldots, \alpha_n)$.

(2) *Hat f den höchsten Koeffizienten $k \neq 0$, dann heißt K'* Zerfällungskörper von f über K, *wenn K' Zerfällungskörper von $k^{-1}f$ über K ist.*

Beobachtung 1.1.4.2. Zerfällungskörper innerhalb eines umfassenden Körpers sind eindeutig.

Beispiel 1.1.4.3 (Existenz und Eindeutigkeit von Zerfällungskörpern innerhalb $\mathbb{C}$). Seien $f \in \mathbb{Q}[x]$, $\deg f = n \geq 1$, und der höchste Koeffizient von f sei 1. Es gibt dann $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ derart, dass $f = (x - \alpha_1) \cdots (x - \alpha_n)$. $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ ist dann *der* Zerfällungskörper von f über $\mathbb{Q}$ *innerhalb* $\mathbb{C}$.

Satz 1.1.4.4 (Existenz von Zerfällungskörpern). *Zu jedem Körper K und jedem nicht konstanten Polynom $f \in K[x]$ gibt es einen Zerfällungskörper von f über K.*

Satz 1.1.4.5 (Eindeutigkeit von Zerfällungskörpern). *Seien K, K' Körper, $\varphi : K \to K'$ ein Isomorphismus, $f \in K[x]$, $\deg f = n \geq 1$, $\varphi(f) =: f' \in K'[x]$. Dabei wird φ auf $K[x]$ kanonisch fortgesetzt. Sei nun L ein Zerfällungskörper von f über K und L' ein Zerfällungskörper von f' über K'. Dann gibt es einen Isomorphismus $\Phi : L \to L'$ mit $\Phi|_K = \varphi$.*

Zum Beweis von Satz 1.1.4.5 benötigen wir folgenden

Satz 1.1.4.6. *Seien K, K' Körper und $\varphi : K \to K'$ ein Isomorphismus.*

(a) *Der Isomorphismus φ setzt sich auf natürliche Weise fort auf $K[x]$ durch die Fortsetzung*

$$\varphi\left(\sum_{i=0}^{n} a_i x^i\right) := \sum_{i=0}^{n} \varphi(a_i) y^i \in K'[y].$$

(b) *Sei $p \in K[x]$, $p' := \varphi(p) \in K'[y]$. Dann gilt*

$$K \subset K[x]/pK[x] \cong K'[y]/p'K'[y] \supset K'$$

mit einem Isomorphismus, der φ fortsetzt.

1.1.5 Weitere Eigenschaften von Zerfällungskörpern

- Satz 1.1.5.1 befreit die Definition des Zerfällungskörpers von einem willkürlichen Polynom.
- Satz 1.1.5.7 macht die Definition völlig unabhängig von Polynomen.
- Invariante Hülle einer endlichen algebraischen Erweiterung.

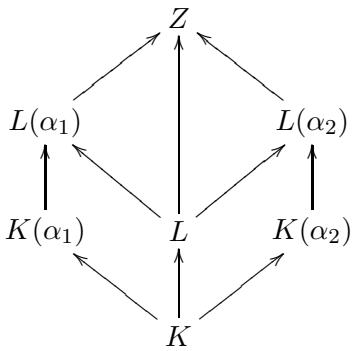
Satz 1.1.5.1. *Sei L eine Körpererweiterung von K. Dann sind die folgenden Aussagen äquivalent:*

(a) *L ist Zerfällungskörper eines Polynoms $f \in K[x] \setminus K$ über K;*

(b) *$[L : K]$ ist endlich und jedes unzerlegbare Polynom $g \in K[x]$ zerfällt über L in ein Produkt gleichgradiger Polynome;*

(c) *$[L : K] < \infty$ und jedes unzerlegbare Polynom $g \in K[x]$, das eine Nullstelle in L besitzt, zerfällt in Linearfaktoren.*

Beweis. **(b) ⇒ (c):** ✓
(c) ⇒ (a): Es ist $[L : K] < \infty$. Es gibt also $\alpha_1, \ldots, \alpha_r \in L$ so, dass $L = K(\alpha_1, \ldots, \alpha_r)$ ist. Die α_i sind algebraisch über K, und seien p_i die Minimalpolynome der α_i über K $(i = 1, \ldots, r)$, und setze $f := \prod_{i=1}^{n} p_i$. Da α_i Nullstelle von p_i ist, zerfällt p_i nach Voraussetzung über L in Linearfaktoren, und damit auch f. Damit ist L Zerfällungskörper von f über K.
(a) ⇒ (b): Sei L Zerfällungskörper von f über K. Seien $p_1, p_2 \in L[x]$ Primteiler des über K unzerlegbaren Polynoms $g \in K[x]$. Sei Z ein Zerfällungskörper von g, und seien α_1, α_2 Nullstellen von p_1, p_2 aus Z. Es ist $K(\alpha_1) \cong K(\alpha_2)$, da g unzerlegbar und damit $K(\alpha_1) \cong K[x]/gK[x] \cong K(\alpha_2)$. Nun ist $L(\alpha_i)$ Zerfällungskörper von f über $K(\alpha_i)$, $i = 1, 2$, und damit folgt mit Satz 1.1.4.5 $L(\alpha_1) \cong L(\alpha_2)$. Nun gilt $[L(\alpha_2) : L][L : K] = [L(\alpha_2) : K] = [L(\alpha_1) : K] = [L(\alpha_1) : L][L : K]$, und da $0 < [L : K] < \infty$ folgt $[L(\alpha_2) : L] = [L(\alpha_1) : L]$. Da weiterhin $\operatorname{grad} p_i = [L(\alpha_i) : L]$ für $i = 1, 2$ folgt die Behauptung.



□

Satz 1.1.5.1 ermöglicht einen Negativ-Test für die Zerfällungskörper-Eigenschaft, wenn eine Primzerlegung über L berechnet werden kann.

Beispiel 1.1.5.2. $f = X^6 - 2 \in \mathbb{Q}[x]$, $\alpha = \sqrt[6]{2}$, eine Primzerlegung ist $f = (X-\alpha)(X+\alpha)(X^2+\alpha X+\alpha^2)(X^2-\alpha X+\alpha^2) \in \mathbb{Q}(\alpha)[x]$. Damit ist $\mathbb{Q}(\alpha)$ kein Zerfällungskörper über $\mathbb{Q}$. Über $\mathbb{Q}(\sqrt{2})$ ist $f = (X^3 + \sqrt{2})(X^3 - \sqrt{2})$ eine Primzerlegung von f. Es ist jedoch $\mathbb{Q}(\sqrt{2})$ Zerfällungskörper von $X^2 - 2$.

Definition 1.1.5.3. *Sei E Körpererweiterung von K und σ ein Automorphismus von E. σ heißt dann* Automorphismus von E über K *oder* K-linearer Automorphismus von E *oder* K-Automorphismus von E, *wenn zusätzlich gilt $\sigma|_K = \mathbf{id}_K$, oder äquivalent σ ist K-linear.*

Beweis. Zur Äquivalenz: $\sigma|_K = \mathbf{id}_K$, dann für $k \in K$, $e \in E$: $\sigma(ke) = \sigma(k)\sigma(e) = k\sigma(e)$. σ K-linear, dann für $k \in K$: $\sigma(k) = \sigma(k \cdot 1) = k\sigma(1) = k$. □

Motivation 1.1.5.4 (für Definition 1.1.5.5). *$K \subseteq L \subseteq E$, σ Automorphismus von E über K, $f \in K[x] \setminus K$, $\alpha \in L$ mit $f(\alpha) = 0$. Es ist $0 = \sigma(f(\alpha)) \underset{f \in K[x]}{=} f(\sigma(\alpha))$. Ist also $N = \{\alpha \in L \mid f(\alpha) = 0\}$, so gilt $\sigma(N) = N$ (die Gleichheit folgt, da N endlich ist), also ist $\sigma|_N$ eine Permutation.*

Sei zusätzlich L Zerfällungskörper von f über K. Dann gilt $\sigma(L) \subseteq L$, und da σ K-linear und $[L : K] = \dim_K L < \infty$ folgt $\sigma(L) = L$.

Definition 1.1.5.5. *Sei L eine Körpererweiterung von K. L heißt* invariant über K, *wenn in allen Erweiterungskörpern E von L und für alle Automorphismen σ von E über K gilt $\sigma(L) \subseteq L$.*

Beobachtung 1.1.5.6.

(a) Sei $[L : K] < \infty$, dann gilt $\sigma(L) \subseteq L \Rightarrow \sigma(L) = L$.

(b) Ist L invariant über K, E Erweiterung von L, σ Automorphismus von E über K, dann gilt $\sigma(L) = L$.

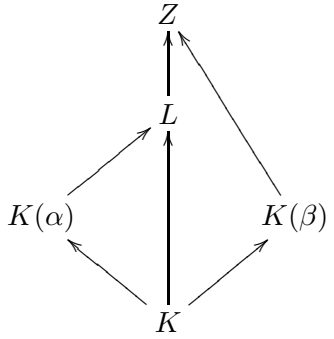
Beweis. (a) ist klar nach der Motivation. Zu (b): Es ist σ^{-1} ebenfalls ein Automorphismus von E über K. Nun gilt $L = \sigma^{-1}(\sigma(L)) \subseteq \sigma^{-1}(L) \subseteq L$. □

Satz 1.1.5.7. *Sei L ein Erweiterungskörper von K. Dann sind äquivalent:*

(a) *Es ist $[L : K] < \infty$, und L ist invariant über K;*

(b) *Der Körper L ist ein Zerfällungskörper von $f \in K[x] \setminus K$ über K.*

Beweis. **(a) ⇒ (b):** Sei L endlich algebraisch über K, etwa $L = K(\alpha_1, \ldots, \alpha_r)$. Die α_i sind algebraisch über K, p_i die Minimalpolynome von α_i über K, $i = 1, \ldots, r$. Setze $f := \prod_{i=1}^{r} p_i$ und sei Z ein Zerfällungskörper von f über L.



Sei $p \in \{p_1, \ldots, p_r\}$, $\alpha \in \{\alpha_1, \ldots, \alpha_r\}$ mit $p(\alpha) = 0$, und sei $\beta \in Z$ mit $p(\beta) = 0$. Es gibt einen Isomorphismus $\varphi : K(\alpha) \to K(\beta)$ mit $\sigma(\alpha) = \beta$ (Vorkenntnis). φ kann auf den Zerfällungskörper von f fortgesetzt werden zu einem Automorphismus Φ von Z. Nach (a) folgt $\Phi(L) \subseteq L$. Da $\Phi(\alpha) = \varphi(\alpha) = \beta$ folgt $\beta \in L$. Da p, α, β beliebig sind, folgt dass L ein Zerfällungskörper von f über K ist.
(b) ⇒ (a): Es gelte $L = K(\alpha_1, \ldots, \alpha_r)$ und $f = \prod_{i=1}^{r}(x - \alpha_i)$ über L. Sei E Erweiterungskörper von L und σ K-Automorphismus von E. Es ist $\sigma(f) = f$, also $\sigma(\alpha_i) \subseteq \{\alpha_1, \ldots, \alpha_r\}$ und damit $\sigma(L) \subseteq L$, da $L = K(\alpha_1, \ldots, \alpha_r)$. □

Beispiel 1.1.5.8. $f = X^6 - 2 \in \mathbb{Q}[x]$, $\alpha = \sqrt[6]{2}$, $\zeta = e^{\frac{2\pi \mathbf{i}}{6}}$, und $N := \{\zeta^i \alpha \mid i = 0, \ldots, 5\}$ sind die Nullstellen von f über $\mathbb{C}$.

(a) $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{C}$, σ komplexe Konjugation, $\sigma|_{\mathbb{Q}(\alpha)} = \mathbf{id}_{\mathbb{Q}(\alpha)}$.

Bemerkung: Jeder Automorphismus von $\mathbb{R}$ läßt $\mathbb{Q}(\alpha)$ invariant.

(b) $\zeta\alpha$ ist Nullstelle von f. $N \subseteq \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(N) =: L$ Zerfällungskörper von f über $\mathbb{Q}$. $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\zeta\alpha)$, aber $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\zeta\alpha)$.

Setze $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\zeta\alpha)$ fort zu Automorphismus Φ von L. Dann gilt $\Phi(\mathbb{Q}(\alpha)) = \mathbb{Q}(\zeta\alpha) \not\subseteq \mathbb{Q}(\alpha)$.

Invariante Hülle:

Definition 1.1.5.9. *Sei $K \subseteq L \subseteq E$ ein Körperturm. E heißt* invariante Hülle *von L über K, wenn gilt*

(i) *E ist invariant über K;*

(ii) *Ist $E' \subseteq E$ Unterkörper, gilt $L \subseteq E'$ und ist E' invariant über K, so folgt $E = E'$.*

Satz 1.1.5.10. *Sei $K \subseteq L$ und $[L : K] < \infty$. Dann gilt*

(a) *Es existiert eine invariante Hülle, diese ist endlich über K.*

(b) *Je zwei invariante Hüllen von L über K sind isomorph.*

(c) *Jede über K invariante Körpererweiterung von L enthält genau eine invariante Hülle von L über K.*

Diese wird mit $\overline{L}^{inv}$ bezeichnet.

(d) *Es ist $\overline{\overline{L}^{inv}}^{inv} = \overline{L}^{inv}$.*

(e) *Ist $K \subseteq L \subseteq L'$ ein Körperturm, dann gilt $\overline{L}^{inv} \subseteq \overline{L'}^{inv}$.*

Beweis. Zur Übung. □

1.1.6 Einfache Körpererweiterungen

Definition 1.1.6.1. *Die Körpererweiterung $L : K$ heißt* einfach über K, *wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$. Wenn α algebraisch über K ist, dann heißt α* primitives Element *von/für L über K.*

Satz 1.1.6.2. *Endliche Körper sind einfach über ihrem Primkörper.*

Beweis. Es ist $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ ist zyklisch (vergleiche Algebra-I-Skript). □

Satz 1.1.6.3 (Steinitz 1871–1921). *Sei L eine Körpererweiterung von K. Dann ist L einfach algebraisch über K genau dann, wenn es zwischen L und K nur endlich viele Zwischenkörper gibt.*

Beweis. **"⇒":** $L = K(\alpha)$, α algebraisch über K. Dann gibt es $f = \mathrm{MiPo}(\alpha, K) \in K[x]$. Setze $\mathscr{Z} := \{Z \text{ Zwischenkörper zwischen } K \text{ und } L\}$. Es gilt insbesondere $K, L \in \mathscr{Z}$. Betrachte $\mu : \mathscr{Z} \to L[x]$, $\mu(Z) = \mathrm{MiPo}(\alpha, Z) =: g_Z$. Dann gilt $g_Z \mid f$ in $Z[x]$ und damit auch in $L[x]$. Also gilt $|\mu(\mathscr{Z})| < \infty$. Wir zeigen nun μ injektiv, woraus folgt $|\mathscr{Z}| = |\mu(\mathscr{Z})| < \infty$.

Gelte $g_{Z_1} = g_{Z_2}$ mit $Z_1, Z_2 \in \mathscr{Z}$. Also $g_{Z_1}, g_{Z_2} \in (Z_1 \cap Z_2)[x]$. Sei $d = \operatorname{grad} g_{Z_1}$. Nun ist g_{Z_1} auch gleich $\mathrm{MiPo}(\alpha, Z_1 \cap Z_2)$, also $g_{Z_1} = g_{Z_1 \cap Z_2} = g_{Z_2}$. Also $[Z_1(\alpha) : Z_1] = [(Z_1 \cap Z_2)(\alpha) : Z_1 \cap Z_2] = [Z_2(\alpha) : Z_2]$, und dann $Z_1 = Z_1 \cap Z_2 = Z_2$, da damit Z_1, Z_2 und $Z_1 \cap Z_2$ Untervektorräume der gleichen endlichen Dimension innerhalb von L sind.

"⇐": Es genügt zu zeigen: zu $\alpha_1, \alpha_2 \in L$ existiert ein $\alpha \in L$ mit $K(\alpha_1, \alpha_2) = K(\alpha)$. Ist dann $L = K(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in L$, so kann dies durch Induktion auf $L = K(\alpha)$ für ein $\alpha \in L$ rezudiert werden. Es sei ohne Einschränkung $|K| = \infty$.

Betrachte die Abbildung $F : K \to \mathscr{Z}$, $k \mapsto K(\alpha_1 + k\alpha_2)$. Da $|K| = \infty$ ist F nicht injektiv. Gelte $K(\alpha_1 + k\alpha_2) = K(\alpha_1 + k'\alpha_2) =: Z$ mit $k, k' \in K$, $k \neq k'$. Also $\alpha_1 + k\alpha_2$, $\alpha_1 + k'\alpha_2 \in Z$, und somit $\alpha_1, \alpha_2 \in Z$. Setze $\alpha := \alpha_1 + k\alpha_2$. Dann gilt also $K(\alpha) = K(\alpha_1, \alpha_2)$. □

Zusammen mit Ergebnissen aus Kapitel II (siehe unten) ergibt der Satz von Steinitz direkt folgenden Satz:

Satz 1.1.6.4 (Satz vom primitiven Element). *Sei $L = K(\alpha_1, \ldots, \alpha_n)$ eine algebraische Erweiterung von K und seien $\alpha_2, \ldots, \alpha_r$* separabel*, d. h. die Minimalpolynome von $\alpha_2, \ldots, \alpha_r$ haben keine mehrfachen Nullstellen in ihren Zerfällungskörpern. Dann ist L einfach über K.*

Beweis. Sei ohne Einschränkung $|K| = \infty$, und weiter $L = K(\alpha, \beta)$ mit β separabel (ansonsten verwende Induktion). Setze $f = \mathrm{MiPo}(\alpha, K)$, $g = \mathrm{MiPo}(\beta, K)$. Sei M ein Zerfällungskörper von fg über K und seien $\alpha = \alpha_1, \ldots, \alpha_r$, $\beta = \beta_1, \ldots, \beta_s$ die Nullstellen von fg.

Ansatz: $\gamma = \alpha + k\beta$, $k \in K$ geeignet zu suchen.

Trick: Substitution: $\tilde{f} = f(-kx + \gamma) \in K(\gamma)[x]$. Gilt dann $\tilde{f}(\beta_i) = 0$ für ein $i > 1$, so muss $0 = \tilde{f}(\beta_i) = f(-k\beta_i + \alpha + k\beta) = f(\alpha + k(\beta - \beta_i))$ sein, also $\alpha + k(\beta - \beta_i) = \alpha_j$ für ein $j \in \{1, \ldots, r\}$. Es gilt also $k = \frac{\alpha_j - \alpha}{\beta - \beta_i}$. Da $|K| = \infty$ kann k so gewählt werden, dass $\tilde{f}$ und g nur die Nullstelle β gemeinsam haben. β ist einfache Nullstelle, da β separabel. $\tilde{f}$, $g \in K(\gamma)[x]$.

Insbesondere folgt: $\mathrm{ggT}(\tilde{f}, g) = x - \beta \in K(\gamma)[x]$. Also $\beta \in K(\gamma)$ und damit auch $\alpha \in K(\gamma)$.

Ergebnis: $K(\alpha, \beta) = K(\gamma)$. □

Siehe auch B. L. van der Waerden.

Für ein Beispiel siehe Aufgabe 7/8.

Folgerung 1.1.6.5. *Jede endliche algebraische Erweiterung eines Körpers der Charakteristik* 0 *(d. h. $k \cdot 1_K = 0 \Leftrightarrow k = 0$ für $k \in \mathbb{Z}$) ist einfach (z. B. über $\mathbb{Q}$).*

Bemerkung 1.1.6.6. Zur Berechnung:

(a) Berechne $\mathrm{MiPo}(\alpha + k\beta, K)$, wenn (im Beispiel $X^6 - 2$) Grad 12, fertig.

(b) Mit diesem Beweis:

Voraussetzung: man kennt die Nullstellen und K ist groß genug: wähle $k \neq \frac{\alpha_j - \alpha}{\beta_i - \beta}$, $1 \leq i \leq s$, $1 \leq j \leq r$. Dann ist $\gamma = \alpha + k\beta$ primitives Element.

1.2 Galoistheorie

Siehe die Vorbemerkungen aus Kapitel 0. Es geht im Groben um die “Feinstruktur” von Zerfällungskörpern.

1.2.1 Die Verbände $\mathscr{Z}$ und $\mathscr{U}$

Die wichtigsten Objekte der Galoistheorie:
Sei L eine Körpererweiterung von K. Setze

$$\begin{aligned}\mathscr{Z} &:= \mathscr{Z}_K(L) := \{Z \mid Z \text{ Unterkörper von } L \text{ und } K \subseteq Z\}\\ &= \{Z \mid Z \text{ Zwischenkörper zwischen } K \text{ und } L\},\\ G &:= \mathrm{Aut}_K(L) := \{\varphi : L \to L \mid \varphi \text{ Automorphismus von } L \text{ über } K\}.\end{aligned}$$

G ist eine Gruppe. Schreibe

$$\mathscr{U} := \mathscr{U}(G) := \mathscr{U}_K(L) := \{U \subset G \mid U \text{ Untergruppe von } G\}.$$

Beobachtung 1.2.1.1.

(a) $\mathscr{U}$, $\mathscr{Z}$ sind geordnet bzgl. $\subseteq$.

(b) $\mathscr{U}$, $\mathscr{Z}$ sind abgeschlossen bzgl. $\cap$ und $\vee$, wobei für Z_1, $Z_2 \in \mathscr{Z}$

$$Z_1 \vee Z_2 := \bigcap\{Z \in \mathscr{Z} \mid Z_1 \cup Z_2 \subseteq Z\}$$

und für U_1, $U_2 \in \mathscr{U}$

$$U_1 \vee U_2 := \bigcap\{U \in \mathscr{U} \mid U_1 \cup U_2 \subseteq U\}.$$

Beweis.

(a) Klar.

(b) $Z_1 \vee Z_2$ ist Körper zwischen L und K, und $U_1 \vee U_2$ ist Gruppe zwischen $\{1\}$ und G.

□

Definition 1.2.1.2. *Eine (partiell) geordnete Menge heißt* Verband, *wenn zu je zwei Elementen ein Supremum und ein Infimum existieren.*

Definition 1.2.1.3. *Ein Verband heißt* vollständig, *wenn zu jeder beliebigen Teilmenge Supremum und Infimum existieren.*

Beobachtung 1.2.1.4. $\mathscr{Z}$ und $\mathscr{U}$ sind vollständige Verbände.

Beweis. Zur Übung. □

Herzstück der Galois-Theorie ist das Wechselspiel zwischen $\mathscr{Z}$ und $\mathscr{U}$. Wie groß sind $\mathscr{Z}$ und $\mathscr{U}$?

Satz 1.2.1.5. *Ist* $[L : K] < \infty$, *dann folgt* $|\mathrm{Aut}_K(L)| < \infty$ *und damit* $|\mathscr{U}_K(L)| < \infty$.

Beweis. Sei $L = K(\alpha_1, \ldots, \alpha_n)$, α_i algebraisch über K, und sei $f_i := \mathrm{MiPo}(\alpha_i, K)$. Setze $N_{f_i} := \{z \in L \mid f_i(z) = 0\}$ (es ist $\alpha_i \in N_{f_i}$), und $G := \mathrm{Aut}_K(L)$. Betrachte die Abbildung

$$\nu : G \to N_{f_1} \times \cdots \times N_{f_n}, \qquad \sigma \mapsto (\sigma(\alpha_1), \ldots, \sigma(\alpha_n)).$$

Dann ist ν injektiv: Sei $\nu(\sigma) = \nu(\tau)$, also $\sigma(\alpha_i) = \tau(\alpha_i)$ für $i = 1, \ldots, n$. Ist $\ell \in L$, $\ell = \sum_{i_1,\ldots,i_n} k_{i_1,\ldots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}$, dann ist $\sigma(\ell) = \sum k_{i_1,\ldots,i_n} \sigma(\alpha_1)^{i_1} \cdots \sigma(\alpha_n)^{i_n} = \sum k_{i_1,\ldots,i_n} \tau(\alpha_1)^{i_1} \cdots \tau(\alpha_n)^{i_n} = \tau(\ell)$, also $\sigma = \tau$.
Daraus folgt $|G| < \infty$. □

Die Endlichkeit von $\mathscr{Z}$ wurde in Abschnitt 1.6 untersucht. Insbesondere über $\mathbb{Q}$: $[L : \mathbb{Q}] < \infty \Rightarrow |\mathscr{Z}| < \infty$.

Beispiel 1.2.1.6. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\alpha = \sqrt{2} + \sqrt{3}$. Es ist $\mathrm{MiPo}(\alpha, \mathbb{Q}) = x^4 - 10x^2 + 1 = (x^2-\alpha^2)(x^2-\tilde{\alpha}^2) = (x-\alpha)(x+\alpha)(x-\tilde{\alpha})(x+\tilde{\alpha})$ mit $\tilde{\alpha} = \sqrt{2}-\sqrt{3}$. $L = \mathbb{Q}(\alpha)$, also ist α primitives Element. Nach dem Satz vom primitiven Element gilt $|\mathscr{Z}| < \infty$. Wieviele Zwischenkörper gibt es aber genau?

Nach dem Beweis vom Steinitz'schen Satzes gilt

$$|\mathscr{Z}_{\mathbb{Q}}(L)| \leq |\{ \text{ normierte Teiler von } f \text{ in } L[x]\}| = 2^4 = 16,$$

aber diese Abschätznung ist noch zu groß. Echte Zwischenkörper haben den Grad 2 über $\mathbb{Q}$; Teiler von f vom Grad 1 oder 3 scheiden also aus. Dies ergibt $|\mathscr{Z}| \leq 8$.

Behauptung: $|\mathscr{Z}| = 5$. Wer findet sie? $\rightarrow$ später: $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Wieviele Automorphismen? $L = \mathbb{Q}(\alpha)$ ist einfach, $\sigma \in G = \mathrm{Aut}_{\mathbb{Q}}(L)$ ist vollständig durch $\sigma(\alpha)$ festgelegt. Möglichkeiten sind $\alpha \mapsto \alpha$, $\alpha \mapsto -\alpha$, $\alpha \mapsto \tilde{\alpha}$, $\alpha \mapsto -\tilde{\alpha}$. Alle vier sind Automorphismen! (Siehe Aufgabe 5.)

Also: $|G| = 4$. Und $|\mathscr{U}| =$? Antwort hierauf erfordert Kenntnisse über die Struktur von G.

Als kleiner Vorgriff auf den Hauptsatz in Abschnitt 2.3:

Satz 1.2.1.7. *Sei $L = K(\alpha)$, α algebraisch über K, $f = \mathrm{MiPo}(\alpha, K)$. Dann ist* $|\mathrm{Aut}_K(L)| = |\{\beta \in L \mid f(\beta) = 0\}|$.

Beweis. Siehe Aufgabe 5. □

Beispiel 1.2.1.8. Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$, $L = \mathbb{Q}(\alpha)$, $\mathrm{MiPo}(\alpha, \mathbb{Q}) = x^3 - 2$. Es ist $\mathrm{Aut}_{\mathbb{Q}}(L) = \{\mathbf{id}_L\}$, da die weiteren Nullstellen aus $\mathbb{C} \setminus \mathbb{Q}(\alpha)$ sind.

1.2.2 Galois-Korrespondenz

(Stichwort "galois connection"; vergleiche [Bir73].)

Zunächst allgemein für Körpererweiterungen, später spezialisieren auf "Galois-Erweiterungen". Sei L ein Erweiterungskörper von K. Wir betrachten die Abbildungen

$$\begin{aligned} \mathrm{Aut} &: \mathscr{Z} \to \mathscr{U}, \qquad Z \mapsto \mathrm{Aut}_Z(L), \\ \mathrm{Fix} &: \mathscr{U} \to \mathscr{Z}, \qquad U \mapsto \mathrm{Fix}_U(L) := \{\alpha \in L \mid \forall \sigma \in U : \sigma(\alpha) = \alpha\} =: \mathrm{Fix}_U\,. \end{aligned}$$

Dabei ist zu klären:

Beobachtung 1.2.2.1.

(a) $Z' := \mathrm{Aut}(Z) \in \mathscr{U}$,

(b) $U' := \mathrm{Fix}(U) \in \mathscr{Z}$.

Beweis.

(a) ✓ per Definition (Z-linear impliziert K-linear).

(b) Seien $a, b \in U'$, $\sigma \in U$. Dann ist $\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$ und $\sigma(ab) = \sigma(a)\sigma(b) = ab$, und falls $a \neq 0$ ist $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$.

□

Mit Galois-Korrespondenz bezeichnet man das Zusammenspiel von $\mathscr{U}$, $\mathscr{Z}$, Fix und Aut.

Beobachtung 1.2.2.2.

(a) Die Abbildungen Aut und Fix sind antiton[1]. Entsprechend sind $\mathrm{Aut} \circ \mathrm{Fix}$ und $\mathrm{Fix} \circ \mathrm{Aut}$ *isoton*[2].

(b) Für alle $U \in \mathscr{U}$, $Z \in \mathscr{Z}$ gilt $U \subseteq U''$ und $Z \subseteq Z''$.

(c) Für alle $U \in \mathscr{U}$, $Z \in \mathscr{Z}$ gilt $U' = U'''$ und $Z' = Z'''$.

(d) Für alle $Z_1, Z_2 \in \mathscr{Z}$ ist $(Z_1 \vee Z_2)' = Z_1' \cap Z_2'$, und für alle $U_1, U_2 \in \mathscr{U}$ ist $(U_1 \vee U_2)' = U_1' \cap U_2'$. Dies gilt im allgemeinen nicht für die "gespiegelten" Aussagen $(A \cap B)' = A' \vee B'$.

Beweis.

(a) Seien $Z_1, Z_2 \in \mathscr{Z}$, und $Z_1 \subseteq Z_2$. Zu zeigen: $Z_2' \subseteq Z_1'$. $\sigma \in Z_2'$ lässt jedes Element von Z_2 fest, also auch jedes von Z_1. Damit $\sigma \in Z_1'$. Analog zeigt man die Behauptung für Untergruppen.

Da weiterhin die Verknüpfung zweier antitoner Abbildungen isoton ist, folgt der zweite Teil der Behauptung.

(b) Sei $\sigma \in U$. Dann hält σ alle Elemente aus U' fest, womit $\sigma \in U''$ gilt. Analog zeigt man $Z \subseteq Z''$.

(c) Es gilt $U \subseteq U''$, $U' \subseteq U'''$. Aus $U \subseteq U''$ folgt $U' \supseteq U'''$, also $U' = U'''$. Analog $Z' = Z'''$.

(d) Seien $Z_1, Z_2 \in \mathscr{Z}$. Es ist $Z_1 \vee Z_2 \supseteq Z_1, Z_2$, und $Z_1', Z_2' \supseteq (Z_1 \vee Z_2)'$. Also gilt $Z_1' \cap Z_2' \supseteq (Z_1 \vee Z_2)'$. Für die andere Richtung sei $\sigma \in Z_1' \cap Z_2'$. Dann hält σ Z_1 und Z_2 fest, und damit auch alle Elemente aus $Z_1 \vee Z_2$, also $\sigma \in (Z_1 \vee Z_2)'$.

□

Wichtig: i. a. sind Aut, Fix nicht surjektiv!

[1] Eine Abbildung $f : A \to B$ zwischen zwei geordneten Mengen A, B ist *antiton* genau dann, wenn für alle $a, b \in A$ gilt $a \leq b \Rightarrow f(b) \leq f(a)$.

[2] Eine Abbildung $f : A \to B$ zwischen zwei geordneten Mengen A, B ist *isoton* genau dann, wenn für alle $a, b \in A$ gilt $a \leq b \Rightarrow f(a) \leq f(b)$.

Beispiel 1.2.2.3.

(a) $r = \sqrt[3]{2}$, $s = \sqrt{2}$, $L = \mathbb{Q}(r,s)$, $[L:\mathbb{Q}] = 6$. $\mathrm{Aut}_{\mathbb{Q}}(L)$ besteht aus zwei Elementen. $\mathbb{Q}' = (\mathbb{Q}(r))'$, also ist Fix nicht injektiv.

(b) Siehe Aufgabe 12.

Galois-Hüllenoperationen in $\mathscr{Z}$ und $\mathscr{U}$:
in $\mathscr{Z}$: $\overline{Z} := Z''$,
in $\mathscr{U}$: $\overline{U} := U''$.
Hülleneigenschaften ergeben sich mit Beobachtung 2:

(i) $Z \subseteq \overline{Z}$;

(ii) $\overline{\overline{Z}} = \overline{Z}$;

(iii) $Z_1 \subseteq Z_2 \Rightarrow \overline{Z_1} \subseteq \overline{Z_2}$.

(Analog mit U.)

Definition 1.2.2.4. *Setze* $\mathscr{Z}' := \{Z' \mid Z \in \mathscr{Z}\}$ *und* $\mathscr{U} := \{U' \mid U \in \mathscr{U}\}$, *und weiter*

$$\overline{\mathscr{Z}} := \{Z \in \mathscr{Z} \mid Z = \overline{Z}\} \qquad \textit{und} \qquad \overline{\mathscr{U}} := \{U \in \mathscr{U} \mid U = \overline{U}\}.$$

Beobachtung 1.2.2.5.

(a) Es ist
$$\overline{\mathscr{Z}} = \mathscr{U}' = \{Z \in \mathscr{Z} \mid Z \text{ abgeschlossen }\} = \{\overline{Z} \mid Z \in \mathscr{Z}\},$$
und
$$\overline{\mathscr{U}} = \mathscr{Z}' = \{U \in \mathscr{U} \mid U \text{ abgeschlossen }\} = \{\overline{U} \mid U \in \mathscr{U}\}.$$

(b) $\overline{\mathscr{Z}}$ und $\overline{\mathscr{U}}$ sind Verbände bezüglich $\subseteq$, $\cap$ und der folgenden Supremums-Konstruktion: Für $Z_1, Z_2 \in \overline{\mathscr{Z}}$ und $U_1, U_2 \in \overline{\mathscr{U}}$ setze

$$Z_1 \sqcup Z_2 := \overline{Z_1 \vee Z_2} \qquad \text{und} \qquad U_1 \sqcup U_2 := \overline{U_1 \vee U_2}.$$

Warnung: Im Allgemeinen sind $\overline{\mathscr{Z}}$, $\overline{\mathscr{U}}$ keine Unterverbände von $\mathscr{Z}$, $\mathscr{U}$.

Bemerkung 1.2.2.6. Die Verbände $\overline{\mathscr{Z}}$, $\overline{\mathscr{U}}$ sind Unterverbände von $\mathscr{Z}$, $\mathscr{U}$ genau dann, wenn gilt

$$Z_1 \vee Z_2 = Z_1 \sqcup Z_2 \qquad \text{und} \qquad U_1 \vee U_2 = U_1 \sqcup U_2$$

für alle $Z_1, Z_2 \in \overline{\mathscr{Z}}$, $U_1, U_2 \in \overline{\mathscr{U}}$.

Betrachtet man nur die "schönen" (d. h. abgeschlossenen) Objekte, so erhält man schöne Zusammenhänge:

Satz 1.2.2.7. *Die Einschränkungen* $\mathrm{Fix}|_{\overline{\mathscr{U}}}$ *und* $\mathrm{Aut}_{\overline{\mathscr{Z}}}$ *sind sich gegenseitig umkehrende Verbandsantiisomorphismen.*

Beweis.

(a) Wir betrachten zuerst $\mathrm{Fix}|_{\overline{\mathscr{U}}}$:

- Injektivität: Seien $U_1, U_2 \in \overline{\mathscr{U}}$, etwa mit $Z_1' = U_1$ und $Z_2' = U_2$. Annahme: $U_1' = U_2'$, also $Z_1'' = U_1' = U_2' = Z_2'' \Rightarrow U_1 = Z_1' = Z_1''' = U_1'' = U_2'' = Z_2''' = Z_2' = U_2$.
- Surjektivität: Sei $Z \in \overline{\mathscr{Z}}$, also $Z = Z''$. Dann gibt es $U \in \mathscr{U}$ mit $U' = Z'' = Z$. Nun $U = Z'$ und damit $U = Z' = Z''' = U''$, also $U = U''$ und damit $U \in \overline{\mathscr{U}}$.

(b) Die Betrachtung von $\mathrm{Aut}|_{\overline{\mathscr{Z}}}$ erfolgt analog zu der von $\mathrm{Fix}|_{\overline{\mathscr{U}}}$.

(c) Der Rest (Umkehren, Antiisomorphie) verbleibt zur Übung.

□

Bemerkung 1.2.2.8 (Schlußbemerkung zu § 2). Uns interessiert die Situation $[L : K] < \infty$, und dort die Zusammenhänge zwischen $\mathscr{Z}, \mathscr{U}$ und $G = \mathrm{Aut}_K(L)$. Wir wissen bereits, dass $|\mathscr{U}| < \infty$ ist. Aber gilt auch $|\mathscr{Z}| < \infty$?

Wir wissen: Ist L einfach, so gilt $|\mathscr{Z}| < \infty$. L ist einfach z. B. wenn $K = \mathbb{Q}$. Galois' Ansatz dazu ist: Studiere G statt L.

Dies wirft neue Fragen auf:

- Was ist mit L, wenn G zyklisch ist?
- Was ist mit L, wenn G kommutativ ist?
- Was ist mit G, wenn L auflösbar ist?
- Wie kann man Normalteiler von G interpretieren, ...?

Definition 1.2.2.9. *Wenn $Z \in \overline{\mathscr{Z}}$ ist, dann heißt L* galois'sch über Z. *Insbesondere ist L Galois'sch über K, wenn $K = \overline{K}$.*

1.2.3 Hauptsatz der Galois-Theorie

Siehe [Kap72], [Art04] oder [Wae03].

Satz 1.2.3.1 (Hauptsatz der Galoistheorie). *Sei L eine Körpererweiterung von K, $G = \mathrm{Aut}_K(L)$, und weiterhin $\mathscr{Z}$, $\mathscr{U}$ wie in § 2, und sei $[L:K] < \infty$ und $K \in \overline{\mathscr{Z}}$, also K abgeschlossen in L bzw. $\overline{K} = K$. Dann gilt:*

(a) *Es ist $\mathscr{Z} = \overline{\mathscr{Z}}$ und $\mathscr{U} = \overline{\mathscr{U}}$.*

(b) *Es sind* Fix *und* Aut *sich gegenseitig umkehrende Antiisomorphismen.*

(c) *Für alle $Z_1, Z_2 \in \mathscr{Z}$ mit $Z_1 \subseteq Z_2$ gilt $[Z_2 : Z_1] = [Z_1' : Z_2'] = |Z_1'/Z_2'|$.*

(d) *Für alle $U_1, U_2 \in \mathscr{U}$ gilt $|U_2/U_1| = [U_2 : U_1] = [U_1' : U_2']$.*
Insbesondere ist $|G| = [L:K]$.

(e) *Ein $U \in \mathscr{U}$ ist genau dann ein Normalteiler in G, wenn K abgeschlossen in U' ist. Analog ist K genau dann abgeschlossen in $Z \in \mathscr{Z}$, wenn Z' ein Normalteiler in G ist.*

(f) *Ist K abgeschlossen in $Z \in \mathscr{Z}$, so gilt $\mathrm{Aut}_K(Z) \cong G/Z'$. Genauer: wir haben eine exakte Sequenz*

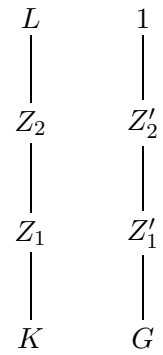
$$0 \longrightarrow Z' \longrightarrow\!\!\!\!\!= \mathrm{Aut}_Z(L) \hookrightarrow \mathrm{Aut}_K(L) \twoheadrightarrow \mathrm{Aut}_K(Z) \longrightarrow 0$$

von Gruppen.

Der Beweis des Hauptsatzes ergibt sich aus den nächsten Sätzen:

Satz 1.2.3.2. *Für alle $Z_1, Z_2 \in \mathscr{Z}$ mit $Z_1 \subseteq Z_2$ und für $n \in \mathbb{N}_{>0}$ gilt $[Z_2 : Z_1] = n \Rightarrow [Z_1' : Z_2'] \leq n$.*

Beweis. Betrachte die Wirkung der Automorphismen auf Z_2. Seien $\sigma, \tau \in G$.



Dann gilt $\sigma|_{Z_2} = \tau|_{Z_2} \Leftrightarrow \tau^{-1}\sigma|_{Z_2} = \mathbf{id}_{Z_2} \Leftrightarrow \tau^{-1}\sigma \in Z_2' \Leftrightarrow \tau^{-1}\sigma Z_2' = Z_2' \Leftrightarrow \sigma Z_2' = \tau Z_2'$.

Zu $\sigma \in G$: Sei $\tilde{\sigma} = \sigma|_{Z_2}$. Sei $(\tilde{\sigma}_i)_{i \in I}$ ein Vertretersystem für die Einschränkungen von Automorphismen auf Z_2.

Ergebnis: Die Anzahl der Nebenklassen von Z_2' in Z_1' ist gleich der Anzahl von verschiedenen Einschränkungen von Automorphismen auf Z_2. Wir brauchen eine Übersicht über die Möglichkeiten, die identische Abbildung von Z_1 fortzusetzen zu einem Monomorphismus[3] von Z_2 in L. Mit Satz 1.2.3.3,(b) folgt die Behauptung: □

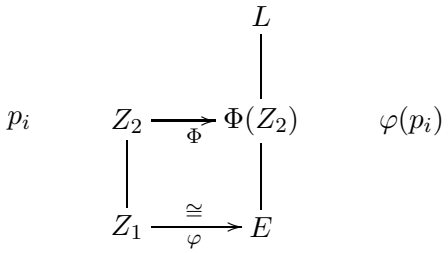
Satz 1.2.3.3 (Fortsetzungshauptsatz). *Sei Z_2 eine Körpererweiterung von Z_1, L Körpererweiterung von E. Es sei weiter $\varphi : Z_1 \to E$ ein Isomorphismus.*

(a) *Sei Z_2 einfach algebraisch über Z_1, etwa $Z_2 = Z_1(\alpha)$, und sei $p = \mathrm{MiPo}(\alpha, Z_1)$. Dann gibt es genauso viele Fortsetzungen von φ zu einem Monomorphismus $\Phi : Z_2 \to L$, wie es verschiedene Nullstellen von $\varphi(p)$ in L gibt, also höchstens* $\operatorname{grad} p$.

[3] Ein Homomorphismus heisst *Monomorphismus*, wenn er injektiv ist.

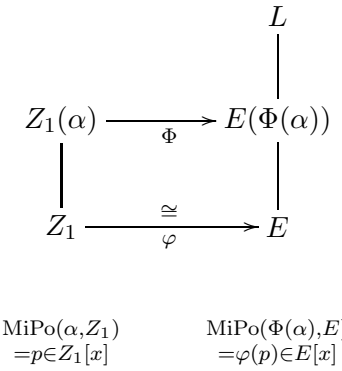
(b) *Sei* $[Z_2 : Z_1] = n$*, etwa* $Z_2 = Z_1(\alpha_1, \ldots, \alpha_r)$ *mit* $p_i = \mathrm{MiPo}(\alpha_i, Z_1) \in Z_1[x]$*,* $i = 1, \ldots, r$*. Dann gibt es höchstens* n *verschiedene Fortsetzungen* $\Phi : Z_2 \to L$ *von* φ*.*

(c) *Enthält* L *einen Zerfällungskörper von* $\varphi(p_1) \cdots \varphi(p_r)$*, und zerfallen die Polynome* $\varphi(p_i)$ *alle in paarweise verschiedene Nullstellen, dann gibt es genau* n *Fortsetzungen.*



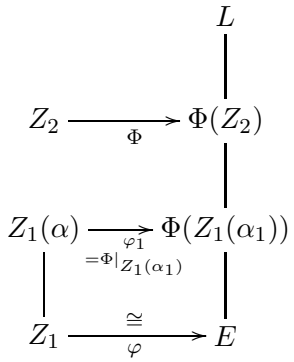
Beweis.

(a) Sei Φ eine Fortsetzung von φ zu einem Isomorphismus $\Phi : Z_1(\alpha) \to E(\Phi(\alpha))$ (bzw. zu einem Monomorphismus $\Phi : Z_1(\alpha) \to L$).



Dann hat $\varphi(p)$ höchstens $\operatorname{grad}\varphi(p) = \operatorname{grad} p$ Nullstellen. Also ist die Anzahl der Möglichkeiten für Φ kleinergleich $\operatorname{grad} p$. Wenn L ein Zerfällungskörper von $\varphi(p)$ über E ist und wenn $\varphi(p)$ in L paarweise verschiedene Nullstellen hat, dann gibt es genau $\operatorname{grad} p$ Fortsetzungen.

(b) Sei etwa $Z_2 = Z_1(\alpha_1, \alpha_2)$.



Ist $p_2 = \mathrm{MiPo}(\alpha_2, Z_1(\alpha_1))$ und $p_1 = \mathrm{MiPo}(\alpha_1, Z_1)$, dann hat jede Fortsetzung von φ auf $Z_1(\alpha_1)$ höchstens (oder gegebenenfalls genau) $\operatorname{grad} p_1$ Fortsetzungen. Insgesamt gibt es also höchstens $\operatorname{grad} p_1 \cdot \operatorname{grad} p_2 = [Z_2 : Z_1]$ Fortsetzungen (oder gegebenenfalls genauso viele).

(c) Folgt aus den Beweisen zu (a) und (b).

□

Satz 1.2.3.4. *Für alle* $U_1, U_2 \in \mathscr{U}$ *mit* $U_1 \subseteq U_2$ *und für* $n \in \mathbb{N}_{>0}$ *gilt*

$$[U_2 : U_1] = n \Rightarrow [U_1' : U_2'] \leq n.$$

Beweis. Da $[U_2 : U_1] = n$ gibt es $\sigma_1, \ldots, \sigma_n \in U_2$ derart, dass U_2 disjunkte Vereinigung der Nebenklassen $\sigma_1 U_1, \ldots, \sigma_n U_1$ ist. Ohne Einschränkung sei $\sigma_1 = 1$. Für alle $\sigma \in U_2$ ist U_2 dann auch disjunkte Vereinigung der Nebenklassen $\sigma\sigma_1 U_1, \ldots, \sigma\sigma_n U_1$. Automorphismen von U_2 aus ein und derselben Nebenklasse haben die gleiche Wirkung auf $F_1 := U_1'$, denn für alle $z \in F_1$ und $\sigma\tau, \sigma\varrho \in \sigma U_1$ gilt $\sigma\tau(z) = \sigma(z)$ und $\sigma\varrho(z) = \sigma(z)$.

Schreiben wir $\tilde{\sigma}$ für die Einschränkung $\sigma|_{F_1}$ von σ auf F_1, so gilt deswegen für alle $\sigma \in U_2$

$$(\widetilde{\sigma\sigma_1}, \ldots, \widetilde{\sigma\sigma_n}) = (\widetilde{\sigma_{i_1}}, \ldots, \widetilde{\sigma_{i_n}}) \tag{1}$$

mit einer von σ abhängigen Permutation $(i_1, \ldots, i_n)$ von $(1, \ldots, n)$. Beachte: Die Abbildungen $\widetilde{\sigma_{i_1}}, \ldots, \widetilde{\sigma_{i_n}}$ sind unter Umständen nicht alle verschieden[4]; dies macht jedoch für den Beweis keinen Unterschied. (Dass die $\widetilde{\sigma\sigma_i}$ eine Permutation der $\widetilde{\sigma_i}$ sind folgt direkt aus der obigen Aussage über die Nebenklassen von U_1.) Nun zeigen wir: Je $n+1$ Elemente $c_1, \ldots, c_{n+1}$ aus F_1 sind linear abhängig über $F_2 := U_2'$, womit die Behauptung $[F_1 : F_2] \leq n$ folgt. Sei dazu

$$A = (\sigma_i(c_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n+1}} \in L^{n \times (n+1)}$$

und $r := \operatorname{rang}_L(A)$. Es ist sicher $r \leq n$. Sei ohne Einschränkung $A \neq 0$ und die ersten r Spalten $a^{(1)}, \ldots, a^{(r)}$ von A L-linear unabhängig. Es gibt dann $\ell_1, \ldots, \ell_r \in L$ derart, dass gilt

$$a^{(r+1)} = \sum_{i=1}^{r} \ell_i a^{(i)}. \tag{2}$$

Durch Anwenden von Automorphismen aus U_2 auf (2) werden wir nun nachweisen, dass die Koeffizienten $\ell_1, \ldots, \ell_r$ in (2) tatsächlich aus F_2 sind. Da $\sigma_1 = 1$ und somit $(c_1, \ldots, c_{n+1})$ die erste Zeile von A ist, folgt dann unmittelbar die lineare Abhängigkeit von $(c_1, \ldots, c_{n+1})$ über F_2.

Sei also $\sigma \in U_2$. Mit (2) erhält man

$$\sigma(a^{(r+1)}) = \sum_{i=1}^{r} \sigma(\ell_i)\sigma(a^{(i)}), \tag{3}$$

wobei σ komponentenweise auf Vektoren und Matrizen angewendet wird. Wegen (1) entsteht σA aus A durch eine Zeilenpermutation. Gelte etwa $\sigma A = PA$ mit einer Permutationsmatrix P. In (3) ergibt sich dann

$$Pa^{(r+1)} = \sum_{i=1}^{r} \sigma(\ell_i) Pa^{(i)}.$$

Darin kann nun P gekürzt werden, so dass gilt

$$a^{(r+1)} = \sum_{i=1}^{r} \sigma(\ell_i) a^{(i)}. \tag{4}$$

Da die $a^{(1)}, \ldots, a^{(r)}$ linear unabhängig über L sind, folgt aus (2) und (4)

$$\sigma(\ell_1) = \ell_1, \ldots, \sigma(\ell_r) = \ell_r,$$

und zwar für alle $\sigma \in U_2$. Da $F_2 = U_2'$ folgt schliesslich $\ell_1, \ldots, \ell_n \in F_2$. □

Satz 1.2.3.4 gilt also ohne Einschränkungen. Er wird für den Hauptsatz in § 3 nur mit abgeschlossenem U_1 benutzt. Wenn U_1 abgeschlossen ist, dann sind im Beweis $\tilde{\sigma_1}, \ldots, \tilde{\sigma_n}$ paarweise verschieden.

Satz 1.2.3.5. *Seien $Z_1, Z_2 \in \mathscr{Z}$, $Z_1 \subseteq Z_2$, und sei $[Z_2 : Z_1] = n < \infty$ und $Z_1 = \overline{Z_1}$, also $Z_1 \in \overline{\mathscr{Z}}$. Dann gilt auch $Z_2 \in \overline{\mathscr{Z}}$ und $[Z_1' : Z_2'] = n$.*

[4] Alternative: (Nach einer Idee von Frau Rull) Nebenklassen von $\overline{U_1} \cap U_2$ betrachten. Dies funktioniert, da wir ja nur Automorphismen aus U_2 betrachten wollen.

Beweis. Es ist

$$n = [Z_2 : Z_1] \leq [Z_2'' : Z_1] = [Z_2'' : Z_1''] \underset{\text{Satz 1.2.3.4}}{\leq} [Z_1' : Z_2'] \underset{\text{Satz 1.2.3.2}}{\leq} [Z_2 : Z_1] = n,$$

also $[Z_1' : Z_2'] = n$ und da $\dim_{Z_1} Z_2 = \dim_{Z_1} \overline{Z_2} < \infty$ und $Z_2 \subseteq \overline{Z_2}$ folgt $Z_2 = \overline{Z_2}$. □

Satz 1.2.3.6. *Seien $U_1, U_2 \in \mathscr{U}$, $U_1 \subseteq U_2$, und sei $[U_2 : U_1] = n < \infty$ und $U_1 = \overline{U_1}$, also $U_1 \in \overline{\mathscr{U}}$. Dann gilt auch $U_2 \in \overline{\mathscr{U}}$ und $[U_1' : U_2'] = n$.*

Beweis. Es ist

$$n = [U_2 : U_1] \leq [U_2'' : U_1] = [U_2'' : U_1''] \underset{\text{Satz 1.2.3.2}}{\leq} [U_1' : U_2'] \underset{\text{Satz 1.2.3.4}}{\leq} [U_2 : U_1] = n,$$

also $[U_1' : U_2'] = n$ und da $[U_2 : U_1] = [\overline{U_2} : U_1] < \infty$ und $U_2 \subseteq \overline{U_2}$ folgt $U_2 = \overline{U_2}$. □

Folgerungen hieraus:

Satz 1.2.3.7. *Spezialfälle der letzten Sätze:*

(a) *Ist $Z \in \mathscr{Z}$, $\overline{K} \subseteq Z$ und $[Z : \overline{K}] < \infty$, so ist $Z \in \overline{\mathscr{Z}}$.*

(b) *Ist $U \in \mathscr{U}$, $[U : \{1\}] < \infty$, dann ist $U \in \overline{\mathscr{U}}$.*

Beweis.

(a) Folgt mit $Z_1 := K$ und $Z_2 := Z$ aus Satz 1.2.3.5.

(b) Folgt mit $\overline{\{1\}} = \{1\}$ aus Satz 1.2.3.6.

□

Die Sätze 1.2.3.2 bis 1.2.3.7 ergeben den Hauptsatz (a) bis (d):

Beweis des Hauptsatzes 1.2.3.1, Teil 1.

(a) folgt aus Satz 1.2.3.7;

(b) folgt mit (a) aus Abschnitt 1.2.1;

(c) folgt aus Satz 1.2.3.5;

(d) folgt aus Satz 1.2.3.6.

□

Beispiel 1.2.3.8.

(a) Sei $K := \mathbb{Q}$, $f := x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1) = (x + \sqrt{2})(x - \sqrt{2})(x + \mathbf{i})(x - \mathbf{i})$, und sei L der Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$, also $L = \mathbb{Q}(\sqrt{2}, \mathbf{i})$. Offensichtlich ist $[L : \mathbb{Q}] = 4$. Behauptet wird nun $\mathscr{Z} = \{\mathbb{Q}, \mathbb{Q}(\mathbf{i}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\mathbf{i}\sqrt{2}), L\}$. Wir bestätigen dies mit Hilfe der Untersuchung der Automorphismengruppe $G := \mathrm{Aut}_{\mathbb{Q}}(L) = \mathrm{Aut}(L)$.

Die Automorphismen der einfachen Erweiterung $\mathbb{Q}(\mathbf{i})$ von $\mathbb{Q}$ sind gegeben durch die Zuordnungen $\mathbf{id} : \mathbf{i} \mapsto \mathbf{i}$ und $\overline{\sigma} : \mathbf{i} \mapsto -\mathbf{i}$.

Die Automorphismen von L über $\mathbb{Q}(\mathbf{i})$ sind gegeben durch die Zuordnungen $\mathbf{id} : \sqrt{2} \mapsto \sqrt{2}$ und $\tau : \sqrt{2} \mapsto -\sqrt{2}$.

Da L Zerfällungskörper über $\mathbb{Q}$, kann $\overline{\sigma}$ fortgesetzt werden durch die Festsetzung $\sigma : \mathbf{i} \mapsto -\mathbf{i}$, $\sqrt{2} \mapsto \sqrt{2}$. Insgesamt haben wir bereits vier Automorphismen:

	$\mathbf{i}$	$-\mathbf{i}$	$\sqrt{2}$	$-\sqrt{2}$
$\mathbf{id}_L$	$\mathbf{i}$	$-\mathbf{i}$	$\sqrt{2}$	$-\sqrt{2}$
σ	$-\mathbf{i}$	$\mathbf{i}$	$\sqrt{2}$	$-\sqrt{2}$
τ	$\mathbf{i}$	$-\mathbf{i}$	$-\sqrt{2}$	$\sqrt{2}$
$\sigma\tau$	$-\mathbf{i}$	$\mathbf{i}$	$-\sqrt{2}$	$\sqrt{2}$

Es ist $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathbf{id}_L$.

Mit Hilfe von Satz 1.2.3.3 erkennt man: $G = \{1, \sigma, \tau, \sigma\tau\}$. Also ist G kommutativ, aber nicht zyklisch. Man sieht leicht $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (bzgl. $+$).

Ist $\mathbb{Q}$ abgeschlossen in $\mathscr{Z}$? Ja, denn nach Satz 1.2.3.5 ist $[L : \overline{\mathbb{Q}}] = [G : 1] = |G| = 4 = [L : \mathbb{Q}]$. Wir werden bald sehen, wie man die Abgeschlossenheit des Grundkörpers direkt an Polynomen ablesen kann.

Teil (a) des Hauptsatzes besagt nun: $\mathscr{Z} = \overline{\mathscr{Z}}$ und $\mathscr{U} = \overline{\mathscr{U}}$, und $\mathscr{Z}$ und $\mathscr{U}$ sind antiisomorph. $\mathscr{U}$ ist aber ganz leicht zu bestimmen:

$$\mathscr{U} = \{\langle 1\rangle, \langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle, G\}.$$

Dabei ist für $g \in G$ mit $\langle g\rangle$ die von g erzeugte zyklische Untergruppe bezeichnet; es ist $\langle g\rangle = \{g^z \mid z \in \mathbb{Z}\}$. Da $|\mathscr{Z}| = |\mathscr{U}|$ besteht $\mathscr{Z}$ tatsächlich genau aus den oben angegebenen Körpern.

(b) Sei $K = \mathbb{Z}_p$, wobei p prim, $[L : K] = n \geq 2$, $G = \mathrm{Aut}_K(L) = \mathrm{Aut}(L)$. Sei φ der Frobenius-Monomorphismus von L; da $|L| < \infty$ ist φ sogar ein Isomorphismus. In diesem Fall ist die Automorphismengruppe G besonders leicht zu bestimmen: es ist $G = \{1, \varphi, \ldots, \varphi^{n-1}\}$.

Dies ergibt sich wie folgt: L ist Zerfällungskörper des Polynoms $x^{p^n} - x$ ohne mehrfache Nullstellen. L besteht demnach genau aus den Nullstellen dieses Polynoms. φ^n ist daher die Identität auf L. $\varphi^r = \mathbf{id}_L$ mit $1 \leq r < n$ ist aber nicht möglich, da dann das Polynom $x^{p^r} - x$ zuviele Nullstellen haben müsste. Es bleibt zu zeigen, dass dies alle Automorphismen von L sind. Sei dazu α ein Generator von L^* und $\psi \in \mathrm{Aut}(L)$. Dann gibt es ein $0 < k < |L|$ mit $\psi(\alpha) = \alpha^k$, und für alle $x \in L$ gilt $\psi(x) = x^k$ (schreibe $x = \alpha^i$ für ein $i \in \mathbb{N}$ und wende die Homomorphismus-Eigenschaften an). Wir zeigen nun, dass k eine Potenz von p ist.

Angenommen $k = p^\ell m$ so, dass m teilerfremd zu k ist. Gilt $m \neq 1$, so betrachte $\psi \circ \varphi^{-\ell} = (x \mapsto x^m)$. Betrachte nun das Polynom $f := (x+1)^m - x^m - 1$; da $x \mapsto x^m$ ein Automorphismus ist muss dieses Polynom jedes Element aus L als Nullstelle haben, und da $m > 1$ ist folgt $f \neq 0$ (betrachte den Koeffizient von x^{m-1}: dieser ist m); also $\deg f \geq |L|$. Dies widerspricht jedoch $\deg f = m \leq k < |L|$.

Wie im Beispiel 25(a) ergibt sich nun auch hier $\mathscr{Z} = \overline{\mathscr{Z}}$ und $\mathscr{U} = \overline{\mathscr{U}}$ und die Antiisomorphie.

An Stelle der Zwischenkörper kann man jetzt genausogut auch die Untergruppen der zyklischen Gruppe G bestimmen. Dies kann in multiplikativer Schreibweise oder in additiver geschehen. Es ist $G \cong (\mathbb{Z}_n, +)$.

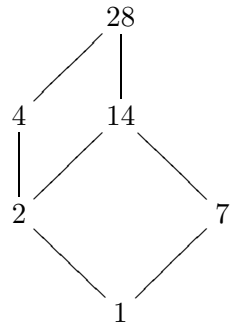
Jede Untergruppe (bzgl. $+$) von $\mathbb{Z}_n$ ist automatisch ein Ideal in $\mathbb{Z}_n$ oder sogar $\mathbb{Z}$-Untermodul. Wenn man also schon einmal alle Ideale in $\mathbb{Z}_n$ bestimmt hat, kann man das hier benutzen. Es ist aber auch nicht besonders schwer, für G in multiplikativer Schreibweise zu zeigen

$$U \text{ Untergruppe von } \langle\varphi\rangle \Leftrightarrow \exists d \in \mathbb{N}_{>0} : U = \left\langle \varphi^d \right\rangle \text{ und } d \mid n.$$

Sei $T_+(n) = \{d \in \mathbb{N}_{>0} \mid d \text{ teilt } n\}$; dann folgt entsprechend $|\mathscr{U}| = |T_+(n)| = |\mathscr{Z}|$.

Außerdem können die Zwischenkörper wie folgt bestimmt werden: $\mathscr{Z} = \{Z(d) \mid d \in T_+(n)\}$ mit $Z(d) = \{\ell \in L \mid \ell^{p^d} = \ell\}$. $Z(d)$ ist ein Körper mit p^d Elementen, denn $[Z(d) : \mathbb{Z}_p] = [G : \langle\varphi^d\rangle] = \frac{|G|}{|\langle\varphi^d\rangle|} = d$. Die 'Lage' der Zwischenkörper zueinander ergibt sich aus der Beziehung $Z(d_1) \subseteq Z(d_2) \Leftrightarrow d_1 \mid d_2$. Sie ergibt sich aus dem Multiplikationssatz für Körperdimensionen. $\mathscr{Z}$ ist demnach isomorph zum Teilerverband der Zahl n.

Für $n = 28$ etwa sieht dieser wie folgt aus:



Definition 1.2.3.9. *Sei $Z \in \mathscr{Z}$. Dann heißt Z G-*invariant *genau dann, wenn für alle $\sigma \in G$ gilt $\sigma Z \subseteq Z$.*

Bemerkung 1.2.3.10.

(a) Für alle $\sigma \in G$ gilt $\sigma Z \subseteq Z \Rightarrow \sigma Z = Z$.

(b) Ist $Z \in \mathscr{Z}$ invariant, so auch insbesondere G-invariant.

Satz 1.2.3.11. *Für alle $Z \in \mathscr{Z}$ und für alle $U \in \mathscr{U}$ gilt:*

(a) (i) *Ist Z G-invariant, so ist Z' Normalteiler in G, in Zeichen $Z' \trianglelefteq G$.*
(ii) *Ist $U \trianglelefteq G$, so ist U' G-invariant.*

(b) (i) *Ist Z G-invariant, so auch $\overline{Z}$.*
(ii) *Ist U Normalteiler, so auch $\overline{U}$.*

(c) *Ist Z G-invariant, so gilt $G|_Z := \{\tau \in \mathrm{Aut}_K(Z) \mid \exists \sigma \in G : \sigma|_Z = \tau\} \cong G/Z'$.*
(Da Z G-invariant ist jede Einschränkung eines Automorphismus aus G auf Z ein Automorphismus von Z über K.)

Beweis.

(a) (i) Sei $\tau \in Z'$ und $\sigma \in G$. Zu zeigen ist $\sigma^{-1}\tau\sigma \in Z'$.
Sei $z \in Z$. Dann ist $(\sigma^{-1}\tau\sigma)(z) = \sigma^{-1}(\tau(\sigma(z)))$, und da $\sigma(z) \in Z$ ist dies gleich $\sigma^{-1}(\sigma(z)) = z$. Damit gilt $\sigma^{-1}\tau\sigma \in Z'$, und da σ, τ beliebig ist Z' Normalteiler in G.
(ii) Sei $z \in U'$ und $\sigma \in G$. Zu zeigen ist $\sigma(z) \in U'$.
Sei $\tau \in U$. Dann is $\sigma^{-1}\tau\sigma \in U$ (da U Normalteiler) und damit $(\sigma^{-1}\tau\sigma)(z) = z$ oder $\tau(\sigma(z)) = \sigma(z)$, also $\sigma(z) \in U'$ da τ beliebig war.

(b) (i) und (ii) folgen durch zweifaches Anwenden von (a).

(c) Betrachte $\varepsilon : G \to G|_Z$, $\sigma \mapsto \sigma|_Z \in \mathrm{Aut}_K(Z)$, da Z G-invariant. Wende den Homomorphie-Satz für Gruppen an: Es ist ε surjektiv per Definition, und ε ist Gruppenhomomorphismus, da für $\sigma, \tau \in G$ gilt $(\sigma \circ \tau)|_Z = \sigma|_Z \circ \tau|_Z$. Weiter ist $\ker \varepsilon = Z'$, da $\sigma|_Z = \mathbf{id}_Z \Leftrightarrow \sigma \in Z'$. Ergebnis: $\sigma(G) = G|_Z \cong G/Z'$.

□

Wir folgern nun weitere Eigenschaften für G-invariante Zwischenkörper.

Satz 1.2.3.12. *Sei $E : K$ eine Körpererweiterung und K abgeschlossen in E. Dann zerfällt jedes unzerlegbare Polynom aus $K[x]$ mit einer Nullstelle in E in paarweise verschiedene Linearfaktoren.*

Beweis. Sei $p \in K[x]$ unzerlegbar, und $\alpha \in E$ mit $p(\alpha) = 0$. Die *G-Bahn* von α in E ist definiert als $B(\alpha) := \{\sigma(\alpha) \mid \sigma \in G\}$. Es gilt $\beta \in B(\alpha) \Rightarrow p(\beta) = 0$. Setze $q := \prod_{\beta \in B(\alpha)}(x - \beta) \in E[x]$. Sei $\sigma \in G$; dann ist $\sigma(q) = \prod_{\beta \in B(\alpha)}(x - \sigma(\beta))$. Da weiter $\sigma(B(\alpha)) = B(\alpha)$ (Beweis zur Übung) ist also $\sigma(q) = q$. Also gilt $q \in \overline{K}[x]$, und da nach Voraussetzung gilt $K = \overline{K}$ folgt also $q \in K[x]$.

Es ist leicht zu zeigen, dass q unzerlegbar ist, und damit $q = \mathrm{MiPo}(\alpha, K)$. Dann folgt die Behauptung. □

Beachte: *Es ist zwangsläufig $p = q$.*

Satz 1.2.3.13. *Sei wieder $G = \mathrm{Aut}_K(L)$.*

(a) *Ist K abgeschlossen in L, dann ist K in allen G-invarianten $Z \in \mathscr{Z}$ abgeschlossen.*

(b) *Ist K abgeschlossen in $Z \in \mathscr{Z}$ und Z algebraisch über K, so ist Z G-invariant.*

Beweis.

(a) Sei $\alpha \in Z \setminus K$. Dann muss es ein $\sigma \in G$ geben mit $\sigma(\alpha) \neq \alpha$ (da $K = \overline{K}^L$). Da Z G-invariant gilt $\sigma(\alpha) \in Z$. Nun ist $\sigma|_Z \in \mathrm{Aut}_K(Z)$, da Z G-invariant. Also gibt es auch in $\mathrm{Aut}_K(Z)$ einen Automorphismus, der α bewegt. Es folgt $\overline{K}^Z = K$.

(b) Sei $\alpha \in Z$ algebraisch über K, und sei $p = \mathrm{MiPo}(\alpha, K)$. Satz 1.2.3.12 besagt: p zerfällt in (paarweise verschiedene) Linearfaktoren über Z. Sei nun $\sigma \in G$, dann gilt also $\sigma(\alpha) \in Z$. Da α, σ beliebig folgt Z G-invariant.

□

Nun ergibt sich der Rest des Hauptsatzes:

Beweis des Hauptsatzes 1.2.3.1, Teil 2. (e) Folgt aus Satz 1.2.3.11(a), Satz 1.2.3.13(a), Satz 1.2.3.13(b).

(f) Folgt aus Satz 1.2.3.13(b), Satz 1.2.3.11(a) und (c). Man erhält zunächst $G/Z' \cong G|_Z \subseteq \mathrm{Aut}_K(Z)$, und es bleibt zu zeigen $G|_Z = \mathrm{Aut}_K(Z)$. Dabei sind L und Z Zerfällungskörper über K. Jeder Automorphismus von Z über K kann dann fortgesetzt werden auf L, und dann gilt auch "=".

□

Definition 1.2.3.14. *Die Körpererweiterung L heißt* (endliche) Galois-Erweiterung von K *oder* (endlich) galois'sch über K, *wenn K abgeschlossen ist in L (und $[L : K] < \infty$).* $\mathrm{Aut}_K(L)$ *heißt dann* Galois-Gruppe *von L über K.*

(Diese abstrakte Definition geht auf Emil Artin zurück.)

Diese Definition ist sehr abstrakt und *ohne* Bezug zu einem konkreten Polynom.
Wir beobachten:

Satz 1.2.3.15. *Endliche Galois-Erweiterungen sind einfach.*

Beweis. Der Hauptsatz besagt $|\mathscr{Z}| < \infty$, und der Satz von Steinitz (Abschnitt 1.1.6, Satz 1.1.6.3) liefert dann die Behauptung. □

Jedoch ist nicht jede einfache Körpererweiterung galois'sch.

Beispiel 1.2.3.16. Ist $\mathbb{Q}(x)$ galois'sch über $\mathbb{Q}$? Ja, denn:

Wir nehmen an, $\overline{\mathbb{Q}} \neq \mathbb{Q}$. Dann wäre nach Aufgabe 12(a) $[\mathbb{Q}(x) : \overline{\mathbb{Q}}] < \infty$. Da $\left|\mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{Q}(x))\right| = \infty$ ergibt sich ein Widerspruch zu Satz 1.2.3.2.

Satz 1.2.3.17. *Es ist L endlich galois'sch über K genau dann, wenn L Zerfällungskörper eines Polynoms aus $K[x]$ ist, dessen unzerlegbare Faktoren paarweise verschiedene Nullstellen haben.*

Beweis. **"⇒":** Klar nach Satz 1.2.3.12.
"⇐": Sei $f = p_1 \cdots p_r$, wobei die p_i paarweise verschiedene Nullstellen haben. Satz 1.2.3.3(c) besagt $[L : K] = |\mathrm{Aut}_K(L)| = |G|$. Satz 1.2.3.2 besagt $|G| = [G : \langle 1 \rangle] \leq [L : \overline{K}]$. Da aber $[L : K] \geq [L : \overline{K}]$ folgt $[L : \overline{K}] = [L : K]$, und da $[L : K] < \infty$ folgt $K = \overline{K}$ und somit ist L galois'sch über K. □

Bemerkung 1.2.3.18. Insbesondere ist jeder Zerfällungskörper über $\mathbb{Q}$ galois'sch, und ebenso über einem endlichen Körper.

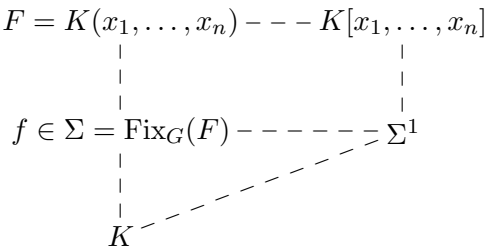
Zusammenhang zur Invarianz:

Satz 1.2.3.19. *Sei L endlich galois'sch über K, und $G = \mathrm{Aut}_K(L)$. Dann sind alle G-invarianten $Z \in \mathscr{Z}$ bereits invariant.*

Beweis. Nach Satz 1.2.3.13 ist Z galois'sch über K. Der Rest ergibt sich aus Abschnitt 1.1.5. □

1.2.4 Symmetrische Polynome

Sei K ein Körper und $x_1, \ldots, x_n$ unabhängige Variablen (Unbestimmte über K), d. h. $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_{\geq 0}^n\}$ ist K-Basis von $K[x_1, \ldots, x_n]$. Sei $F = K(x_1, \ldots, x_n)$ und S_n die Gruppe der Permutationen von $\{1, \ldots, n\}$. Jede Permutation $\pi \in S_n$ führt zu einem Automorphismus von F über K: Die Abbildung $\pi \mapsto \varphi_\pi \in \mathrm{Aut}_K(F)$ ist injektiver Gruppenhomomorphismus. Das Bild ist $G := \{\varphi_\pi \mid \pi \in S_n\}$. (Es ist $G \cong S_n$.)



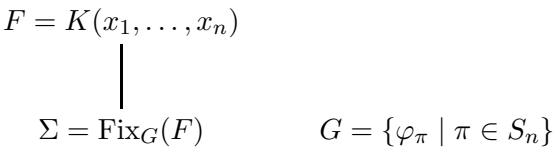
Sei $\Sigma := \mathrm{Fix}_G(F) = G'$ und $\Sigma^1 := \Sigma \cap K[x_1, \ldots, x_n]$.

Definition 1.2.4.1. *Es heißt* Σ *der* Körper der symmetrischen Funktionen *und* Σ^1 *der* Ring der symmetrischen Polynome.

Beispiele 1.2.4.2. Die Polynome $s_1^{(n)} = \sum_{i=1}^n x_i$, $s_2^{(n)} = \sum_{1 \leq i < j \leq n} x_i x_j$, und allgemein $s_r^{(n)} := \sum_{1 \leq i_1 < \cdots < i_r \leq n} x_{i_1} \cdots x_{i_r}$ sind symmetrisch.

Definition 1.2.4.3. *Die Polynome* s_r *für* $r \in \mathbb{N}_{>0}$ *heissen* elementare symmetrische Polynome.

Sei $f = \prod_{i=1}^n (x - x_i) \in F[x]$, $F = K(x_1, \ldots, x_n)$ wie oben.



Nun hat f per Definition paarweise verschiedene Nullstellen, und weiterhin ist es unzerlegbar über $\Sigma = \mathrm{Fix}_G(F)$; einmal ist es über Σ definiert, da $\sigma(f) = f$ für alle $\sigma \in G$ gilt, und weiterhin gilt $B(x_1) = \{\sigma(x_1) \mid \sigma \in G\} = \{x_1, \ldots, x_n\}$, womit mittels Übungsaufgabe 13(c) die Unzerlegbarkeit folgt.

Beobachtung 1.2.4.4 (Vietasche Wurzelsätze). Sei $f = \prod_{i=1}^n (x - x_i) \in F[x]$. Dann ist

$$f = x^n - s_1^{(n)} x^{n-1} \pm \cdots + (-1)^n s_n^{(n)} = \sum_{k=0}^{n} s_k^{(n)} (-1)^k x^{n-k}$$

mit $s_0 := 1$, wobei x_i die Nullstellen von f sind.

Beweis. Beweis durch vollständige Induktion nach n.
Anfang: Es ist $s_1^{(1)} = x_1$ und damit $f = x - x_1$, ✓
Voraussetzung: Die Behauptung gelte für ein $n \in \mathbb{N}$.

Schluß: Es ist

$$\begin{aligned} f &= \left(\prod_{i=1}^{n}(x-x_i)\right)(x-x_{n+1}) \overset{\text{I.V.}}{=} \left(\sum_{k=0}^{n} s_k^{(n)}(-1)^k x^{n-k}\right)(x-x_{n+1}) \\ &= \sum_{k=0}^{n} s_k^{(n)}(-1)^k x^{n+1-k} - \sum_{k=0}^{n} s_k^{(n)} x_{n+1}(-1)^k x^{n-k} \\ &= x^{n+1} + \sum_{k=1}^{n} s_k^{(n)}(-1)^k x^{n+1-k} - \sum_{k=1}^{n} s_{k-1}^{(n)} x_{n+1}(-1)^{k-1} x^{n+1-k} - s_n^{(n)} x_{n+1}(-1)^n \\ &= x^{n+1} + \sum_{k=1}^{n}(-1)^k [s_k^{(n)} + s_{k-1}^{(n)} x_{n+1}] x^{n+1-k} + s_{n+1}^{(n+1)}(-1)^{n+1} \\ &= x^{n+1} + \sum_{k=1}^{n}(-1)^k s_k^{(n+1)} x^{n+1-k} + s_{n+1}^{(n+1)}(-1)^{n+1} = \sum_{k=0}^{n+1}(-1)^k s_k^{(n+1)} x^{n+1-k}, \end{aligned}$$

was zu zeigen war. □

Folgerung 1.2.4.5. *Es sind $s_1, \ldots, s_n \in \Sigma_1$!*

Beispiel 1.2.4.6. Es ist $t_1 = s_1$, $t_2 = x_1^2 + \cdots + x_n^2$, $t_3 = x_1^3 + \cdots + x_n^3$, $\ldots$, $t_n = x_1^n + \ldots x_n^n \in \Sigma_1$.
Die Umrechnungen zwischen s und t werden als Newton-Identitäten bezeichnet.

Satz 1.2.4.7 (Hauptsatz über symmetrische Polynome).

(a) *Es ist F ein Zerfällungskörper von f über Σ und somit galoissch über Σ, und weiterhin ist $\Sigma = K(s_1, \ldots, s_n)$. Das Polynom f ist hierbei wieder gegeben durch*

$$f = \prod_{i=1}^{n}(x - x_i) \in K[x_1, \ldots, x_n][x].$$

Die Galoisgruppe ist isomorph zu S_n.

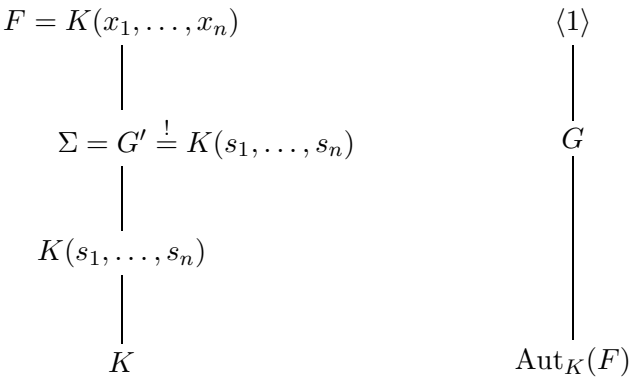
(b) *Die Polynome $s_1, \ldots, s_n$ sind algebraisch unabhängig über K, und die $s_1, \ldots, s_n$ bilden eine Transzendenzbasis von F.*

(c) *Es ist $\Sigma_1 = K[s_1, \ldots, s_n]$.*

(d) *Zu jedem symmetrischen Polynom $f \in K[x_1, \ldots, x_n]$ gibt es genau ein Polynom $h \in K[y_1, \ldots, y_n]$ mit $f = h(s_1, \ldots, s_n)$.*

Beweis.

(a) Betrachte die Diagramme



Nun ist f unzerlegbar über Σ und F ist ein Zerfällungskörper von f über $K(s_1, \ldots, s_n)$, und es ist $\deg f = n$. Damit folgt $[F : K(s_1, \ldots, s_n)] \leq n!$. Weiterhin ist $|G| = n!$, womit nach Satz 1.2.3.6 $[F : \Sigma] = n!$ ist. Da $K(s_1, \ldots, s_n) \subseteq \Sigma$ folgt somit $\Sigma = K(s_1, \ldots, s_n)$.

Dass die Galoisgruppe isomorph zu S_n ist folgt direkt daraus, dass jede Nullstelle von f auf jede andere abgebildet werden kann.

(b) Siehe unten (Exkurs zum Transzendenzgrad).

(c) **Konstruktiver Beweis:** Sei $f \in \Sigma_1$. Zu zeigen: $f \in K[s_1, \ldots, s_n]$. Betrachte die lexikographische Anordnung der Monome $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, und sei $x_1 > \cdots > x_n$. (Beispiel: $x_1^3 x_2^5 > x_1^3 x_3^6$; siehe auch Abschnitt 2.1.)

Betrachte die elementarsymmetrischen Polynome; es ist $s_1 = x_1 + \cdots + x_n$, $s_2 = x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n$, $\ldots$, $s_n = x_1 \cdots x_n$.

Nun lässt sich f so anordnen: $f = x_1^{\alpha_1} \cdots x_n^{\alpha_n} + \ldots$, so dass $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ das Leitmonom ist (ohne Einschränkung sei der höchste Koeffizient gleich 1). Weiterhin muss dann $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$ gelten (gilt z.B. $\alpha_1 < \alpha_2$, ist wegen der Symmetrie auch $x_1^{\alpha_2} x_2^{\alpha_1} \cdots$ ein Monom in f).

Bilde dann $\tilde{f} := f - s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_{n-1}^{\alpha_{n-1} - \alpha_n} s_n^{\alpha_n}$. Dann ist das (lexikographisch) grösste Monom von $\tilde{f}$ kleiner als das von f.

Nach endlich vielen Schritten verbleibt eine Konstante.

Beispiel zum konstruktiven Beweis: Im Fall $n = 2$: Sei $f = x_1^2 + x_2^2$. Dann sind $\alpha_1 = 2$, $\alpha_2 = 0$, also $\tilde{f} = f - s_1^2 s_2^0 = -2s_2$, also insgesamt $f = s_1^2 - 2s_2$.

Im Fall $n = 3$: Betrachte $t_3 = x_1^3 + x_2^3 + x_3^3$. Dann sind $\alpha_1 = 3$, $\alpha_2 = \alpha_3 = 0$, also $\tilde{f} = f - s_1^3 s_2^0 s_3^0 = x_1^3 + x_2^3 + x_3^3 - (x_1 + x_2 + x_3)^3 = \ldots$ (weiter zur Übung).

Weiterhin im Fall $n = 3$: Betrachte $f = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = x_1^4 x_2^2 \pm \ldots$. Erster Reduktionsschritt: $f - s_1^{4-2} s_2^2 = f - (x_1 + x_2 + x_3)^2 (x_1x_2 + x_2x_3 + x_3x_1)^2 = \ldots$.

Weiterer Beweis: Es ist $K[x_1, \ldots, x_n]$ ganz algebraisch über $K[s_1, \ldots, s_n]$ (d. h. alle Elemente sind ganz[5] über $K[s_1, \ldots, s_n]$). Die x_i sind ganz über $K[s_1, \ldots, s_n]$, und die Theorie liefert dann, dass alle $f \in K[x_1, \ldots, x_n]$ ganz sind.

Also ist $K[x_1, \ldots, x_n]$ endlicher (d. h. er hat ein endliches Erzeugendensystem) $K[s_1, \ldots, s_n]$-Modul.

Weiterhin liefert die Theorie $K[s_1, \ldots, s_n]$ ganz abgeschlossen in $K(s_1, \ldots, s_n) = \Sigma$, d. h. $f \in \Sigma$ ganz über $K[s_1, \ldots, s_n] \Leftrightarrow f \in K[s_1, \ldots, s_n]$. Dies liefert die Behauptung.

(d) Folgt direkt aus (b).

□

Satz 1.2.4.8 (Abel[6] und Ruffini[7]). *Seien $c_1, \ldots, c_n$ algebraisch unabhängig über K. Die sogenannte* allgemeine Gleichung n-ten Grades *über K,*

$$g = x^n - c_1 x^{n-1} \pm \cdots + (-1)^n c_n = 0$$

ist über $K(c_1, \ldots, c_n)$ für $n \geq 5$ nicht auflösbar. *(Genaue Definition davon in Abschnitt 1.2.5.)*

Beweis. (Zum Teil mit Verweis auf Abschnitt 1.2.5.)

Sei E ein Zerfällungskörper von g über $K(c_1, \ldots, c_n)$, und seien $\alpha_1, \ldots, \alpha_n \in E$ die Nullstellen von g. Dann ist $E = K(c_1, \ldots, c_n)(\alpha_1, \ldots, \alpha_n)$. Wir wissen nach Vieta, dass $c_k = s_k(\alpha_1, \ldots, \alpha_n)$ ist, d. h. $c_1, \ldots, c_n \in K(\alpha_1, \ldots, \alpha_n)$. Da der Transzendenzgrad $\mathrm{Tr.deg}_K K(\alpha_1, \ldots, \alpha_n)$ eindeutig ist, müssen die $\alpha_1, \ldots, \alpha_n$ paarweise verschieden sein (ansonsten hätte $K(\alpha_1, \ldots, \alpha_n)$ einen Transzendenzgrad kleiner n, der Unterkörper $K(c_1, \ldots, c_n)$ hat jedoch nach Voraussetzung den Transzendenzgrad n).

Es liegt also genau die Situation von Satz 1.2.4.7 vor. Damit ist E galoissch über $K(c_1, \ldots, c_n)$ mit einer Galoisgruppe isomorph zu S_n. In Abschnitt 1.2.5 wird gezeigt: Wenn f auflösbar ist, dann ist auch G auflösbar. Da für $n \geq 5$ die Gruppe S_n nicht auflösbar ist (siehe Satz 1.2.5.14), folgt somit die Behauptung. □

[5] Sei S eine Ringerweiterung eines Ringes R. Dann heißt $\alpha \in S$ *ganz* über R, wenn es ein Polynom $f \in R[x] \setminus R$ mit $LK(f) = 1$ gibt so, dass $f(\alpha) = 0$ ist.

[6] Abel, 1802–1829, allgemeiner Beweis

[7] Ruffini, 1765–1822, Beweis für $n = 5$

Nun ein wenig Informationen zu den Begriffen Transzendenzbasis und -grad. Vergleiche Jacobson, van der Waerden, Lang u.v.m.

Sei im folgenden L eine Körpererweiterung von K.

Definition 1.2.4.9. *Sei Θ eine Teilmenge oder Familie aus L.*

(a) *Die Familie Θ heisst* algebraisch abhängig *(a. a.) über K, wenn es $n \in \mathbb{N}_{>0}$, $\theta_1, \ldots, \theta_n \in \Theta$ paarweise verschieden und ein $f \in K[x_1, \ldots, x_n] \setminus K$ gibt mit $f(\theta_1, \ldots, \theta_n) = 0$.*

(b) *Die Familie Θ heisst* algebraisch unabhängig *(a. u.) über K, wenn Θ nicht a. a. ist.*

Definition 1.2.4.10. *Eine maximale (d. h. nicht vergrößerbare) algebraisch unabhängige Teilmenge oder Familie $\Theta \subseteq L$ heißt* Transzendenzbasis *von L über K, und ihre Mächtigkeit* Transzendenzgrad *von L über K.*

Die Zweckmäßigkeit der Definition (insbesondere der des Transzendenzgrades) ergibt sich unter anderen aus folgendem Satz:

Satz 1.2.4.11.

(a) *Die Körpererweiterung L besitzt eine Transzendenzbasis.*

(b) *Alle Transzendenzbasen von L sind gleich mächtig. Man kann also von* dem *Transzendenzgrad von L über K sprechen.*

(c) *Jedes Erzeugendensystem von L enthält eine Transzendenzbasis.*

(d) *Sei etwa $L = K(\Theta)$. Jede algebraisch unabhängige Teilmenge oder Familie aus Θ kann gegebenenfalls durch Elemente aus Θ zu einer Transzendenzbasis von L über K ergänzt werden (vergleiche Basisergänzungssatz in der linearen Algebra).*

(e) *Für Teilmengen oder Familien Θ aus L gilt: Es ist L algebraisch über $K(\Theta)$ genau dann, wenn Θ eine Transzendenzbasis von L über K enthält.*

(f) *Ist $K \subseteq L \subseteq M$ ein Körperturm und ist Θ Transzendenzbasis von L über K, Σ Transzendenzbasis von M über L, so ist $\Theta \cup \Sigma$ Transzendenzbasis von M über K. Der Transzendenzgrad ist also additiv im Vergleich zum Körpergrad.*

Einen gut lesbaren und dennoch kurzen Textabschnitt, der gut zu dieser kurzen Einführung passt, bilden die Seiten 139–149 in dem Buch *A course in Galois Theory* von D. h. H. Garling [HG86].

Aber auch in den bereits mehrfach erwähnten Algebrawerken von Scheja-Storch, Jacobson, Lang und van der Waerden und vielen weiteren werden Transzendente Erweiterungen ausführlich behandelt. Im Falle der *Basic Algebra I* von Jacobson [Jac85] geschieht dies in Band 2, Seiten 510–512, als Beispiel zu einer axiomatisierten Abhängigkeitstheorie (Seiten 122–125), die dann in recht unterschiedlichen Kontexten benutzt werden kann.

1.2.5 Auflösen von Gleichungen durch iteriertes Wurzelziehen ("Radikale")

Bekannte Auflösungen von algebraischen Gleichungen:

quadratische Gleichungen (Char $K \neq 2$)	Schule
kubische Gleichungen	[Ebb92], [Jac85], [Wae03], [Tig02], ... (siehe auch Übung 19/20)
4. Grades	[Jac85], [Wae03], [Tig02], ...

In allen drei Fällen sind die Lösungen iterierte Wurzelausdrücke.

Definition 1.2.5.1.

(a) *Eine Körpererweiterung W von K heißt* Wurzelerweiterung *(WE) oder* radikale Erweiterung *von K, wenn (i) $W = K(\alpha)$ für ein $\alpha \in W$, und (ii) es ein $n \in \mathbb{N}_{>0}$ gibt mit $\alpha^n \in K$. (Dann ist α Nullstelle des Polynoms $x^n - \alpha^n \in K[x]$.)*

(b) *Ein Körperturm $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = W$ heißt* Wurzelturm *über K und W eine* iterierte Wurzelerweiterung *von K (iWE), wenn für $1 \leq i \leq r$ der Körper E_i eine Wurzelerweiterung von E_{i-1} ist.*

Definition 1.2.5.2. *Eine Polynom $f \in K[x] \setminus K$ heißt* zerlegbar *oder* auflösbar durch iteriertes Wurzelziehen*, wenn es eine iterierte Wurzelerweiterung W von K gibt so, dass W einen Zerfällungskörper von f enthält. Kurz: f z. i. W/a. i. W.*

Ist f zerlegbar in W, so nennt man die Gleichung $f(x) = 0$ auflösbar in W.

Beispiele 1.2.5.3.

(a) Eine Rechnung in MAPLE:

> $f := x^{12} - 10x^6 + 1;$

$$f := x^{12} - 10\,x^6 + 1$$

> $factor(f);$

$$x^{12} - 10\,x^6 + 1$$

> $factor(f, \sqrt{2});$

$$-(x^6 + 2\,x^3\,\sqrt{2} - 1)\,(-x^6 + 2\,x^3\,\sqrt{2} + 1)$$

> $factor(f, \sqrt{3});$

$$-(-x^6 + 2\,x^3\,\sqrt{3} - 1)\,(x^6 + 2\,x^3\,\sqrt{3} + 1)$$

> $factor(f, \{\sqrt{2}, \sqrt{3}\});$

$$(x^3 + \sqrt{3} + \sqrt{2})\,(x^3 - \sqrt{3} + \sqrt{2})\,(-x^3 - \sqrt{3} + \sqrt{2})\,(-x^3 + \sqrt{3} + \sqrt{2})$$

> $alias(\alpha = (\sqrt{2} + \sqrt{3})^{(1/3)});$

$$\alpha$$

> $ff := simplify(factor(f, \{\sqrt{2}, \sqrt{3}, \alpha\}));$

$$\begin{aligned} ff := &-(x^2 - x\,\alpha + \diamond)\,(-x^2 - \diamond\,x\,\sqrt{3} + \diamond\,x\,\sqrt{2} - \alpha\,\sqrt{3} + \alpha\,\sqrt{2}) \\ &(x^2 - \diamond\,x\,\sqrt{3} + \diamond\,x\,\sqrt{2} + \alpha\,\sqrt{3} - \alpha\,\sqrt{2})\,(x^2 + x\,\alpha + \diamond)\,(x - \diamond\,\sqrt{3} + \diamond\,\sqrt{2}) \\ &(-x - \diamond\,\sqrt{3} + \diamond\,\sqrt{2})\,(-x^2 + \diamond) \\ &\text{wobei} \qquad \diamond := (\sqrt{3} + \sqrt{2})^{(2/3)} \end{aligned}$$

> $g := op(1, ff); h := op(2, ff); k := op(3, ff); l := op(4, ff);$

$$g := -1$$

$$h := x^2 - x\,\alpha + (\sqrt{3} + \sqrt{2})^{(2/3)}$$

$$k := -x^2 - (\sqrt{3}+\sqrt{2})^{(2/3)}\, x\, \sqrt{3} + (\sqrt{3}+\sqrt{2})^{(2/3)}\, x\, \sqrt{2} - \alpha\, \sqrt{3} + \alpha\, \sqrt{2}$$

$$l := x^2 - (\sqrt{3}+\sqrt{2})^{(2/3)}\, x\, \sqrt{3} + (\sqrt{3}+\sqrt{2})^{(2/3)}\, x\, \sqrt{2} + \alpha\, \sqrt{3} - \alpha\, \sqrt{2}$$

> $collect(l, X)$;

$$x^2 - (\sqrt{3}+\sqrt{2})^{(2/3)}\, x\, \sqrt{3} + (\sqrt{3}+\sqrt{2})^{(2/3)}\, x\, \sqrt{2} + \alpha\, \sqrt{3} - \alpha\, \sqrt{2}$$

> $solve(\%)$;

$$\frac{(\sqrt{3}+\sqrt{2})^{(2/3)}\,\sqrt{3}}{2} - \frac{(\sqrt{3}+\sqrt{2})^{(2/3)}\,\sqrt{2}}{2} + \frac{1}{2}\,\mathbf{i}\,\sqrt{-5\,\diamond + 2\,\diamond\,\sqrt{3}\,\sqrt{2} - 4\,\alpha\,\sqrt{2} + 4\,\alpha\,\sqrt{3}},$$
$$\frac{(\sqrt{3}+\sqrt{2})^{(2/3)}\,\sqrt{3}}{2} - \frac{(\sqrt{3}+\sqrt{2})^{(2/3)}\,\sqrt{2}}{2} - \frac{1}{2}\,\mathbf{i}\,\sqrt{-5\,\diamond + 2\,\diamond\,\sqrt{3}\,\sqrt{2} - 4\,\alpha\,\sqrt{2} + 4\,\alpha\,\sqrt{3}}$$
$$\text{wobei} \qquad \diamond := (\sqrt{3}+\sqrt{2})^{(4/3)}$$

> $ff := simplify(factor(f, \{\sqrt{2}, \sqrt{3}, \alpha, \mathbf{i}\}))$;

$$\begin{aligned} ff := {} & (-\alpha + \alpha\,\sqrt{3}\,\mathbf{i} + 2\,x)\,(\alpha + \alpha\,\sqrt{3}\,\mathbf{i} - 2\,x) \\ & (\diamond\,\sqrt{3} - \diamond\,\sqrt{2} + \diamond\,\sqrt{2}\,\sqrt{3}\,\mathbf{i} - 3\,\mathbf{i}\,\diamond + 2\,x) \\ & (\diamond\,\sqrt{2}\,\sqrt{3}\,\mathbf{i} + \diamond\,\sqrt{2} - 3\,\mathbf{i}\,\diamond - \diamond\,\sqrt{3} - 2\,x) \\ & (-\diamond\,\sqrt{3} + \diamond\,\sqrt{2} - 3\,\mathbf{i}\,\diamond + \diamond\,\sqrt{2}\,\sqrt{3}\,\mathbf{i} + 2\,x) \\ & (\diamond\,\sqrt{3} - \diamond\,\sqrt{2} - 3\,\mathbf{i}\,\diamond + \diamond\,\sqrt{2}\,\sqrt{3}\,\mathbf{i} - 2\,x)\,(\alpha + \alpha\,\sqrt{3}\,\mathbf{i} + 2\,x) \\ & (-\alpha + \alpha\,\sqrt{3}\,\mathbf{i} - 2\,x)\,(x - \diamond\,\sqrt{3} + \diamond\,\sqrt{2})\,(-x - \diamond\,\sqrt{3} + \diamond\,\sqrt{2})\,(-x^2 + \diamond)\,/ \\ & 256 \end{aligned}$$
$$\text{wobei} \qquad \diamond := (\sqrt{3}+\sqrt{2})^{(2/3)}$$

> $simplify(subs(x = -(\alpha + \mathbf{i}\alpha\sqrt{3})/2, f))$;

$$0$$

> $alias(\beta = RootOf(f))$;

$$\alpha,\ \beta$$

> $factor(f, \beta)$;

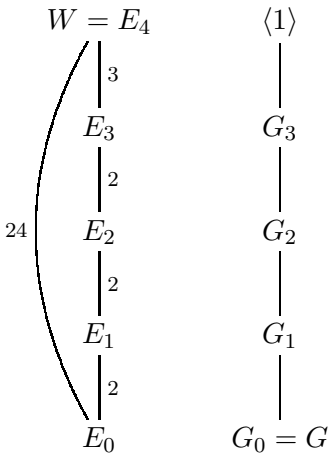
$$-(\beta^2 + \beta\,x + x^2)\,(-x^2 - 10\,\beta^5\,x + \beta^{11}\,x - 10\,\beta^4 + \beta^{10})\,(x^2 - 10\,\beta^5\,x + \beta^{11}\,x + 10\,\beta^4 - \beta^{10})$$
$$(\beta^2 - \beta\,x + x^2)\,(x - 10\,\beta^5 + \beta^{11})\,(-x - 10\,\beta^5 + \beta^{11})\,(x + \beta)\,(-x + \beta)$$

> $factor(f, \{\beta, RootOf(x^2 + 10x\beta^5 - x\beta^{11} + 10\beta^4 - \beta^{10})\})$;

$$\begin{aligned} & (10\,\beta^5 - \beta^{11} + \diamond + x)\,(-x + \diamond)\,(x + \diamond)\,(10\,\beta^5 - \beta^{11} + \diamond - x)\,(x - 10\,\beta^5 + \beta^{11}) \\ & (-x - 10\,\beta^5 + \beta^{11})\,(\beta + \diamond\,\beta^2 - x)\,(\diamond\,\beta^2 + x)\,(\beta + \diamond\,\beta^2 + x)\,(\diamond\,\beta^2 - x)\,(x + \beta) \\ & (-x + \beta) \end{aligned}$$
$$\text{wobei} \qquad \diamond := \mathrm{RootOf}(\_Z^2 + (10\,\beta^5 - \beta^{11})\,\_Z - \beta^{10} + 10\,\beta^4)$$

Setze $E_0 := \mathbb{Q}$, $E_1 := E_0(\mathbf{i})$, $E_2 := E_1(\sqrt{2})$, $E_3 := E_2(\sqrt{3})$, $E_4 := E_3(\sqrt[3]{\sqrt{2}+\sqrt{3}}) =: W$. Wir wollen zeigen, dass W ein Zerfällungskörper von $x^{12} - 10x^6 + 1$ über $\mathbb{Q}$ ist (nur speziell

in diesem Beispiel!).



Hier speziell ist E_1 galoissch über E_0, E_2 galoissch über E_1, E_3 galoissch über E_2 und E_4 galoissch über E_3.

- Satz 1.2.3.13: E_i ist G_{i-1}-invariant für $0 < i \leq 4$.
- Satz 1.2.3.11: G_i ist Normalteiler in G_{i-1}, und $G_{i-1}/G_i \cong \mathrm{Aut}_{E_{i-1}}(E_i)$.

Es liegt also eine Normalteilerkette vor:

$$\langle 1 \rangle = G_4 \trianglelefteq G_3 \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G,$$

wobei der Faktor G_{i-1}/G zyklisch ist (also insbesondere kommutativ). Siehe auch Definition 1.2.5.6.

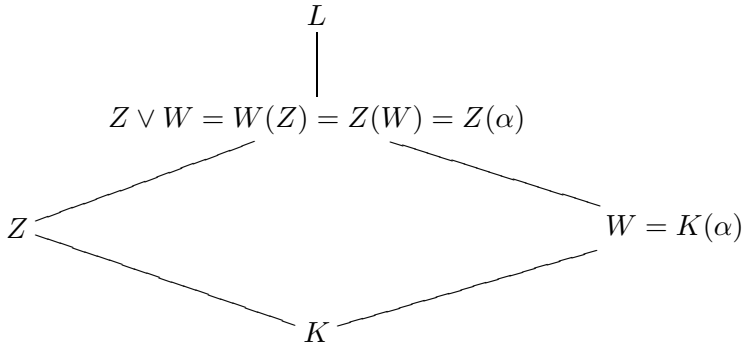
(b) Ist $|K| < \infty$, $f \in K[x] \setminus K$, dann ist f auflösbar durch iteriertes Wurzelziehen.

Beweis. Es sei L ein Zerfällungskörper von f über K, $\mathrm{Char}\, K = p$. Dann ist L einfach über K, und $|L| = p^r$. Sei $L = K(\zeta)$, $\zeta^{p^r-1} = 1 \in K$, also ist L Wurzelerweiterung über K. □

(c) Das Polynom $x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist *nicht* auflösbar durch iteriertes Wurzelziehen (siehe unten).

Beobachtung 1.2.5.4.

(a) (i) Sei L eine Körpererweiterung von K, und $Z, W \in \mathscr{Z}_K(L)$. Sei W eine Wurzelerweiterung von K, etwa $W = K(\alpha)$ mit $\alpha^n \in K$. Dann ist $Z(W)$ eine Wurzelerweiterung über Z und insbesondere $Z(W) = Z(\alpha)$.



(ii) Ist W iterierte Wurzelerweiterung über K, dann auch $Z(W)$ über Z.

(b) Sei $W = K(\alpha)$ Wurzelerweiterung über K, $\alpha^n \in K$, $f = x^n - k \in K[x]$ mit $k = \alpha^n$. Ist weiterhin Z ein Zerfällungskörper von f über $K(\alpha)$, so ist Z eine iterierte Wurzelerweiterung von K.

Beweis.

(a) ✓

(b) Sei $G = \mathrm{Aut}_K(Z)$, $K(\alpha) = E \subseteq Z$. Dann ist $\sigma(E) \subseteq Z$ für $\sigma \in G$. Weiterhin ist $Z = \bigvee_{\sigma \in G} \sigma(E)$ (dabei ist $\sigma(E)$ eine Wurzelerweiterung von K). Benutze (a): $E \subseteq E(\sigma_1(E)) \subseteq \cdots \subseteq Z$ iterierte Wurzelerweiterung.

□

Beobachtung 1.2.5.5.

(a) Sei $W = K(\alpha)$, $\alpha^n \in K$, $n > 1$ eine Wurzelerweiterung. Dann gibt es Primzahlen $p_1, \ldots, p_r$ mit $p_i \mid n$ und $\alpha_1, \ldots, \alpha_r \in W$ mit $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_r) = W$ und $\alpha_i^{p_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$.

(b) Jeder Wurzelturm kann zu einem Primwurzelturm verfeinert werden. Sprechweise: iterierte Primwurzelerweiterung (i. PWE).

Beweis.

(a) Sei $p_1 \mid n$, $n = mp_1$. Dann setze $\alpha_1 := \alpha^m$. Nun ist $K(\alpha)$ eine Wurzelerweiterung von $K(\alpha_1)$, wobei $\alpha^m \in K(\alpha_1)$ ist. Fahre iterativ fort, bis $m = 1$ ist.

(b) Folgt aus (a).

□

Definition 1.2.5.6. *Sei G eine endliche Gruppe. G heißt* auflösbar*, wenn es eine Normalteilerkette (*Normalreihe*)* $\langle 1 \rangle = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$ *gibt derart, dass die Faktoren G_{i-1}/G_i kommutativ sind.*

Insbesondere ist also jede endliche abelsche Gruppe auflösbar. Nun ein Satz aus der Gruppentheorie:

Satz 1.2.5.7.

(a) *Untergruppen und Faktorgruppen auflösbarer Gruppen sind auflösbar.*

(b) *Sei G eine Gruppe und H ein Normalteiler in G. Wenn H und G/H auflösbar sind, dann auch G.*

Wir benutzen (a) (ohne Beweis).

Satz 1.2.5.8 (Notwendige Bedingung für die Auflösbarkeit einer algebraischen Gleichung in einer Variablen durch iteriertes Wurzelziehen). *Sei W eine iterierte Wurzelerweiterung über K und F ein Zwischenkörper ($K \subseteq F \subseteq W$). Dann ist* $\mathrm{Aut}_K(F)$ *auflösbar.*

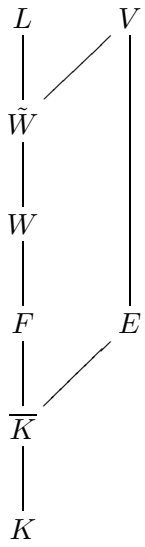
Bemerkung 1.2.5.9. Die Umkehrung gilt bei $\mathrm{Char}\, K = 0$. Bei Charakteristik p gilt die Umkehrung nach Modifikation des Begriffes "iterierte Wurzelerweiterung".

Beweis von Satz 1.2.5.8.

(I) (Einführung von $\overline{K}$.) Es ist $\mathrm{Aut}_K(F) = \mathrm{Aut}_{\overline{K}}(F)$, und F ist über $\overline{K}$ galoissch.

(II) (Einführung von $\tilde{W}$.) Sei L ein Zerfällungskörper über $\overline{K}$, der W enthält, und $\tilde{W}$ die invariante Hülle von W in L (es ist $\tilde{W} = \bigvee_{\sigma \in \mathrm{Aut}_K(L)} \sigma(W)$).

Es ist $\tilde{W}$ eine iterierte Wurzelerweiterung über K (siehe Beobachtung 1.2.5.4). Ohne Einschränkung sei $\tilde{W}$ eine iterierte Primwurzelerweiterung.



Jeder Automorphismus von F in K lässt sich fortsetzen auf $\tilde{W}$. Es ist $\overline{K}$ abgeschlossen in F, und $[F : K] < \infty$.

Satz 1.2.3.13 liefert: F ist $\tilde{G}$-invariant mit $\tilde{G} = \mathrm{Aut}_{\overline{K}}(\tilde{W})$.

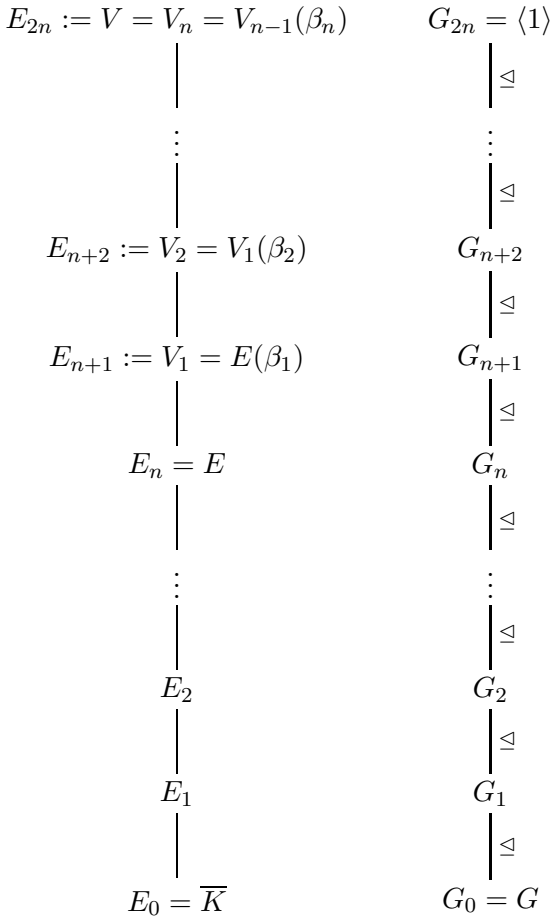
Satz 1.2.3.11(c) liefert: $F' = \mathrm{Aut}_F(\tilde{W}) \trianglelefteq \tilde{G}$, und $\tilde{G}|_F \cong \tilde{G}/F'$, wobei $\tilde{G}|_F = \mathrm{Aut}_{\overline{K}}(F)$ ist.

Mit Satz 1.2.5.7(a) reicht es also zu zeigen, dass $\tilde{G}$ auflösbar ist (da $G = \mathrm{Aut}_K(F) = \mathrm{Aut}_{\overline{K}}(F)$ ist und $\mathrm{Aut}_{\overline{K}}(F) = \tilde{G}|_F$ ein Quotient von $\tilde{G}$ ist).

(III) (Einführung von V und E.) Sei $\tilde{W} = \overline{K}(\beta_1, \ldots, \beta_n)$ mit $\beta_1^{p_1} \in \overline{K}$, $\beta_i^{p_i} \in \overline{K}(\beta_1, \ldots, \beta_{i-1})$ für $2 \leq i \leq n$, p_i prim. Sei nun V ein Zerfällungskörper des Polynoms $g := (x^{p_1} - 1) \cdots (x^{p_n} - 1)$ über $\tilde{W}$. Der Körper V enthält einen Zerfällungskörper E von g über $\overline{K}$.

Es genügt, $G = \mathrm{Aut}_{\overline{K}}(V)$ zu betrachten, da $\tilde{G}$ (wie in (II)) eine Faktorgruppe von G ist.

(IV) (Auflösbarkeit von G.) Betrachte folgendes Diagramm:



Es ist V_n Zerfällungskörper von $x^{p_n} - \beta_n^{p_n}$ über V_{n-1} in V, ..., V_2 Zerfällungskörper von $x^{p_2} - \beta_2^{p_2}$ über V_1 in V, V_1 Zerfällungskörper von $x^{p_1} - \beta_1^{p_1}$ über E in V, E Zerfällungskörper von $x^{p_n} - 1$ über E_{n-1} in V, ... E_2 Zerfällungskörper von $x^{p_2} - 1$ über E_1 in V, und E_1 Zerfällungskörper von $x^{p_1} - 1$ über $\overline{K}$ in V.

Setze $A_{i+1} := \mathrm{Aut}_{E_i}(E_{i+1})$, $1 \leq i < 2n$. Dann gilt $A_{i+1} \cong G_i/G_{i+1}$, $1 \leq i < 2n$ (siehe unten).

Nach Beobachtung 1.2.5.10 und Beobachtung 1.2.5.11 (siehe unten) sind $\mathrm{Aut}_{E_i}(E_{i+1})$, $i = 0, \ldots, n-1$ und $\mathrm{Aut}_{V_i}(V_{i+1})$, $i = 0, \ldots, n-1$ (mit $V_0 := E_n$) kommutativ. Da alle V_{i+1} Zerfällungskörper über V_i und alle E_{i+1} Zerfällungskörper über E_i sind folgt (siehe oben in (II))

$$G_{i+1} \trianglelefteq G_i \qquad (i = 0, \ldots, 2n-1)$$

und

$$G_i/G_{i+1} \cong \mathrm{Aut}_{E_i}(E_{i+1}), \qquad G_{n+i}/G_{n+i+1} \cong \mathrm{Aut}_{V_i}(V_{i+1}) \qquad (i = 0, \ldots, n-1).$$

Insgesamt folgt die Auflösbarkeit von G. □

Die folgenden beiden Beobachtungen komplettieren den Beweis von Satz 1.2.5.8. Sie ergeben die Kommutativität sämtlicher Faktoren $A_{i+1} = \mathrm{Aut}_{E_i}(E_{i+1})$.

Beobachtung 1.2.5.10. Sei q eine Primzahl und L ein Zerfällungskörper von $x^q - 1$ über K, dann ist $\mathrm{Aut}_K(L)$ kommutativ.

Beweis. Ist $\mathrm{Char}\, K = q$, dann ist $x^q - 1 = (x-1)^q$ und daher $L = K$ und $A = \langle 1 \rangle$ kommutativ. Sei also $\mathrm{Char}\, K \neq q$. Dann hat $x^q - 1$ paarweise verschiedene Nullstellen (betrachte die Ableitung). Die Menge N der q Nullstellen ist eine multiplikative Untergruppe von $L \setminus \{0\}$ und zyklisch, etwa $N = \langle \varphi \rangle$. Dann ist $L = K(\varphi)$. Ein Automorphismus aus $\mathrm{Aut}_K(L)$ ist durch seine Wirkung auf φ völlig bestimmt. Seien $\sigma, \tau \in \mathrm{Aut}_K(L)$, dann gibt es $i, j \in \{1, \ldots, q-1\}$ mit denen $\sigma(\varphi) = \varphi^i$ und $\tau(\varphi) = \varphi^j$ gilt. Offensichtlich ist dann $\sigma\tau(\varphi) = \tau\sigma(\varphi)$, woraus $\sigma\tau = \tau\sigma$ folgt. Demnach ist $\mathrm{Aut}_K(L)$ kommutativ. □

Beobachtung 1.2.5.11. Sei q eine Primzahl, K ein Körper und $a \in K$. In $K[x]$ zerfalle $x^q - 1$ in Linearfaktoren. Sei außerdem L ein Zerfällungskörper von $x^q - a$ über K. Dann ist $\mathrm{Aut}_K(L)$ kommutativ.

Beweis. Die Nullstellenmenge N von $x^q - 1$ ist eine kommutative Gruppe. Für die Nullstellenmenge M von $x^q - a$ gilt $M = N\alpha$, wobei α eine Nullstelle von $x^q - a$ ist. Seien nun $\sigma, \tau \in \mathrm{Aut}_K(L)$, dann muß mit geeigneten $\varphi, \psi \in N$ gelten $\sigma(\alpha) = \varphi\alpha$ und $\tau(\alpha) = \psi\alpha$. Da $L = K(\alpha)$ ergibt sich $\sigma\tau = \tau\sigma$. □

Übungsaufgabe: Zeigen Sie in beiden Beobachtungen, dass $\mathrm{Aut}_K(L)$ sogar zyklisch ist.

Was hilft uns Satz 1.2.5.8?

Bei konkretem $f \in \mathbb{Q}[x]$ etwa: Theorieorientiert: Konstruiere Zerfällungskörper und betrachte die Gruppe. (Ist f unzerlegbar? Dann $F_1 := \mathbb{Q}[x]/f\mathbb{Q}[x]$, und zerlege f über F_1 in Primfaktoren; dies ist in endlich vielen Schritten berechenbar.) Zur Berechnung der Automorphismengruppe (Galois-Gruppe) siehe weiter unten.

Wenn G nicht auflösbar ist, ist Satz 1.2.5.8 nützlich.

Beispiele nicht auflösbarer Polynome: Siehe zum Beispiel das Aufgabenblatt.

Definition 1.2.5.12. *Sei $f \in K[x] \setminus K$, L ein Zerfällungskörper von f über K und $LK(f) = 1$ (also f normiert). Dann heißt* $\mathrm{Aut}_K(L)$ Galois-Gruppe *von f über K. Bezeichne* $\mathrm{Aut}_K(L)$ *mit G_f.*

Beobachtung 1.2.5.13 (Wiederholung). Ist f unzerlegbar, $\deg f = n$, $L = K(\alpha_1, \ldots, \alpha_n)$, so ist G_f isomorph zu einer Untergruppe von S_n. Also ist $|G_f|$ ein Teiler von $n!$. Dabei kommt S_n selber vor!

Ist S_n auflösbar? Da hilft folgender Satz aus der Gruppentheorie (vergleiche z. B. Jacobson, S. 240):

Satz 1.2.5.14. *Ist $n \geq 5$, so ist S_n nicht auflösbar.*

Satz 1.2.5.15. *Sei p prim, $f \in \mathbb{Q}[x]$ unzerlegbar, $\deg f = p$. Wenn f genau zwei nicht-reelle Nullstellen hat, dann ist $G_f \cong S_p$.*

Beweis. Sei L ein Zerfällungskörper von f über $\mathbb{Q}$ und $n = [L : \mathbb{Q}]$. Sei $\alpha \in L$ mit $f(\alpha) = 0$.

$$\begin{array}{c} L \\ {\scriptstyle n}\,\big| \\ \mathbb{Q} \end{array}$$

Es folgt (Gradsatz, $f = \mathrm{MiPo}(\alpha, \mathbb{Q})$)

$$p \mid n.$$

Dann hat $G = \mathrm{Aut}_{\mathbb{Q}}(L)$ genau n Elemente. Gruppentheorie: Es gibt eine Untergruppe der Ordnung p (und diese ist zyklisch). Sei etwa σ der Erzeuger; dann muss σ ein p-Zyklus sein. Entspreche τ der komplexen Konjugation. Dann wirkt τ als Transposition auf $\{\alpha_1, \ldots, \alpha_n\}$. Die Behauptung folgt mit Lemma 1.2.5.16: □

Lemma 1.2.5.16. *Sei U eine Untergruppe von S_p, p prim, die einen p-Zyklus und eine Transposition enthält. Dann ist $U = S_p$.*

Beispiele 1.2.5.17.

- $x^5 - 6x + 3$ [Kap72, S. 34];
- $x^5 - 4x + 3$ [Kun94, S. 193].

Vor dem Beweis möchten wir die Zykelschreibweise für Permutationen einführen. Wir schreiben $(i_1 i_2 \cdots i_r)$ für die Permutation der Menge $\{1, \ldots, n\}$, die i_j auf i_{j+1} und i_r auf i_1 abbildet und sonst die Identität ist. Nun kann jede Permutation $\sigma \in S_n$ als Produkt solcher Zyklen geschrieben werden:

$$\sigma = (i_1^{(1)} \cdots i_{r^{(1)}}^{(1)}) \cdots (i_1^{(k)} \cdots i_{r^{(k)}}^{(k)}).$$

Eine Transposition ist also ein Zykel der Form (ij).

Beweis von Lemma 1.2.5.16. Sei ohne Einschränkung $p \geq 3$.

Sei σ der p-Zykel und $\tau = (ij)$, $i < j$ die Transposition. Es gibt ein $k \in \{1, \ldots, p-1\}$ mit $\sigma^k(i) = j$. Da p prim ist σ^k ein p-Zyklus. Ohne Einschränkung sei $\sigma = (12 \cdots p)$, $\tau = (12)$. Nun gilt $\sigma\tau\sigma^{-1} = (23)$, $\sigma^2\tau\sigma^{-2} = (34)$, …(denn: $(1 \cdots p)(12)(1p \cdots 2) = (23)$). Nun ist jede Transposition als Produkt der Transpositionen (12), (23), …, $(p-1, p)$, $(p1)$ darstellbar und liegt damit in U, und damit wiederum folgt $U = S_p$. □

1.2.6 Zur Berechnung von Galois-Gruppen

Literatur:

- Garling, *A course in Galois-Theory* [HG86],
- van der Waerden, *Algebra* [Wae03],
- Cohen, *A Course in Computational Number Theory* [Coh03].

Hier:

- prinzipielles Verfahren
- Anwendung: modulares Verfahren
- Hinweise zu "realistischen" Verfahren

Idee: Sei $f \in \mathbb{Q}[x]$ unzerlegbar, $\deg f = n$, $[L : \mathbb{Q}] \leq n!$ mit L Zerfällungskörper von f über $\mathbb{Q}$. Es sei L galoissch über $\mathbb{Q}$ (also $\mathbb{Q} = \overline{\mathbb{Q}}$). Es gibt ein β derart, das $L = \mathbb{Q}(\beta)$. Seien $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f, dann kann β in der Form $\sum_{i=1}^{n} \alpha_i \eta_i$ gefunden werden mit $\eta_i \in \mathbb{Q}$ (Satz vom primitiven Element). Sei $\sigma \in G_f$ (also Permutation der α_is). Dann ist $\sigma(\beta) = \sum \alpha_{\sigma(i)} \eta_i = \sum \alpha_i \eta_{\sigma^{-1}(i)}$. Es ist $\mathrm{MiPo}(\beta, \mathbb{Q}) = \prod_{\sigma \in G_f} (x - \sigma(\beta))$.
Universell/Allgemein: Sei K ein Körper, $t_1, \ldots, t_n$, $y_1, \ldots, y_n$ algebraisch unabhängig über K. Betrachte

$$p := \prod_{\sigma \in S_n} \left(x - \sum_{i=1}^{n} t_{\sigma(i)} y_i \right) = \prod_{\sigma \in S_n} \left(x - \sum_{i=1}^{n} t_i y_{\sigma^{-1}(i)} \right) = \sum_{i=0}^{n!} c_i x^i,$$

wobei

$$c_i \in K[t_1, \ldots, t_n, y_1, \ldots, y_n] \qquad \text{und} \qquad p \in K[t_1, \ldots, t_n, y_1, \ldots, y_n][x] \qquad \text{ist.}$$

Die c_i sind symmetrisch in $(K[y_1, \ldots, y_n])[t_1, \ldots, t_n]$ und in $(K[t_1, \ldots, t_n])[y_1, \ldots, y_n]$. Der Hauptsatz über symmetrische Polynome besagt, dass die c_i darstellbar sind durch symmetrische Polynome.

Beispiele 1.2.6.1.

(a) Für $n = 2$: $p = (x - t_1 y_1 - t_2 y_2)(x - t_2 y_1 - t_1 y_2) = x^2 - s_1(t) p_1(y) x + (s_2(t) p_2(y) + p_2(t) s_2(y))$ wobei $p_1(y) = s_1(y) = y_1 + y_2$ und $p_2(y) = y_1^2 + y_2^2$.

(b) Für $n = 3$: $p = x^6 - \cdots + (s_3(t) p_3(y) + p_3(t) s_3(y))$ mit $p_3(y) = y_1^3 + y_2^3 + y_3^3$.

(c) Allgemein: p hat $(n+1)^{n!}$ Terme. Im Fall $n = 9$ sind dies bereits über 10^{362881} Terme!

Im folgenden werden Permutationen $\sigma \in S_n$ auf sehr unterschiedliche Weisen interpretiert:

- σ_α:
  - Automorphismen von $L = K(\alpha_1, \ldots, \alpha_n)$ über K, und die α_i sind die paarweise verschiedenen Nullstellen von $f \in K[x]$;
  - Automorphismen von $L[y_1, \ldots, y_n]$ über $K[y_1, \ldots, y_n]$;
  - Automorphismen von $L[y_1, \ldots, y_n][x]$ über $K[y_1, \ldots, y_n][x]$.
- τ_y:
  - Automorphismen von $K[y_1, \ldots, y_n]$ über K;
  - Automorphismen von $L[y_1, \ldots, y_n]$ über L;
  - Automorphismen von $L[y_1, \ldots, y_n][x]$ über $L[x]$.

Insbesondere werden diese Interpretationen auch benutzt für $\sigma \in G_f \subseteq S_n$. Sei nun $f \in K[x]\backslash K$, $LK(f) = 1$, und f habe die paarweise verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n$ ($n = \deg f$) in L, wobei L Zerfällungskörper von f über K sei (insbesondere $K = \overline{K}$). Einsetzen der α_i in p liefert:

$$\begin{aligned} F &= \prod_{\sigma\in S_n} (x - \alpha_{\sigma(1)}y_1 - \cdots - \alpha_{\sigma(n)}y_n) = \prod_{\sigma\in S_n} (x - \sigma_\alpha(\beta)) \qquad (\beta = \sum \alpha_i y_i) \\ &= \prod_{\sigma\in S_n} \Big(x - \sum \alpha_i y_{\sigma^{-1}(i)}\Big) = \prod_{\sigma\in S_n} (x - \sigma_y^{-1}(\beta)) = \prod_{\sigma\in S_n} (x - \sigma_\alpha(\beta)). \end{aligned}$$

Es ist $F \in K[y_1, \ldots, y_n][x]$, denn (siehe oben bei p) die c_i sind symmetrisch in den α_i. Einsetzen der α_i führt nach K. Beachte, dass $\sigma_y(\beta) = \sigma_\alpha^{-1}(\beta)$ für alle $\sigma \in S_n$ gilt (Umordnung der Summe). **Wichtig:** Die $c_i(\alpha_1, \ldots, \alpha_n)$ können ohne Kenntnis der α_i berechnet werden. Zerlege F in Primfaktoren in $K[y_1, \ldots, y_n][x]$ (zum Beispiel über $\mathbb{Q}$ in endlich vielen Schritten möglich).

Nun gilt F unzerlegbar $\Leftrightarrow$ $G_f = S_n$. Sei nun $F = F_1 \cdots F_r$, $r \geq 2$, F_i prim (paarweise verschieden!). Dann gibt es $N_1, \ldots, N_r \subseteq S_n$ mit $\bigcup N_i = S_n$, $N_i \cap N_j = \emptyset$ für $i \neq j$, und

$$F_i = \prod_{\sigma\in N_i} (x - \sigma_\alpha(\beta)) = \prod_{\sigma\in N_i} (x - \sigma_\alpha^{-1}(\beta)).$$

Beachte: Anwenden von σ_y auf F permutiert die Primfaktoren.
Wo steckt die Galois-Gruppe G_f?: Sei $G_i := \{\sigma \in S_n \mid \sigma_y(F_i) = F_i\}$.

> **Behauptung:** Alle G_i sind konjugiert, d. h. zu G_i, G_j gibt es ein $\tau \in S_n$ mit $\tau_y G_i \tau_y^{-1} = G_j$.
>
> **Beweis:** Da S_n auf den $n!$ Linearfaktoren $(x - \sigma_y(\beta))$ transitiv operiert gibt es zu $i \neq j$ stets ein $\tau \in S_n$ derart, dass $\tau_y F_i = F_j$. Dann ist $\tau_y G_i \tau_y^{-1} = G_j$, und insbesondere $G_i \cong G_j$. □

Satz 1.2.6.2. *Unter obrigen Voraussetzungen und der Annahme $(x - \beta) \mid F_1$ bzw.* **id** $\in N_1$ *gilt $G_f = G_1$.*

Beweis. Sei $H = \prod_{\sigma\in G_f}(x - \sigma_y(\beta))$. Wir zeigen, dass H unzerlegbar in $K[y_1, \ldots, y_n][x]$ ist. Da F_1 und H beide β als Nullstelle haben und unzerlegbar und normiert sind folgt $F_1 = H$ und somit $G_f = N_1$. Nun ist N_1 eine Untergruppe von S_n, womit $G_1 = \{\sigma \in S_n \mid \sigma N_1 = N_1\} = N_1 = G_f$ folgt.

Beachte, dass $K(y_1, \ldots, y_n)(\alpha_1, \ldots, \alpha_n)$ galois'sch über $K(y_1, \ldots, y_n)$ ist, und dass man die zugehörige Galoisgruppe durch $\{\tau_\alpha \mid \tau \in G_f\}$ gegeben ist. Sei $\tau \in G_f$; dann ist

$$\tau_\alpha(H) = \prod_{\sigma\in G_f} (x - \tau_\alpha\sigma_y(\beta)) = \prod_{\sigma\in G_f} (x - \sigma_y\tau_y^{-1}(\beta)) = \prod_{\sigma\in G_f} (x - \sigma_y(\beta)) = H.$$

Damit folgt $H \in K(y_1, \ldots, y_n)[x]$ und auch $H \in K[y_1, \ldots, y_n][x]$. Dass H unzerlegbar ist folgt daraus, dass alle $\sigma_\alpha(\beta)$, $\sigma \in G_f$ Nullstellen von H sein müssen. □

Folgerung 1.2.6.3. *Die Galois-Gruppe G_f ist effektiv berechenbar z. B. über $\mathbb{Q}$ oder gewissen Erweiterungen.*

Erläuterung: Ein möglicher Algorithmus:

- Eingabe $f \in \mathbb{Q}[x] \setminus \mathbb{Q}$ mit $LK(f) = 1$, $\deg f = n$, und f ohne mehrfache Nullstellen.

1. Stelle p dar in $\mathbb{Q}[t_1, \ldots, t_n, y_1, \ldots, y_n][x]$:

$$p = \sum_{k=0}^{n!} \sum g_d^{(k)} y^d x^k \qquad (g_d^{(k)} \in \mathbb{Q}[t_1, \ldots, t_n],\ d = (d_1, \ldots, d_n) \in \mathbb{N}^n,\ y^d = y_1^{d_1} \cdots y_n^{d_n}).$$

Es ist p symmetrisch in den t_i.

2. Stelle g_d durch elementarsymmetrische Polynome dar:

$$p \in \mathbb{Q}[s_1(t), \ldots, s_n(t)][y_1, \ldots, y_n][x].$$

3. Es sei $f = x^n + \sum_{i=0}^{n-1} a_i x^i$. Setze a_j für s_i ein (i, j geeignet) und erhalte F.

4. Faktorisiere F, $F = F_1 \cdots F_r$.

5. Für ein F_i bestimmte $G_i \cong G_f$.

Abschluss von Abschnitt 6: Das Verfahren, welches sich aus Satz 1.2.6.2 bzw. Folgerung 1.2.6.2 ergibt, ist praktisch gesehen für wachsende n unrealistisch ("Explosion"). Aber es gibt praktische relevante Konsequenzen!

Satz 1.2.6.4. *Seien $f \in \mathbb{Z}[x]$, p prim, $\overline{f} \equiv f \pmod{p}$ (in $\mathbb{Z}_p$), $LK(f) = 1$. Es habe f paarweise verschiedene Nullstellen in $\mathbb{C}$ und $\overline{f}$ habe paarweise verschiedene Nullstellen in einem Zerfällungskörper über $\mathbb{Z}_p$. Dann ist $G_{\overline{f}}$ isomorph zu einer Untergruppe von G_f. Bei geeigneter Interpretation: $G_{\overline{f}} \subseteq G_f$ Untergruppe.*

Beweis. Siehe van der Waerden [Wae03] oder Garling [HG86]. □

Beachte: $G_{\overline{f}}$ ist die Galoisgruppe von $\overline{f}$ über $\mathbb{Z}_p$ und daher zyklisch (ohne Beweis).

Beispiel 1.2.6.5. Sei $f = x^6 + x^4 + 1$, unzerlegbar in $\mathbb{Z}[x]$.

- $n = 2$: $\overline{f} = (x^3 + x^2 + 1)^2$;
- $n = 3$: $\overline{f} = (x^4 + 2x^3 + 1)(x + 1)(x + 2)$;
- $n = 5$: $\overline{f} = (x^3 + 4x^2 + x + 2)(x^3 + x^2 + x + 3)$;
- $n = 7$: $\overline{f} = x^6 + x + 1$.

Auswertung:

- Modulo 7: G_f enthält einen Automorphismus der Ordnung 6, da $[\mathbb{Z}_7[x]/\overline{f}\mathbb{Z}_7[x] : \mathbb{Z}_7] = 6$.
- Es ist $[\mathbb{Z}_3[x]/(x^4 + 2x^3 + 1)\mathbb{Z}_3[x] : \mathbb{Z}_3] = 4$. G_f enthält ein Element der Ordnung 4.

Solche Informationen genügen oft zur vollständigen Bestimmung von G_f.

Weiteres realistisches Verfahren: (vergleiche [Coh03]) Resolventenpolynome $F \in \mathbb{Z}[t_1, \ldots, t_n]$, $U := \{\sigma \in G_f \mid F(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) = F(t_1, \ldots, t_n)\}$. V sei Vertretersystem für G_f Modulo U. Die *Resolvente* ist gegeben durch $R(F, f) := \prod_{\sigma \in V}(x - F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}))$.

- Berechne numerisch annhäherungsweise $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ (Nullstellen von f).
- Berechne damit $R(F, f)$ näherungsweise. Da $R(F, f)$ ganzzahlige Koeffizienten haben muss, kann man unter der Voraussetzung, dass genau genug gerechnet wurde, die Koeffizienten des näherungsweise bestimmten Polynoms runden und erhält das exakte $R(F, f)$.
- Benutze Satz von Soicher!

Wahl von F jeweils speziell für jedes $n \rightarrow$ [Coh03].

Schlussbemerkung zur Galois-Theorie

- vieles erreicht;
- vieles könnte folgen, nicht behandelt wurden unter anderen
  - Umkehrung des Hauptsatzes (Satz 1.2.3.1),
  - allgemeine Diskriminanten,
  - Normen und Spuren,
  - Normalbasis

  und so weiter;
- die Galoistheorie ist ein Herzstück der Mathematik mit prägender Wirkung!
- Ein Beispiel ist die differentielle Galoistheorie.

  Sei $\mathcal{M}_{\mathbb{R}}$ der Körper der reellen meromorphen Funktionen, $\mathbb{C} \subset \mathcal{M}_{\mathbb{R}}$. Zum Beispiel sind sin, cos, exp transzendent über $\mathbb{C}$, und ebenso alle nicht konstanten Polynome. Aber: $(D^2+1)\sin = 0$, also mit $f := D^2+1$ gilt $f(\sin) = \sin'' + \sin = 0$; der Sinus ist also *differentialalgebraisch* über $\mathbb{R}$.

  Beispiel einer differentialtranszendenten Funktion ist die Γ-Funktion.

  Vergleiche Kaplanski, *An Introduction to Differential Algebra* [Kap76] und Magid, *Lectures on Differential Galois Theory* [Mag94].

  Zusatz: Was ist eine transzendente Funktion? Sei

  $$\mathcal{M}_{\mathbb{R}} = \{ \text{ reelle meromorphe Funktionen } \}, \qquad \mathbb{R}[x] \subseteq \mathcal{M}_{\mathbb{R}}$$

  mit $x = \mathbf{id}_{\mathbb{R}}$. Dann heißt $f \in \mathcal{M}_{\mathbb{R}}$ eine *transzendente Funktion*, wenn f transzendent über $\mathbb{R}[x]$ ist. Zum Beispiel sind sin, cos, exp transzendent.

1.2.7 Konstruktion mit Zirkel und Lineal

Literatur: Es gibt unübersehbar viele Darstellungen der Galoistheorie. Alle bisher in der Vorlesung genannten Algebra-Werke enthalten auch Kapitel über Galoistheorie und bei fast allen ist darin ein Abschnitt über Konstruktionen mit Zirkel und Lineal enthalten. Darüber hinaus seien besonders hervorgehoben:

- Josef Rotmann, *Galois Theory* [Rot90];
- Charles Robert Hadlock, *Field Theory and its Classical Problems* [Had78];
- Ian Stewart, *Galois Theory* [Ste73].

Das Buch von Rotman enthält einen sehr lesenswerten (in der 2. Auflage berichtigten) Anhang über "old-fashioned Galois Theory". Eine Besonderheit des Buches von Hadlock ist, dass Sätze stets so elementar wie möglich bewiesen werden und das alle Übungsaufgaben gelöst sind. Lesenswert sind zum Beispiel auch die historischen Bemerkungen bei Stewart, Seite 57ff.

Kurze historische Hinweise finden sich in allen angegebenen Büchern. Ausführlichere finden sich in

- N. Bourbaki, *Elements de Mathematiques, Algebra Ch. 4, 5, Notes historiques* [Bou59],
- B. L. v. d. Waerden, *A history of Algebra* [Wae85].

Vorbemerkungen: Die klassischen Konstruktionsprobleme, um die es im folgenden geht, sind:

- Quadratur des Kreies,
- Rektifikation des Kreisumfanges,
- Würfelverdoppelung,
- Dreiteilung eines Winkels und schließlich die
- Konstruktion eines regelmäßigen n-Eckes.

Das Problem der Würfelverdoppelung wird oft auch Deli'sches Problem genannt; siehe dazu Hadlock S. 2/3.

"Konstruktion" heißt dabei stets Konstruktion mit Zirkel und Lineal. Alle aufgeführten Probleme sind zumindest teilweise unlösbar, wenn man sich strikt an gewisse Konstruktionsregeln (siehe unten) hält. Innerhalb der nach diesen Regeln konstruierten Geometrie wird die Unmöglichkeit gewisser Konstruktionsergebnisse nicht deutlich. Erst die analytisch-algebraische Interpretation der Konstruktion ebnete den Weg zu einer Klärung, indem sie die geometrischen Probleme in algebraische Probleme übersetzte, die im Laufe des 19. Jahrhundert gelöst wurden. Ausnahme dabei ist die Konstruktion eines regelmäßigen n-Eckes, bei der das zugehörige algebraische Problem bis heute noch nicht vollständig gelöst ist (siehe unten).

Die "Übersetzung" der Konstruktionsprobleme in algebraische Probleme ergibt sich mit elementaren Hilfsmitteln der analytischen Geometrie und der Körpertheorie: Der Schwierigkeitsgrad der entstehenden algebraischen Probleme ist recht unterschiedlich:

- die Quadratur des Kreises und die Rektifikation des Kreisumfanges sind äquivalent zur Transzendenz von π;
- die Würfelverdoppelung ist äquivalent zur Bestimmung von $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$;
- die Dreiteilung des Winkels φ ist äquivalent zur Bestimmung von $[\mathbb{Q}(\cos\varphi)(\cos\frac{\varphi}{3}) : \mathbb{Q}(\cos\varphi)]$;
- und die Konstruktion eines regelmäßigen n-Eckes ist äquivalent zur Bestimmung aller Fermat-Primzahlen.

Nur bei dem zuletzt aufgeführten "Übersetzungs"-Problem werden wir die Galoistheorie und insbesondere die Ergebnisse aus Abschnitt 5 einsetzen.

Die zulässigen Konstruktionsschritte: Es geht um Konstruktionen mit Zirkel und Lineal in der Ebene. Letzere fassen wir als $\mathbb{R}^2 = \mathbb{C}$ auf mit dem rechtwinkligen Koordinatensystem, das durch 1 und **i** vorgegeben ist.

Stets ist eine Punktmenge M vorgegeben ($\emptyset \neq M \subset \mathbb{C}$), aus der heraus neue Punkte nach gewissen Regeln konstruiert werden können:

- Mit dem *Lineal* können wir durch je zwei verschiedene Punkte $a, b \in M$ eine Gerade ziehen:

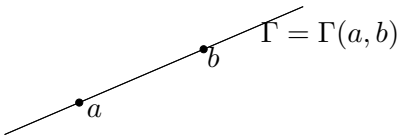


Abbildung 1.1: Konstruktion einer Linie durch zwei Punkte

Diese sei mit $\Gamma(a,b)$ bezeichnet. Es ist $\Gamma(a,b) = \Gamma(b,a)$.

- Mit dem *Zirkel* können wir zu zwei gegebenen verschiedenen Punkten $a, b \in M$ um a herum einen Kreis schlagen mit dem Radius $|b-a|$, der durch b geht:

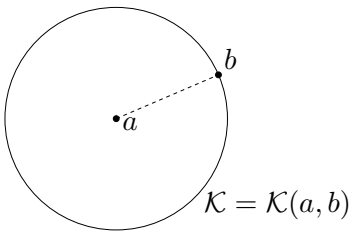


Abbildung 1.2: Konstruktion eines Kreises mit Hilfe von zwei Punkten

Dieser sei mit $\mathcal{K}(a,b)$ bezeichnet. Es gilt im allgemeinen $\mathcal{K}(a,b) \neq \mathcal{K}(b,a)$!

Offensichtlich ist es dabei sinnvoll, $|M| \geq 2$ stets vorauszusetzen. Außerdem wird weiter unten vorausgesetzt, dass $0, 1 \in M$ ist. Dies kann im Fall $|M| \geq 2$ durch einen affinen Koordinatenwechsel erreicht werden.

Definition 1.2.7.1. *Sei $M \subset \mathbb{C}$ mit $|M| \geq 2$.*

(a) *Es heißt $c \in \mathbb{C}$* (in einem Schritt) aus M konstruierbar*, wenn es $a, b, a', b' \in M$ mit $a \neq b$, $a' \neq b'$ gibt so, dass mit $\Gamma = \Gamma(a,b)$, $\Gamma' = \Gamma(a',b')$, $\mathcal{K} = \mathcal{K}(a,b)$, $\mathcal{K}' = \mathcal{K}(a',b')$ gilt*

  (i) *$c \in \Gamma \cap \Gamma'$ und $|\Gamma \cap \Gamma'| = 1$;*
  (ii) *$c \in \Gamma \cap \mathcal{K}$ und $|\Gamma \cap \mathcal{K}| = 2$; oder*
  (iii) *$c \in \mathcal{K} \cap \mathcal{K}'$ und $|\mathcal{K} \cap \mathcal{K}'| = 2$.*

(b) *Seien $M^{(0)} := M$, $M^{(1)} := \{c \in \mathbb{C} \mid c$ aus M in einem Schritt konstruierbar $\}$ und für $r \geq 1$ sei $M^{(r)} := (M^{(r-1)})^{(1)}$ rekursiv definiert, und schließlich*

$$\overset{\circ}{\overline{M}} := \bigcup_{r \geq 0} M^{(r)}.$$

Es heißt c aus M in endlich vielen Schritten konstruierbar*, wenn gilt $c \in \overset{\circ}{\overline{M}}$.*

Beachte dabei: Stets ist $M \subset M^{(1)}$, und deswegen ist $M \subset M^{(1)} \subset M^{(2)} \subset \cdots \subset M^{(r)} \subset \cdots \subset \overset{\circ}{\overline{M}}$ eine aufsteigende Kette.

Beachte weiterhin: Es gilt $c \in \overset{\circ}{\overline{M}}$ genau dann, wenn es ein $r \in \mathbb{N}$ gibt mit $c \in M^{(r)}$. Weiterhin ist selbst im Fall $|M| = 2$ bereits $\left|\overset{\circ}{\overline{M}}\right| = \infty$!

1.2.7.1 Algebraische Beschreibung der Konstruktionsschritte und einige Folgerungen

Die Auffassung der Konstruktionsebene als $\mathbb{R}^2$ oder $\mathbb{C}$ beinhaltet bereits die Zugrundelegung eines rechtwinkligen (cartesischen) Koordinatensystems. Dies ist die Grundlage für die algebraische Formulierung von Konstruktionsproblemen. Geraden und Kreise lassen sich durch Gleichungen beschreiben. Die Punkte in $M^{(1)}$ ergeben sich dann als Lösungen von Gleichungssystemen. Da wir (im Sinne der Algebraisierung) $\mathbb{C}$ dem $\mathbb{R}^2$ vorziehen, ist es dann auch zweckmäßig, Geraden und Kreise im Komplexen zu beschreiben ohne Rückgriff auf die reellen Koordinaten (Real- und Imaginärteil). Dies geschieht im folgenden:

Hilfssatz 1.2.7.2. *Seien $a, b \in \mathbb{C}$ und $a \neq b$.*

(a) *Es ist* $\Gamma(a,b) = \{z \in \mathbb{C} \mid (b-a)\overline{(z-a)} = \overline{(b-a)}(z-a)\}$

(b) *und* $\mathcal{K}(a,b) = \{z \in \mathbb{C} \mid (z-a)\overline{(z-a)} = (b-a)\overline{(b-a)}\}$.

Dabei wurde wie üblich die zu $w \in \mathbb{C}$ konjugierte komplexe Zahl mit $\overline{w}$ bezeichnet.

Beweis.

(a) Sei Δ die rechtsstehende Menge. Man rechnet nach: $\Gamma = \{a + (b-a)t \mid t \in \mathbb{R}\} \subset \Delta$. Umgekehrt gilt für $z \in \Delta$

$$(z-a)(b-a)^{-1} = \overline{(z-a)(b-a)^{-1}},$$

daher gibt es ein $t \in \mathbb{R}$ mit $(z-a) = t(b-a)$. Somit $z \in \Gamma$, bzw. $\Delta \subset \Gamma$.

(b) Ist wohl allgemein bekannt.

□

Sind im Hilfssatz $a, b \in M$, dann sind sowohl $b-a$, $\overline{b-a}$ nicht mehr notwendigerweise in M. Bei der Bestimmung etwa von $\Gamma(a,b) \cap \mathcal{K}(a',b')$ und $a', b' \in M$ treten noch verwickeltere Ausdrücke in a, b, a', b' auf, die im Allgemeinen alle nicht mehr in M liegen. Allerdings liegen sie alle in $\mathbb{Q}(M \cup \overline{M})$ oder in einer Erweiterung vom Grad 2 von $\mathbb{Q}(M \cup \overline{M})$. Unter der zusätzlichen Voraussetzung $0, 1 \in M$ wird sich später noch ergeben, dass $\mathbb{Q}(M \cup \overline{M}) \subset \overline{M}^{\circ}$ gilt (folgt unmittelbar aus Satz 1.2.7.8, siehe unten). Vorläufig spielt dies allerdings noch keine Rolle.

Satz 1.2.7.3. *Sei $c \in M^{(1)}$. Dann ist*

$$[\mathbb{Q}(M \cup \overline{M})(c) : \mathbb{Q}(M \cup \overline{M})] \leq 2.$$

Dabei ist $\overline{M} = \{\overline{z} \mid z \in M\}$.

Bemerkung 1.2.7.4 (Wiederholung). Wenn $\operatorname{Char} K \neq 2$ und $[F : K] = 2$, dann gibt es $\alpha \in F$, $d \in K$ mit $F = K(\alpha)$ und $\alpha^2 = d$ (oder $\alpha =$ "$\sqrt{d}$"). Körpererweiterungen der Dimension ≤ 2, wie sie im Definition 1.2.7.1 auftreten, sind also stets Quadratwurzelerweiterungen (QWE).

Beweis von Satz 1.2.7.3.

(a) Betrachte folgende Zeichnung (Abbildung 1.3):

mit $a \neq b$, $a' \neq b'$ und $a, b, a', b' \in M$. Nach Hilfssatz 1.2.7.2(a) gilt

$$\Gamma = \{z \in \mathbb{C} \mid (b-a)\overline{(z-a)} = \overline{(b-a)}(z-a)\}$$
$$\text{und} \qquad \Gamma' = \{z \in \mathbb{C} \mid (b'-a')\overline{(z-a')} = \overline{(b'-a')}(z-a')\}.$$

Für $z \in \Gamma \cap \Gamma'$ gilt dann

$$\overline{z} = \frac{\overline{b-a}}{b-a}(z-a) + \overline{a} \qquad \text{und} \qquad \overline{z} = \frac{\overline{b'-a'}}{b'-a'}(z-a') + \overline{a'},$$

also $zu = v$ für $u, v \in \mathbb{Q}(M \cup \overline{M})$.

Man sieht: Falls $\Gamma \cap \Gamma' \neq \emptyset$, und $\Gamma \neq \Gamma'$ ist $z \in \mathbb{Q}(M \cup \overline{M})$.

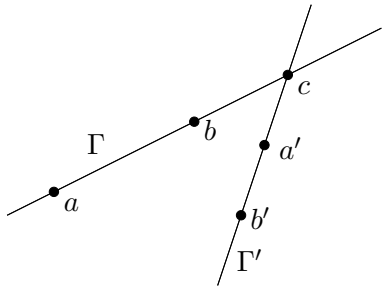


Abbildung 1.3: Skizze zum Beweis von Satz 1.2.7.3, Beweisschritt (a)

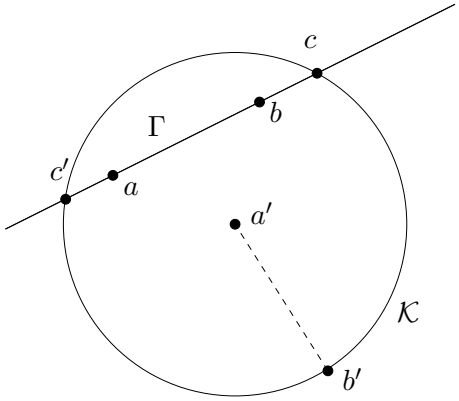


Abbildung 1.4: Skizze zum Beweis von Satz 1.2.7.3, Beweisschritt (b)

(b) Mit Hilfssatz 1.2.7.2(a) und (b) erhält man (Abbildung 1.4):

$$\Gamma = \{z \in \mathbb{C} \mid (b-a)\overline{(z-a)} = \overline{(b-a)}(z-a)\} \qquad (*)$$

$$\text{und} \qquad \mathcal{K} = \{z \in \mathbb{C} \mid (z-a')\overline{(z-a')} = (b'-a')\overline{(b'-a')}\}. \qquad (1.2.7.1)$$

Für $z \in \Gamma \cap \mathcal{K}$ gilt zunächst wieder $\overline{z} = \frac{\overline{b-a}}{b-a}(z-a)+\overline{a}$. Damit kann in $(*)$ $\overline{z}$ eliminiert werden und es ergibt sich eine quadratische Lösung für z über $\mathbb{Q}(M \cup \overline{M})$. Da $b \neq a$ hat diese zwar stets Lösungen, aber die Lösungen führen nicht immer zu Punkten in $\Gamma \cap \mathcal{K}$.

(c) Hier gilt nach Hilfssatz 1.2.7.2(b) (Abbildung 1.5):

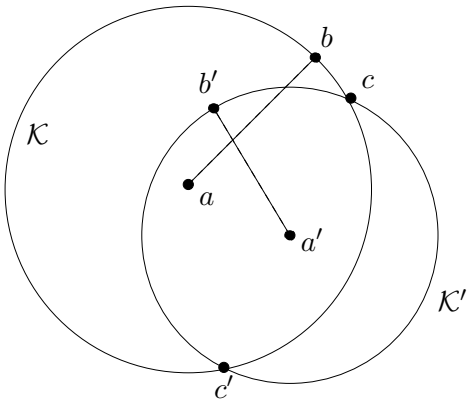


Abbildung 1.5: Skizze zum Beweis von Satz 1.2.7.3, Beweisschritt (c)

Für $z \in \mathcal{K} \cap \mathcal{K}'$ gilt $\overline{z} = \frac{(b-a)\overline{(b-a)}}{z-a} + \overline{a}$ und $\overline{z} = \frac{(b'-a')\overline{(b'-a')}}{z-a'} + \overline{a'}$. Es resultiert wieder eine quadratische Gleichung für z mit Koeffizienten aus $\mathbb{Q}(M \cup \overline{M})$.

□

Beispiel 1.2.7.5 (zu Beweisteil (b)). Sei $a = 0$, $b = \mathbf{i}$, $a' = 2$, $b' = 3$. Dann ist $\Gamma = \{z \in \mathbb{C} \mid \overline{z} = -z\}$ und $\mathcal{K} = \{z \in \mathbb{C} \mid (z-2)(\overline{z}-2) = 1\}$ und die resultierende quadratische Gleichung lautet $z^2 = 3$.

Bemerkung 1.2.7.6. Sei K ein Unterkörper von $\mathbb{C}$ mit $\overline{K} = K$ und sei $c \in \mathbb{C}$. Dann gilt

$$[K(c) : K] = [K(\overline{c}) : K],$$

denn die komplexe Konjugation $\bar{\cdot}$ ist ein Automorphismus von $\mathbb{C}$.

Definition 1.2.7.7. *Sei $K = F_0 \subset F_1 \subset \cdots \subset F_r = F$ ein Körperturm und es gelte $[F_i : F_{i-1}] \leq 2$ für alle $1 \leq i \leq r$, dann heißt F* iterierte Quadratwurzelerweiterung *(kurz: iQWE) von K.*

Als Motivation für diese Definition dient der folgende Satz.

Satz 1.2.7.8. *Sei $K = \mathbb{Q}(M \cup \overline{M})$.*

(a) *Ist $c \in \mathbb{C}$ konstruierbar aus M, dann liegt $K(c)$ in einer iterierten Quadratwurzelerweiterung innerhalb $\mathbb{C}$ von K.*

(b) *Insbesondere ist $[K(c) : K] = 2^m$ mit geeignetem $m \in \mathbb{N}$.*

Für (a) gibt es eine Umkehrung, siehe Satz 1.2.7.12. Aus $[K(c) : K] = 2^m$ folgt jedoch im Allgemeinen nicht die Konstruierbarkeit von c. Für ein Gegenbeispiel siehe J. Rotmann: Galois Theory*, Remark p. 90.*

Beweis. Seien $c_1, \ldots, c_n = c$ die Punkte, die sich jeweils bei den endlich vielen Konstruktionsschritten ergeben. Und zwar c_1 aus $M^{(1)}$ und c_i aus $(M \cup \{c_1, \ldots, c_{i-1}\})^{(1)}$ für $1 < i \leq s$. Wir betrachten folgenden Körperturm:

$$K \subset K(c_1) \subset \underbrace{K(c_1, \overline{c_1})}_{=:K_1} \subset K_1(c_2) \subset \underbrace{K_1(c_2, \overline{c_2})}_{=:K_2} \subset \cdots \subset K_{s-1}(c_s) \subset \underbrace{K_{s-1}(c_s, \overline{c_s})}_{=:K_s} =: F.$$

Wegen Satz 1.2.7.3 und der nachfolgenden Bemerkung 1.2.7.6 ist F eine iterierte Quadratwurzelerweiterung von K. Beachte dabei, dass $K_\nu = \mathbb{Q}(M \cup \{c_1, \ldots, c_\nu\} \cup \overline{M \cup \{c_1, \ldots, c_\nu\}})$ ist. □

Der in den Vorbemerkungen angesprochene "Übersetzungsvorgang" wird durch Satz 1.2.7.8(a) und seine spätere Umkehrung in Satz 1.2.7.12 geleistet:

Es ist c aus M konstruierbar genau dann, wenn $\mathbb{Q}(M \cup \overline{M})(c)$ Teilmenge einer iterierten Quadratwurzelerweiterung von $\mathbb{Q}(M \cup \overline{M})$ ist.

Will man darauf hinaus, dass c nicht konstruierbar ist, genügt schon Satz 1.2.7.8(a): Man versucht zu zeigen, dass c nicht in einem Quadratwurzelturm über $\mathbb{Q}(M \cup \overline{M})$ liegen kann.

Auch ohne die Umkehrung von Satz 1.2.7.8(a) lassen sich daher die oben angegebenen klassischen Konstruktionsprobleme schon weitgehend klären.

(a) **Quadratur des Kreises:** Gegeben $M = \{0, 1\} = \overline{M}$, also $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Zu konstruieren: $c = \frac{\sqrt{\pi}}{2}$.

Da $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] = 2$ und $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ wegen der Transzendenz von π[8] ist $[\mathbb{Q}(c) : \mathbb{Q}] = \infty$. Also kann $\mathbb{Q}(c)$ nicht in einer iterierten Quadratwurzelerweiterung von $\mathbb{Q}$ liegen. Wegen Satz 1.2.7.8 ist c nicht konstruierbar.

(b) **Rektifikation des Kreisumfanges:** Gegeben $M = \{0, \mathbf{i}\}$, zu konstruieren ist $c = 2\pi$. Vorgehen analog zu (a) liefert das Ergebnis: c ist nicht konstruierbar.

(c) **Würfelverdoppelung:** Gegeben ist $M = \{0, 1\}$, und zu konstruieren ist $c = \sqrt[3]{2}$. Da $[\mathbb{Q}(c) : \mathbb{Q}] = 3$ ist c nach Satz 1.2.7.8 nicht konstruierbar.

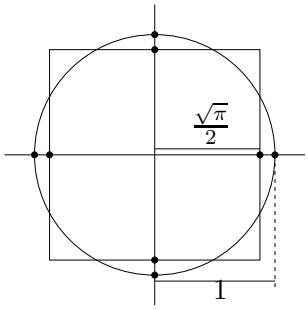


Abbildung 1.6: Quadratur des Kreises

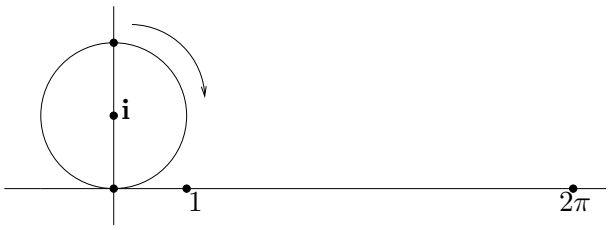


Abbildung 1.7: Rektifikation des Kreisumfanges

(d) **Dreiteilung des Winkels φ:** Gegeben ist $\{0, 1, a\}$. Zu konstruieren ist irgendein Punkt $b \neq 0$ auf Γ (siehe Abbildung 1.9). Offensichtlich ist ein solcher Punkt b genau dann konstruierbar aus $\{0, 1, a\}$, wenn $\cos\frac{\varphi}{3}$ aus $M = \{0, 1, \cos\varphi\}$ konstruierbar ist.

Für gewisse φ ist eine Konstruktion möglich, zum Beispiel für $\varphi = 90$ Grad. Wegen Satz 1.2.7.8 untersuchen wir an Stelle des geometrischen Problems die Körpererweiterung $F = K(\cos\frac{\varphi}{3})$ mit $K = \mathbb{Q}(\cos\varphi)$. Ist $[F : K]$ ungerade, ergibt sich die Unmöglichkeit einer Konstruktion für den gegebenen Winkel φ.

Aus der Beziehung

$$\cos\varphi + \mathbf{i}\sin\varphi = e^{\mathbf{i}\varphi} = \left(e^{\mathbf{i}\frac{\varphi}{3}}\right)^3 = \left(\cos\tfrac{\varphi}{3} + \mathbf{i}\sin\tfrac{\varphi}{3}\right)^3$$

erhält man eine Gleichung für $\alpha = 2\cos\frac{\varphi}{3}$ über K:

$$\left(2\cos\frac{\varphi}{3}\right)^3 - 3\left(2\cos\frac{\varphi}{3}\right) - 2\cos\varphi = 0$$

bzw. $\alpha^3 - 3\alpha - 2\cos\varphi = 0$.

Behauptung: Für $\varphi = 60$ Grad ist $\cos\frac{\varphi}{3} = \cos 20$ Grad nicht konstruierbar.

Beweis: Dann ist $\cos\varphi = \frac{1}{2}$ und $f = x^3 - 3x^2 - 1$ hat $2\alpha = 2\cos 20$ Grad als Nullstelle. Es ist $f \in \mathbb{Z}[x]$ mit $LK(f) = 1$. Dann müssen alle rationalen Nulsltellen ganz sein und den konstanten Term -1 teilen. Da $f(1) \neq 0 \neq f(-1)$ hat f keine rationalen Nullstellen und ist somit als Polynom vom Grad 3 unzerlegbar über $K = \mathbb{Q}(\cos 60\text{ Grad}) = \mathbb{Q}(\frac{1}{2}) = \mathbb{Q}$. Es folgt $[F : K] = 3$ und mit Satz 1.2.7.8 die Behauptung. □

Wie wir gesehen haben, führt die Einführung von Koordinaten und die algebraische Beschreibung (analytische Geometrie) zu einer "Trivialisierung" der betrachteten Konstruktionsprobleme. Das folgende Konstruktionsproblem ist auch auf der algebraischen Seite noch nicht gelöst:

Problem: Für welche n ist die Konstruktion der Eckpunkte eines regelmäßigen n-Eckes aus $M = \{0, 1\}$ mit Zirkel und Lineal möglich?

Unser bisheriger Wissenstand erlaubt immerhin eine folgende Teilaussage, für die wir folgende Definition benötigen:

[8] Satz von Lindemann 1882 zitiert nach Ebbinghaus et al, *Zahlen*, 2. Auflage 1988, Seite 124.

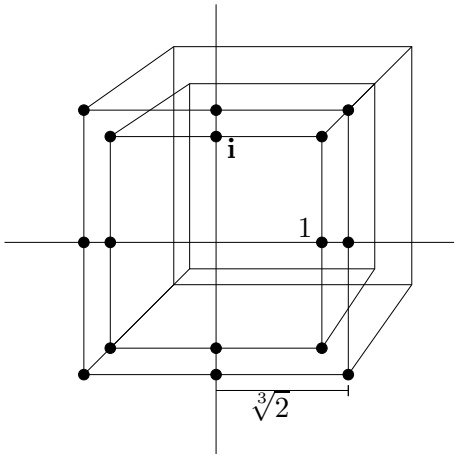


Abbildung 1.8: Würfelverdoppelung

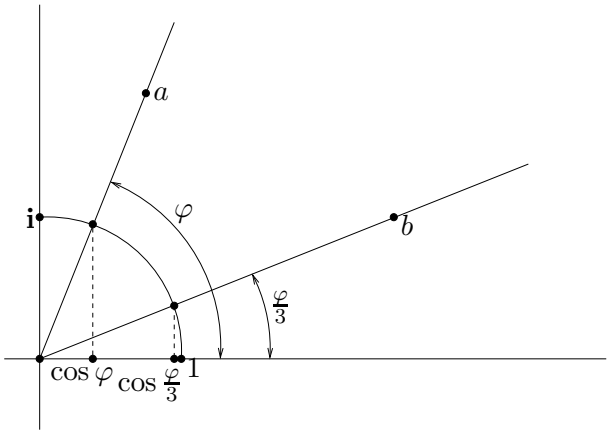


Abbildung 1.9: Dreiteilung des Winkels φ

Definition 1.2.7.9. *Eine Primzahl p heißt* Fermat-Primzahl*, wenn $p = 2^{2^t} + 1$ mit $t \in \mathbb{N}$.*

Bisher sind nur die Fermat-Primzahlen $p = 3,\ 5,\ 17,\ 257$ und 65537 bekannt ($t = 0, \ldots, 4$).

Satz 1.2.7.10. *Sei $n \geq 3$. Wenn das regelmäßige n-Eck aus $\{0,1\}$ durch Zirkel und Lineal konstruierbar ist, dann ist entweder $n = 2^k$ mit $k \geq 2$ oder $n = 2^k p_1 \cdots p_r$ mit paarweise verschiedenen Fermat-Primzahlen $p_1, \ldots, p_r$ und $k \geq 0$.*

Beweis.

(a) Das regelmäßige n-Eck ist konstruierbar genau dann, wenn $\zeta_n := e^{\frac{2\pi \mathbf{i}}{n}}$ konstruierbar ist (jeweils aus $\{0,1\}$).

(b) Wenn ζ_n konstruierbar ist, dann auch ζ_m für alle Teiler m von n, denn $\zeta_n^{\frac{n}{m}} = \zeta_m$.

(c) Wenn ζ_n konstruierbar ist, p prim, $p \neq 2$ und $p \mid n$, dann ist $p = p^{2^t} + 1$, *denn:*

Da $M = \{0,1\}$ ist hier $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist $x^{p-1} + \cdots + x + 1$. Daher ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Wegen Satz 1.2.7.8(b) muss dann gelten $p - 1 = 2^m$, m geeignet. Erstaunlicherweise muss nun zwangsläufig auch m einer Zweierpotenz sein. Denn wäre $q > 2$ ein ungerader Teiler von m mit $m = rq$, so würde gelten

$$\begin{aligned} -p = & -2^m - 1 = -(2^{rq}) - 1 \underset{q \text{ ungerade}}{=} (-2^r)^q - 1 \\ = & \underbrace{((-2^r) - 1)}_{\substack{\neq \pm 1 \\ < p}} \underbrace{((-2^r)^{q-1} + \cdots + (-2^r) + 1)}_{\neq \pm 1}. \end{aligned}$$

(d) Ist p eine ungerade Primzahl mit $p \mid n$ und ist ζ_n konstruierbar, dann gilt nicht $p^2 \mid n$, *denn:* Angenommen, es gelte $p^2 \mid n$. Wegen (b) ist dann ζ_{p^2} konstruierbar. Nun ist ζ_{p^2} Nullstelle von $\frac{x^{p^2}-1}{x^p-1} = \frac{(x^p)^p-1}{x^p-1} = (x^p)^{p-1} + \cdots + (x^p) + 1 = f$. Nun ist f unzerlegbar in $\mathbb{Q}[x]$ (mit $x := u + 1$ und Eisenstein; vergleiche Teil Einführung in die Algebra). Da $\deg f = p(p-1)$ folgt $p \mid [\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}]$ im Widerspruch zu Satz 1.2.7.8(b).

□

Nun möchte man natürlich gerne noch wissen, ob zumindst für die oben angegebenen Fermat-Primzahlen ζ_p auch wirklich konstruierbar ist. Die Vorgabe einer Konstruktion ist eine Möglichkeit, das Problem zu lösen (bis $n = 17$ schon Gauß bekannt; interessante historische Hinweise für $n = 257$ und $n = 65537$ in [FS83, S. 211] und in [Had78, p. 119]). Auf Gauß geht auch die Umkehrung von Satz 1.2.7.10 zurück. Zu ihrer Herleitung benötigen wir eine Umkehrung von Satz 1.2.7.8(a). Diese wird sich unmittelbar aus folgender detaillierten Beschreibung von $\overline{M}^\circ$ ergeben, die auch für sich interessant ist.

Satz 1.2.7.11. *Seien* $0, 1 \in M$.

(a) *Es ist* $\overline{M}^\circ$ *ein Unterkörper von* $\mathbb{C}$.

(b) *Mit dem Körper* $W = \overline{M}^\circ \cap \mathbb{R}$ *gilt* $\overline{M}^\circ = W + \mathbf{i}W$.

(c) *Es ist* $\overline{M}^\circ$ *algebraisch über* $\mathbb{Q}(M)$.

(d) *Der Körper* $\overline{M}^\circ$ *besitzt keine Körpererweiterung der Dimension 2; kurz:* $\overline{M}^\circ$ *ist quadratisch abgeschlossen.*

(e) *Der Körper* $\overline{M}^\circ$ *ist der kleinste Unterkörper von* $\mathbb{C}$*, der* M *enthält und quadratisch abgeschlossen ist.*

(f) *Es ist* $\overline{M}^\circ = \bigcup\{F \mid F \text{ ist iterierte Quadratwurzelerweiterung von } \mathbb{Q}(M) \text{ in } \mathbb{C}\}$.

Der Beweis folgt am Ende des Abschnittes.

Die angekündigte Umkehrung von Staz 1.2.7.8(a) ergibt sich nun unmittelbar aus Satz 1.2.7.11(a) und (d) oder (f):

Satz 1.2.7.12. *Ist* F *eine iterierte Quadratwurzelerweiterung von* $\mathbb{Q}(M)$ *innerhalb* $\mathbb{C}$ *und* $c \in F$*, dann ist* $c \in \overline{M}^\circ$ *(d. h.* c *ist konstruierbar).*

Beweis. Da $M \subset \overline{M}^\circ$ und da $\overline{M}^\circ$ Unterkörper von $\mathbb{C}$ (Satz 1.2.7.11(a)) ist, gilt $\mathbb{Q}(M) \subset \overline{M}^\circ$. Wegen Satz 1.2.7.11(d) oder (f) folgt nun sofort $F \subset \overline{M}^\circ$. □

Bemerkung 1.2.7.13. Satz 1.2.7.11(b) besagt insbesondere $\mathbf{i} \in \overline{M}^\circ$ und $\overline{c}$, $\Re c$, $\Im c \in \overline{M}^\circ$ falls $c \in \overline{M}^\circ$.

Mit Hilfe von Satz 1.2.7.12 erhalten wir Umkehrung von Satz 1.2.7.10:

Satz 1.2.7.14. *Sei* $n = 2^k$ *mit* $k \geq 2$ *oder* $n = 2^k p_1 \cdots p_r$ *mit* $k \geq 0$ *und mit paarweise verschiedenen Fermatprimzahlen* $p_1, \ldots, p_r$*. Dann ist* ζ_n *konstruierbar.*

Bemerkung 1.2.7.15. Die Sätze 1.2.7.10 und 1.2.7.14 liefern eine vollständige Charakterisierung derjenigen n, für die ζ_n konstruierbar ist. Zugleich entsteht aber ein neues, zahlentheoretisches Problem: "Bestimme alle Fermat-Primzahlen." Letzteres ist bislang ungelöst. Immerhin wissen wir genau für welche $n \leq 65537$ (letzte bekannte Fermatprimzahlen) ζ_n konstruierbar ist, nämlich für

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, \ldots$$

Beweis von Satz 1.2.7.14.

(a) Ist $n = 2^k$, dann ist ζ_n offensichtlich konstruierbar.

(b) Sei $n = p$, p eine Fermat-Primzahl. Das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist $x^{p-1}+\cdots+x+1$. Daher ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 = 2^{2^t}$, $t \geq 0$ geeignet. Da $x^{p-1} + \cdots + x + 1 = \prod_{i=1}^{p-1}(x - \zeta_p^i)$ ist $\mathbb{Q}(\zeta_p)$ Zerfällungskörper über K, also galois'sch über K, da ja $\operatorname{Char}\mathbb{Q} = 0$. Sei $G = \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$. Dann ist $|G| = p - 1 = 2^{2^t}$.

Der erste Sylow'sche Satz (siehe [Jac85, S. 78]) besagt insbesondere, dass eine Gruppe der Ordnung 2^m stets eine Untergruppe der Ordnung 2^{m-1} enthält. Diese ist zwangsläufig ein Normalteiler (zur Übung für den Leser)!

Mit Induktion ergibt sich daher, das G auflösbar ist, und zwar genauer, dass es eine Normalteilerkette

$$\langle 1\rangle = G_r \trianglelefteq \cdots \trianglelefteq G_0 = G$$

und $|G_i/G_{i+1}| = [G_i : G_{i+1}] = 2$ gibt. Dem entspricht ein Körperturm

$$\mathbb{Q} \subset F_0 \subset \cdots \subset F_r = \mathbb{Q}(\zeta_p)$$

mit $[F_{i+1} : F_i] = 2$. Mit Satz 1.2.7.12 ist daher $\zeta_p \in \overline{\overset{\circ}{\{0,1\}}}$, bzw. konstruierbar aus $\{0, 1\}$.

(c) Seien $u, v \in \mathbb{N}_{>0}$, $\operatorname{ggT}(u, v) \in \mathbb{Z}^*$ (also u, v teilerfremd) und seien ζ_u, ζ_v konstruierbar. Dann ist auch ζ_{uv} konstruierbar, *denn:*

Es gibt u', v' derart, dass $uv' + vu' = 1$ und es ist dann

$$(\zeta_u)^{u'}(\zeta_v)^{v'} = e^{(\frac{u'}{u}+\frac{v'}{v})2\pi\mathbf{i}} = e^{\frac{2\pi\mathbf{i}}{uv}} = \zeta_{uv}.$$

Da $\zeta_u, \zeta_v \in \overline{\overset{\circ}{\{0,1\}}}$ ist nun nach Satz 1.2.7.11(a) auch $\zeta_{uv} \in \overline{\overset{\circ}{\{0,1\}}}$, oder, wenn man Satz 1.2.7.11 nicht benutzen will:

Nach Satz 1.2.7.8(a) sind $\mathbb{Q}(\zeta_u)$ und $\mathbb{Q}(\zeta_v)$ jeweils in einer iterierten Quadratwurzelerweiterung von $\mathbb{Q}$ innerhalb $\mathbb{C}$ enthalten ,daher auch $\mathbb{Q}(\zeta_u) \vee \mathbb{Q}(\zeta_v)$ (zur Übung für den Leser).

□

Literaturhinweis: Ein Quadratwurzelausdruck für ζ_{17} wird ausführlich bei F. Bachmann, *Algebra* (1990) hergeleitet (Seite 186ff). Dort gibt es weitere Hinweise auf Seite 189. Die folgende Formeln für ζ_{17} ist diesem Buch entnommen:

$$\zeta_{17} = \tfrac{1}{2}S + \mathbf{i}\sqrt{1 - (\tfrac{1}{2}S)^2}$$

mit

$$S = (\zeta_{17} + \zeta_{17}^{-1}) = \frac{-1+\sqrt{17}}{8} + \frac{-1+\sqrt{17}}{16}\sqrt{\frac{17+\sqrt{17}}{2}} + \tfrac{1}{4}\sqrt{17 + 3\sqrt{17} - \frac{7+\sqrt{17}}{2}\sqrt{\frac{17+\sqrt{17}}{2}}}.$$

Offensichtlich ist $0 \leq S \leq 2$, da $|\zeta_{17}| = 1$.

Es bleibt noch der Beweis von Satz 1.2.7.11 nachzutragen:

Beweis zu Satz 1.2.7.11. Die folgenden neun Aussagen lassen sich alle durch Angabe einfacher Konstruktionen beweisen. Sofern diese nicht offensichtlich sind, werden sie kurz angedeutet. Satz 1.2.7.11 ergibt sich dann unmittelbar aus (1)–(9).

(1) $\mathbf{i} \in \overline{\overset{\circ}{M}}$;

(2) $a_1 + \mathbf{i}a_2 \in \overline{\overset{\circ}{M}}$ impliziert $a_1, a_2 \in \overline{\overset{\circ}{M}}$;

(3) $a_1 + \mathbf{i}a_2 \in \overset{\circ}{\overline{M}}$ impliziert $a_2 + \mathbf{i}a_1, a_1 - \mathbf{i}a_2 \in \overset{\circ}{\overline{M}}$;

(4) $a_1, a_2 \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$ impliziert $a_1 + \mathbf{i}a_2 \in \overset{\circ}{\overline{M}}$;

(5) $a, b \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$ impliziert $a + b \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$;

(6) $a, b \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$ impliziert $a \cdot b \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$, *denn:*

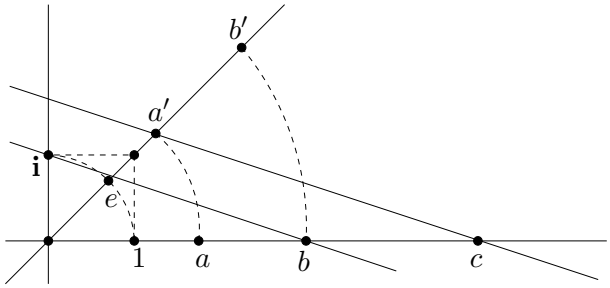


Abbildung 1.10: Skizze zu Schritt (6) im Beweis von Satz 1.2.7.11

Siehe Abbildung 1.10. Es ist $c = ab$ aufgrund des Strahlensatzes.

(7) $0 \neq a \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$ impliziert $a^{-1} \in \overline{M} \cap \mathbb{R}$, *denn:*

Ziehe in obiger Figur die Gerade $\Gamma(1, a')$ und konstruiere dann die Parallele durch e. Diese schneidet die reelle Achse in a^{-1} (Strahlensatz).

(8) $0 < a \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$ impliziert $\sqrt{a} \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$, *denn:*

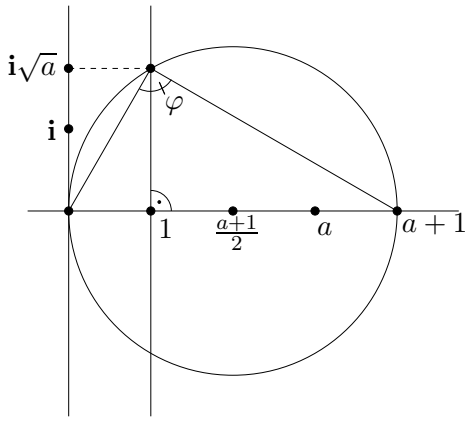


Abbildung 1.11: Skizze zu Schritt (8) im Beweis von Satz 1.2.7.11

Siehe Abbildung 1.11. Aufgrund des Höhensatzes[9] ist $\mathbf{i}\sqrt{a}$ konstruierbar und damit auch $\sqrt{a}$.

(9) $a, b \in \overset{\circ}{\overline{M}}$ impliziert $a + b, a \cdot b \in \overset{\circ}{\overline{M}}$ und $0 \neq a \in \overset{\circ}{\overline{M}}$ impliziert $a^{-1}, \sqrt{a} \in \overset{\circ}{\overline{M}}$.

Beachte dabei: mit $a = re^{\mathbf{i}\varphi}$, $b = se^{\mathbf{i}\psi}$ ist $ab = rse^{\mathbf{i}(\varphi+\psi)}$ und $\sqrt{a} = \sqrt{r}e^{\frac{\mathbf{i}\varphi}{2}}$, und außerdem $a^{-1} = \frac{\overline{a}}{a\overline{a}}$ und $a\overline{a} \in \mathbb{R}$.

□

Schlussbemerkung: Das klassische Thema "Konstruierbarkeit mit Zirkel und Lineal" kann man als abgeschlossen ansehen. Allerdings stellt Satz 1.2.7.14 einen Zusammenhang her zu einem bisher ungelösten Problem der Zahlentheorie. Ganz anders sieht es aus, wenn man andere

[9] Es gilt $h^2 = pq$ in 

.

Konstruktionstechniken zulässt. Ein Beispiel hierfür ist die gut lesbare Arbeit *Constructions Using Conics* von Eric Bainville und Bernard Genèves [BG00]. Dort werden unter anderem schöne Konstruktionen für regelmäßige n-Ecke angegeben. Dabei wird sowohl MAPLE als auch die Cabri-Geometrie-Software benutzt.

Kapitel 2

Einige Grundlagen zur Theorie algebraischer Gleichungen in mehreren Variablen

2.0 Vorbemerkungen

Im Kapitel 1 wurden möglichst kleine Körper untersucht, welche die Koeffizienten von f enthalten, und möglichst kleine Körper, welche die Nullstellen von f enthalten. Solche Körper werden betrachtet, um f zu verstehen.

In Kapitel 2 sind $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ gegeben. Es geht um das Beschreiben von

$$V = \{v \in K^n \mid f_i(v) = 0 \text{ für alle } i = 1, \dots, r\}.$$

Ist zum Beispiel $f = x_1 + x_2 \in \mathbb{Q}[x_1, x_2]$, so ist $f(-\pi, \pi) = 0$, also $\pi \in V$.

Nicht nur der Körper der Koeffizienten bestimmt die algebraische Qualität der Lösungen!

- Fall $n = 1$: Ist $f \in \mathbb{Q}[x] \setminus \mathbb{Q}$ unzerlegbar, $V = \{\alpha \in \mathbb{C} \mid f(\alpha) = 0\}$. Dann ist $\{g \in \mathbb{Q}[x] \mid g|_V \equiv 0\} = f\mathbb{Q}[x]$.
- Im Fall $n \geq 2$ mit $f_1, \dots, f_r \in \mathbb{Q}[x_1, \dots, x_n]$, $V = \{v \in \mathbb{C}^n \mid f_i(v) = 0, i = 1, \dots, r\}$ ist $\{g \in \mathbb{Q}[x_1, \dots, x_n] \mid g|_V \equiv 0\}$ nicht so einfach zu bestimmen.

Zur inhaltlichen Orientierung:

Beispiele 2.0.0.16. für das Auftreten algebraischer Gleichungssysteme und Ausdrücke:

(a) Es ist $F_k(x_1, \dots, x_r, f_1(x_1, \dots, x_r), \dots, f_s(x_1, \dots, x_r)) = 0$ (mit F polynomial), $k = 1, 2, \dots$.
Zum Beispiel $f_1(x_1, \dots) = e^{x_1^2 + x_2^2}$, $f_2(x_1, \dots) = \sin x_3$, ...
Finde "möglichst einfache" und "äquivalente" Ausdrücke $G_1, \dots, G_n$.

(b) Lokale Optima: $F(x_1, \dots, x_r, f_1, \dots, f_s)$ polynomial, $(\frac{\partial F}{\partial x_1}, \dots, \frac{\partial F}{\partial x_1}) = 0$.
Zum Beispiel $F = x^2y^2 + y^2z^2 + z^2x^2 \in \mathbb{R}[x, y, z]$.

Aufgaben: Manipulation, Vereinfachung:

- Systematische Schreibweisen.
- Endliche Darstellung.
- Einfache, "schöne" Darstellung.
- Rechenverfahren, Lösen.
- Wann ist die Lösungsmenge endlich?

2.1 Polynome und Monomordnungen

2.1.1 Vorbetrachtungen

Wie schreibe ich ein Polynom in mehreren Variablen auf? Was soll der Leitterm sein?
Fall $n = 2$: $f = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j$ (der Ausdruck $x^i y^j$ wird *Monom* genannt).
Schöne Veranschaulichung:

Beispiel 2.1.1.1. Sei $f = 2y + xy - x^2 + 5x^3y + x^2y^3 - 8x^4y^4 + x^2y^5 - 11y^3 \in \mathbb{Q}[x, y]$. Betrachte Abbildung 2.1.

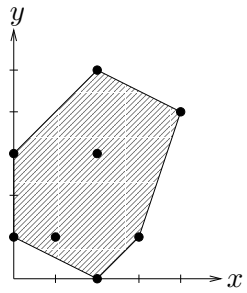


Abbildung 2.1: Das Newtonpolytop eines Polynoms $f \in \mathbb{Q}[x, y]$

Die konvexe Hülle der Punkte im Koordinatensystem wird als *Newtonpolytop* von f bezeichnet, kurz $\mathrm{New}(f)$.

Was soll der Leitterm sein? (Bezeichnung $LT(P)$.) Es soll gelten $LT(f \cdot g) = LT(f) \cdot LT(g)$.

Beispiel 2.1.1.2. Betrachte $f = xy + x^2y + y^2x \in \mathbb{Q}[x, y]$ und $g = x^3 + x^5y + x^4y^2 \in \mathbb{Q}[x, y]$, siehe Abbildung 2.2. Es ist $fg = x^4y + x^5y + x^4y^2 + x^5y^3 + x^6y^2 + x^5y^4 + 2x^6y^3 + x^7y^2 \in \mathbb{Q}[x, y]$.

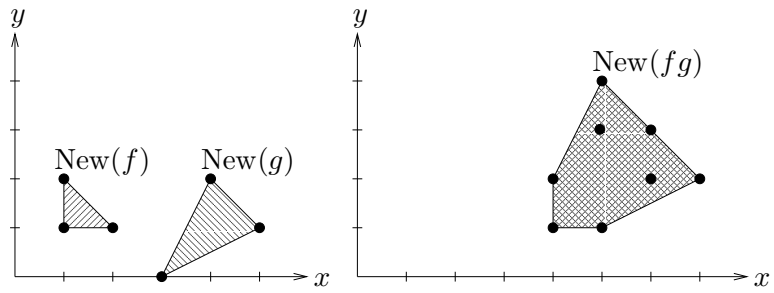


Abbildung 2.2: Die Newtonpolytope zweier Polynome $f, g \in \mathbb{Q}[x, y]$ und das des Produktes fg

2.1.2 Definition und wichtigste Eigenschaften von Monomordnungen

Wir betrachten $K[x_1, \ldots, x_n]$ in den Unbestimmten $x_1, \ldots, x_n$. Diesen bezeichnen wir von nun an kurz als $K[x]$ mit $x = (x_1, \ldots, x_n)$, und mit $\alpha = (i_1, \ldots, i_n) \in \mathbb{N}^n$ schreiben wir x^α für $x_1^{i_1} \cdots x_n^{i_n}$. Damit schreiben sich Polynome $f \in K[x]$ als

$$f = \sum_{\alpha \in \mathbb{N}^n}{}' a_\alpha x^\alpha = \sum_{i=1}^{n} a_{\alpha^{(i)}} x^{\alpha^{(i)}}.$$

Definition 2.1.2.1. *Zu $\alpha \in \mathbb{N}^n$ heißt x^α* Monom *(in $K[x]$). Insbesondere ist $1 = x^0$ und $x_i = x^{e_i}$, $i = 1, \ldots, n$. Bezeichne $|\alpha| := \sum_{i=1}^{n} \alpha_i$ für $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ als den* totalen Grad *oder* Gesamtgrad *von x^α.*

Beobachtung 2.1.2.2.

(a) Die Menge der Monome in $K[x]$ ist ein multiplikativer Untermonoid des multiplikativen Monoiden $K[x]$.

(b) Die Abbildung $\alpha \mapsto x^\alpha$ von $(\mathbb{N}, +)$ nach $(\{ \text{ Monome } \}, \cdot)$ ist ein Monoidisomorphismus.

(c) In $K[x]$ gilt mit $\alpha, \beta \in \mathbb{N}^n$:

$$x^\alpha \mid x^\beta \iff \forall i \in \{1, \dots, n\} : \alpha_i \leq \beta_i \iff \exists \gamma \in \mathbb{N}^n : \alpha + \gamma = \beta \iff \forall \gamma \in \{-\alpha + \mathbb{N}^n\} : x^{\alpha+\gamma} \mid x^{\beta+\gamma}.$$

(d) Für alle $\alpha, \beta, \gamma \in \mathbb{N}^n$ gilt $x^\alpha \mid x^\beta \Leftrightarrow x^{\alpha+\gamma} \mid x^{\beta+\gamma}$.

Beweis. Zur Übung. □

Beispiel 2.1.2.2A. Sei $f = x^r y^s z^t$ und $g = x^{r'} y^{s'} z^{t'}$. Dann gilt $f \mid g$ genau dann, wenn $r \leq r'$, $s \leq s'$ und $t \leq t'$.

Beachte: Bei (b) wird für die Injektivität benötigt, dass Monome K-linear unabhängig bzw. $x_1, \dots, x_n$ algebraisch unabhängig über K sind.

Definition 2.1.2.3. *Eine Menge M heißt (*teilweise, partiell, schwach*)* geordnet*, wenn es eine Relation $\leq$ auf M gibt mit*

(i) $\forall a \in M : a \leq a$ *($\leq$ ist reflexiv);*

(ii) $\forall a, b, c \in M : a \leq b \wedge b \leq c \Rightarrow a \leq c$ *($\leq$ ist transitiv);*

(iii) $\forall a, b \in M : a \leq b \wedge b \leq a \Rightarrow a = b$ *($\leq$ ist antisymmetrisch).*

Ist $\leq$ eine Ordnung, so schreiben wir $a \geq b$ wenn $b \leq a$, $a < b$ wenn $a \leq b$ und $a \neq b$ und $a > b$ analog für $a, b \in M$.

Beispiele 2.1.2.4.

(a) Natürliche Anordnung von $\mathbb{N}^n$:

$$\alpha \leq_0 \beta :\Leftrightarrow \forall i \in \{1, \dots, n\} : \alpha_i \leq \beta_i.$$

(b) Sei $A \in \mathbb{R}^{d \times n}$ und setze $\alpha \leq_A \beta :\Leftrightarrow A\alpha \leq_0 A\beta$ für $\alpha, \beta \in \mathbb{R}^n$. Dann ist $\leq_A$ eine Ordnung auf $\mathbb{R}^n$ genau dann, wenn $\operatorname{rang} A = n$. (Spezialfall $A = E_n$, dann ist $\leq_A = \leq_0$.)

Es gilt stets: $\alpha \leq_A \beta \Leftrightarrow \alpha + \gamma \leq_A \beta + \gamma$.

Frage: Wann gilt $\forall \alpha \in \mathbb{N}^n : 0 \leq_A \alpha$? (Übung: alle Einträge von A sind nicht-negativ.) Leider ist $\leq_0$ nicht linear für $n \geq 2$.

Definition 2.1.2.5. *Es sei M bezüglich $\leq$ geordnet.*

(a) *Die Ordnungsrelation $\leq$ heißt* totale *oder* lineare Ordnung *auf M, falls zusätzlich gilt $\forall a, b \in M : a \leq b \vee b \leq a$.*

(b) *Eine lineare Ordnung $\leq$ auf M heißt* Wohlordnung auf M*, wenn jede nichtleere Teilmenge ein kleinstes Element enthält.*

Beispiele 2.1.2.6.

(a) Die Ordnung $\leq_0$ auf $\mathbb{N}$ ist keine totale Ordnung.

(b) Betrachte die Ordnung $\mathbb{N}^2$ in Abbildung 2.3. Diese Ordnung ist eine Wohlordnung.

(Analog für andere abzählbare Mengen.)

(c) Wohlordnungssatz (äquivalent zum Auswahlaxiom): Auf jeder Menge gibt es eine Wohlordnung.

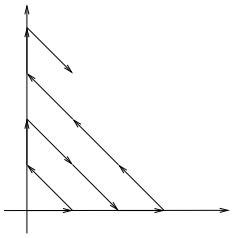


Abbildung 2.3: Eine Wohlordnung auf $\mathbb{N}^2$

Definition 2.1.2.7. *Die Ordnung $\leq$ auf $\mathbb{N}^n$ heißt* verträglich*, wenn für alle $\alpha, \beta, \gamma \in \mathbb{N}^n$ gilt $\alpha \leq \beta \Leftrightarrow \alpha + \gamma \leq \beta + \gamma$.*

Beispiel 2.1.2.7A. Die Ordnungen $\leq_0$ und $\leq_A$ sind mit $+$ auf $\mathbb{N}^n$ verträglich.

Satz 2.1.2.8. *Sei $\leq$ eine lineare mit $+$ verträgliche Ordnung. Dann ist $\leq$ genau dann eine Wohlordnung, wenn gilt $\forall \alpha \in \mathbb{N}^n : 0 \leq \alpha$.*

Beweis. **"$\Rightarrow$":** Sei $W = \{\alpha \in \mathbb{N}^n \mid \alpha < 0\}$ und sei $W \neq \emptyset$. Sei $\alpha_W \in W$ minimal. Dann gilt $\mathbb{N}^n \ni \alpha_W + \alpha_W < \alpha_W < 0$, Widerspruch zur Minimalität.
"$\Leftarrow$": Sei $W \subseteq \mathbb{N}^n$, $W \neq \emptyset$. Sei $\alpha \in W$ und $C_\alpha^+ := \{\beta \in \mathbb{N}^n \mid \alpha \leq_0 \beta\}$. Sei $\beta \in \mathbb{N}^n$. Dann gilt $\beta < \alpha \Rightarrow \beta \notin C_\alpha^+$, denn sonst wäre $\beta - \alpha \in \mathbb{N}^n$ und $0 \leq \beta - \alpha$, also $\alpha \leq \beta$, Widerspruch.

Daher ist folgende Konstruktion möglich:

Wähle $\alpha \in W$. Ist α minimal, so sind wir fertig. Sonst gibt es ein $\beta \in W$ mit $\beta < \alpha$; dann ist $\beta \notin C_\alpha^+$. Ist nun β minimal, so sind wir fertig. Ansonsten gibt es ein $\gamma \in W$ mit $\gamma < \beta$ und $\gamma \notin C_\alpha^+ \cup C_\beta^+$.

Nach endlich vielen Schritten bricht das Verfahren wegen folgendem Satz ab: □

Satz 2.1.2.9. *Sei $\mathcal{P}^+ := \{W \subseteq \mathbb{N}^n \mid \forall \alpha \in W : C_\alpha^+ \subseteq W\}$. Dann gilt*

(a) *$\mathcal{P}^+$ ist noethersch bezüglich $\subseteq$, d. h. alle aufsteigenden Ketten brechen ab.*

(b) *Jede nichtleere Menge aus $\mathcal{P}^+$ besitzt nur endlich viele Minima (bezüglich $\leq_0$).*

Weiterhin sind die Aussagen (a) und (b) äquivalent.

Beweis. Der Teil "(a) $\Leftrightarrow$ (b)" ist zur Übung.

Zum Beweis von (b): Sei $\emptyset \subseteq W \subseteq \mathcal{P}^+$ und sei $A = \{\alpha \in W \mid \alpha \text{ minimal bezüglich } \leq_0\}$. Annahme: A nicht endlich.

Dann gibt es eine injektive Folge $(a^k)_k$ von Minima aus A mit $a^k = (a_1^k, \ldots, a_n^k)$. In dieser Folge gibt es nun eine Teilfolge mit schwach monotonen ersten Komponenten, d. h. es gibt streng monoton steigende $k_i \in \mathbb{N}$ so, dass $(a_1^{k_i})_i$ monoton steigend ist. Von der Teilfolge $(a_1^{k_i})_i$ gibt es wiederum eine Teilfolge mit schwach monotonen zweiten Komponenten, etc. So erhält man schließlich (nach n Schritten) eine Teilfolge von $(a^k)_k$, die in allen Komponenten schwach monoton steigend ist. Damit ist aber $\{a^k \mid k \in \mathbb{N}\}$ total geordnet, Widerspruch. □

Der Satz wird später noch benutzt.

Definition 2.1.2.10. *Eine lineare mit $+$ verträgliche Ordnung auf $\mathbb{N}^n$ heißt* Monomordnung*, falls außerdem gilt $\forall \alpha \in \mathbb{N}^n : 0 \leq \alpha$. Diese Ordnung induziert eine entsprechende Ordnung auf den Monomen x^α in $K[x]$.*

Nach dem obrigen Satz ist jede Monomordnung eine Wohlordnung.

Beispiele 2.1.2.11.

(1) (a) Für $n = 1$ gibt es genau eine Monomordnung auf $\mathbb{N}$.

(b) Mit Aufgabe 29 kann man für $n \geq 2$ zeigen, dass es überabzählbar viele Monomordnungen auf $\mathbb{N}^n$ gibt.

(2) (a) Die *lexikographische Ordnung* "lex" auf $\mathbb{N}^n$:

Definiere $\alpha \leq_{lex} \beta \Leftrightarrow$ erster Eintrag von $\beta - \alpha$, der ungleich 0 ist, ist positiv, oder es ist $\alpha \leq_{lex} \beta \Leftrightarrow$ beim ersten Paar (α_i, β_i) mit $\alpha_i \neq \beta_i$ ist $\alpha_i < \beta_i$, oder $\alpha = \beta$.

Dann ist $\leq_{lex}$ eine Monomordnung.

Für alle $\alpha \in \mathbb{N}^n$ mit $\alpha_1 > 0$ ist $|\{\beta \in \mathbb{N}^n \mid \beta \leq \alpha\}| = \infty$.

(b) Sei P eine Permutationsmatrix. Setze $\alpha \leq_P \beta :\Leftrightarrow P\alpha \leq_{lex} P\beta$. Dann ist $\leq_P$ eine Monomordnung.

Setze $\leq_{invlex} := \leq_{\begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}}$ (inverse lexikographische Ordnung).

(3) Die Monomordnung $\leq_{grlex}$ (andere übliche Bezeichnungen sind $\leq_{hlex}$ und $\leq_{deglex}$) wird definiert durch $\alpha \leq_{grlex} \beta :\Leftrightarrow (|\alpha| < |\beta|) \vee (|\alpha| = |\beta| \wedge \alpha \leq_{lex} \beta)$.

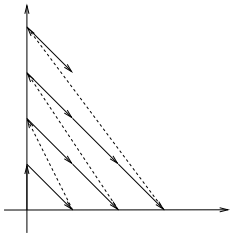


Abbildung 2.4: Die Monomordnung $\leq_{grlex}$

(4) Verallgemeinerung von (3): Sei $\leq$ eine Monomordnung, $\omega \in \mathbb{R}^n_{\geq 0}$. Für $\alpha, \beta \in \mathbb{N}^n$ sei

$$\alpha \leq_\omega \beta :\Leftrightarrow \omega^{\,t}\alpha < \omega^{\,t}\beta \vee (\omega^{\,t}\alpha = \omega^{\,t}\beta \wedge \alpha \leq \beta).$$

Dann ist $\leq_\omega$ eine Monomordnung (Übung).

(5) (a) Iteration von (4): Seien $\omega^{(1)}, \ldots, \omega^{(n)} \in \mathbb{R}^n \setminus \{0\}$ und $U = \begin{pmatrix} \omega^{(1)} \\ \vdots \\ \omega^{(1)} \end{pmatrix}$. Sei $\leq$ linear und mit $+$ verträgliche Ordnung auf $\mathbb{N}^n$. Definiere zu $\alpha, \beta \in \mathbb{N}^n$

$$\alpha \leq_U \beta :\Leftrightarrow U^{\,t}\alpha <_{lex} U^{\,t}\beta \vee (U^{\,t}\alpha = U^{\,t}\beta \wedge \alpha \leq \beta),$$

wobei $\leq_{lex}$ auf $\mathbb{R}^n$ fortgesetzt wird.

Übung: $\leq_U$ ist lineare mit $+$ verträgliche Ordnung.

Ist $\operatorname{rang} U = n$, so ist $\alpha \leq_U \beta \Leftrightarrow U^{\,t}\alpha \leq_{lex} U^{\,t}\beta$.

(b) Wenn in (a) $\operatorname{rang} U = n$ ist, dann lässt sich $\leq_U$ auf $\mathbb{Q}^n$ fortsetzen: Für $\alpha, \beta \in \mathbb{Q}^n$ setze

$$\alpha \leq_U \beta :\Leftrightarrow U^{\,t}\alpha \leq_{lex} U^{\,t}\beta,$$

wobei $\leq_{lex}$ auf $\mathbb{R}^n$ fortgesetzt wird.

(6) "*grevlex*" [CLO96] (schon 1927 von Macanlay, vergleiche [Eis95b, p. 326])

$$\alpha \leq_{grevlex} \beta :\Leftrightarrow |\alpha| < |\beta| \vee (|\alpha| = |\beta| \wedge \alpha \leq_{invlex} \beta),$$

$\alpha, \beta \in \mathbb{N}^n$.

2.1.3 Geometrische Beschreibung von Monomordnungen

Ziel: Überblick über alle Monomordnungen.

Satz 2.1.3.1 (L. Robbiano 1985, Ostrowski 1975). *Sei $\leq$ eine Monomordnung auf $\mathbb{N}^n$. Dann gibt es $u_1, \ldots, u_s \in \mathbb{R}^n$ paarweise orthogonal derart, dass*

$$\alpha \leq \beta \Leftrightarrow U\,{}^{\mathrm{t}}\alpha \leq_{lex} U\,{}^{\mathrm{t}}\beta \tag{2.1.3.1}$$

für alle $\alpha, \beta \in \mathbb{N}^n$, $U = \begin{pmatrix} u_1 \\ \vdots \\ u_s \end{pmatrix} \in \mathbb{R}^{s \times n}$.

Die in Satz 2.1.3.1 auftretende Matrix ist nicht eindeutig:

Satz 2.1.3.2. *Eine Matrix $U \in \mathbb{R}^{s \times n}$ induziert über 2.1.3.1 eine Monomordnung auf $\mathbb{N}^n$ genau dann, wenn gilt*

(i) *Der erste von 0 verschiedene Eintrag in jeder Spalte ist positiv;*

(ii) $(\mathrm{Ker}_{\mathbb{R}}\, U) \cap \mathbb{Q}^n = \{0\}$.

Beweis. Zur Übung. □

Beweis des Satzes von Robbiano und Ostrowski.

(I) Fortsetzung von $\leq$ zu einer mit $+$ verträglichen Ordnung auf $\mathbb{Z}^n$ und dann $\mathbb{Q}^n$.

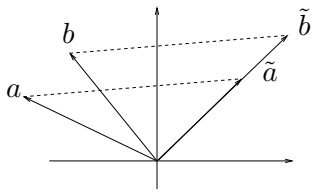


Abbildung 2.5: Fortsetzung von $\leq$ auf $\mathbb{Z}^n$ durch Verschieben der Vektoren zurück in $\mathbb{N}^n$.

- Fortsetzen auf $\mathbb{Z}^n$ durch Verschieben in $\mathbb{N}^n$ (siehe Abbildung 2.5).
- Multiplikation mit Hauptnenner für Fortsetzung auf $\mathbb{Q}^n$.

(II) Setze $H_1 := \{v \in \mathbb{R}^n \mid$ In jeder Umgebung von v liegen rationale Punkte ≤ 0 und $\geq 0\}$.

Behauptung A:

(i) H_1 ist Untervektorraum;

(ii) $\dim_{\mathbb{R}} H_1 = n - 1$;

(iii) $H_1 \cap \mathbb{R}^n_+ = \emptyset$.

(III) Auswahl von $u_1 \in H_1^{\perp}$: Wegen (A)(ii) ist $\dim_{\mathbb{R}} H_1^{\perp} = 1$.

Behauptung B:

(i) Es gibt ein $u_1 \in H_1^{\perp}$ mit $u_1 \geq_o 0$ und $u_1 \neq 0$. Ein solches u_1 zeigt in den positiven Halbraum, d. h. es gibt eine Umgebung von u_1 derart, dass alle rationalen Punkte der Umgebung > 0 sind.

(ii) Für alle $\alpha, \beta \in \mathbb{Q}^n$ mit $\beta - \alpha \notin H_1$ gilt

$$\alpha < \beta \Leftrightarrow u_1\,{}^{\mathrm{t}}\alpha < u_1\,{}^{\mathrm{t}}\beta.$$

(IV) Beschreibung der Anordnung auf $H_1 \cap \mathbb{Q}^n$, Iteration.

Einfachster Fall: $H_1 \cap \mathbb{Q}^n = \{0\}$. Im allgemeinen auf H_1 so verfahren wie oben. Wieviele u_i nötig sind hängt davon ab, wie "irrational" die Monomordnung ist.

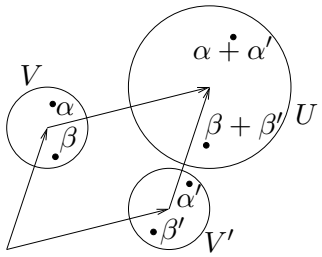


Abbildung 2.6: Teil des Beweises von Behauptung A(i) beim Satz von Robbiano und Ostrowski
Es ist $\alpha \leq 0 \leq \beta$, $\alpha' \leq 0 \leq \beta'$ und damit $\alpha + \alpha' \leq 0 \leq \beta + \beta'$.

Beweis von Behauptung A:

(i) Zu jeder Umgebung U von $v + v'$ ($v, v' \in H_1$) gibt es V, V' (Umgebungen von v, v') mit $U \subseteq V + V'$. Damit ist $v + v' \in H_1$.

Analog: Zu $\lambda \in \mathbb{R}$, $v \in H_1$ ist $\lambda v \in H_1$.

Es ist $0 \in H_1$: Es ist $\frac{1}{n} v > 0$ für $v \in \mathbb{N}^n \setminus \{0\}$, $v > 0$. Dann $-v < 0 \Rightarrow$ Behauptung.

(ii) Es ist $v = (1, \ldots, 1) \notin H_1$, also $\dim_{\mathbb{R}} H_1 \leq n - 1$. (Betrachte Kugel um v mit Radius $\frac{1}{2}$.)

Betrachte

$$\sigma : \mathbb{R}^n \setminus H_1 \to \mathbb{R}, \qquad \sigma(v) = \begin{cases} 1, & \exists \text{ Umgebung von } v \text{ ohne rationale Punkte } \geq 0 \\ -1, & \exists \text{ Umgebung von } v \text{ ohne rationale Punkte } \leq 0 \end{cases}.$$

Es ist σ stetig (trivial: betrachte Umgebung aus Definition von σ).

Konsequenz: $\mathbb{R}^n \setminus H_1$ nicht zusammenhängend. Damit folgt $\dim H_1 = n - 1$ (Beweis von dieser Folgerung zur Übung).

(iii) Sei $v \in H_1 \cap \mathbb{R}^n_+$. Es gibt eine Umgebung V von v derart, dass $V \subseteq \mathbb{R}^n_+$. Da $\leq$ Fortsetzung einer Monomordnung ist, gilt $\mathbb{Q}^n_+ \supseteq V \cap \mathbb{Q}^n \subseteq \{\alpha \in \mathbb{Q}^n \mid 0 < \alpha\}$, Widerspruch zu $v \in H_1$!

Beweis von Behauptung B: Zur Übung. □

Definition 2.1.3.3. *Sei s minimal in Satz 1.3.1. Ist $s = 1$, so heißt $\leq$ vom* archimedischen Typ. *Ist $s = n$, so heißt $\leq$ vom* lexikographischen Typ.

Beispiele 2.1.3.4.

(a) Für $\leq_{lex}$ ist $U = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

Es ist $H_1 = \{v \in \mathbb{R}^n \mid v_1 = 0\}$, also $u_1 = e_1$. Dann ist $H_2 = \{v \in \mathbb{R}^n \mid v_1 = v_2 = 0\} = \{v \in H_1 \mid v_2 = 0\}$, also $u_2 = e_2$.

(b) Für $\leq_{invlex}$ ist $U = \begin{pmatrix} 0 & & 1 \\ & \ldots & \\ 1 & & 0 \end{pmatrix}$.

(c) Für $\leq_{grlex}$ im Falle $n = 3$ ist $U = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$ oder einfacher $U = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

(d) Für $\leq_{grevlex}$ ist $U = \begin{pmatrix} 1 & \cdots & \cdots & \cdots & 1 \\ 0 & \cdots & \cdots & 0 & -1 \\ \vdots & & & \ldots & 0 \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ 0 & -1 & 0 & \cdots & 0 \end{pmatrix}$.

(e) Fall $n = 3$: $U = \begin{pmatrix} 1 & \sqrt{2} & 1+\sqrt{2} \\ 1 & 1 & 1 \end{pmatrix}$.

(f) Fall $n = 3$: $U = \begin{pmatrix} 1 & \sqrt{2} & \sqrt{3} \end{pmatrix}$ beschreibt eine Ordnung von archimedischen Typ (für $v \in \mathbb{Q}^3$ gilt $U\,{}^{\mathrm{t}}v = 0 \Leftrightarrow v = 0$).

Bemerkung 2.1.3.5.

- Vom $\mathbb{R}^n$ aus sehen alle Monomordnungen "gleich" aus.
- Es gibt *viele* Monomordnungen, aber zur Unterscheidung endlicher Polynommengen genügen stets endlich viele (siehe unten).

2.1.4 Einige ordnungsabhängige Definitionen für Polynome

Definition 2.1.4.1. *Sei $\leq$ eine Monomordnung auf $\mathbb{N}^n$ und $f \in K[x_1, \ldots, x_n] \setminus \{0\}$. Dann gibt es eine einelementige Darstellung*

$$f = \sum_{i=1}^{r} a_{\alpha^{(i)}} x^{\alpha^{(i)}}$$

mit $a_{\alpha^{(i)}} \neq 0$ und $\alpha^{(r)} > \cdots > \alpha^{(1)} \geq 0$.

(i) *Es heißt* $\max_{\leq}(f) := \alpha^{(r)}$ *der* (Multi-)Grad *von f;*

(ii) *Es heißt* $\mathrm{LK}_{\leq}(f) := a_{\alpha^{(r)}}$ *der* Leitkoeffizient *von f;*

(iii) *Es heißt* $\mathrm{LM}_{\leq}(f) := x^{\alpha^{(r)}}$ *das* Leitmonom *von f;*

(iv) *Es heißt* $\mathrm{LT}_{\leq}(f) := a_{\alpha}^{(r)} x^{\alpha^{(r)}}$ *der* Leitterm *von f.*

Beobachtung 2.1.4.2. Seien $f, g \in K[x_1, \ldots, x_n] \setminus \{0\}$ und $\leq$ eine Monomordnung.

(i) Es gilt

$$\begin{aligned} LK_{\leq}(f) \cdot LK_{\leq}(g) &= LK_{\leq}(f \cdot g), \\ LM_{\leq}(f) \cdot LM_{\leq}(g) &= LM_{\leq}(f \cdot g), \\ LT_{\leq}(f) \cdot LT_{\leq}(g) &= LT_{\leq}(f \cdot g). \end{aligned}$$

(ii) Es gilt

$$\max_{\leq}(f \cdot g) = \max_{\leq}(f) + \max_{\leq}(g), \qquad \max_{\leq}(f+g) \leq \max\{\max_{\leq}(f), \max_{\leq}(g)\}.$$

Es gilt $\max_{\leq}(f+g) = \max\{\max_{\leq}(f), \max_{\leq}(g)\}$ genau dann, wenn $\mathrm{LT}_{\leq}(f) + \mathrm{LT}_{\leq}(g) \neq 0$.

(iii) Kürzungsregel: Aus $\mathrm{LM}_{\leq}(fh) = \mathrm{LM}_{\leq}(hg) \neq 0$ folgt $\mathrm{LM}_{\leq}(f) = \mathrm{LM}_{\leq}(g)$ und $\max_{\leq}(f) = \max_{\leq}(g)$.

Definition 2.1.4.3. *Zu $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ mit $f = \sum'_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha = \sum_{i=1}^{n} a_{\alpha^{(i)}} x^{\alpha^{(i)}}$ mit paarweise verschiedenen $\alpha^{(i)}$.*

(i) *Es heißt* $\mathrm{supp}(f) := \{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\} = \{\alpha^{(1)}, \ldots, \alpha^{(r)}\} \subseteq \mathbb{N}^n$ *der* Support *oder* Träger *von f.*

(ii) *Es heißt* $\mathrm{New}(f) := \mathrm{conv}(\mathrm{supp}(f))$ *das* Newtonpolyop *von f.*

(iii) *Es heißt* $\mathrm{New\tilde{w}}(f) := \mathrm{New}(f) + \mathbb{R}^n_{\leq 0}$ *das* Newtonpolyeder *von f.*

Beispiel 2.1.4.4.

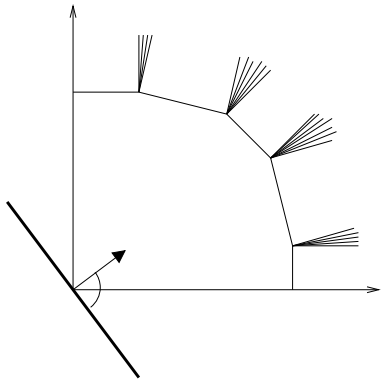
(a) Betrachte die Polynome $f := x^5y^8 + x^4y^{10} + x^3y^6 + x^2y^{11} + xy^9$ und $g := x^{10}y^3 + x^8y^7 + x^5y^7 + x^4y^5 + x^4y^2$.

(b) Betrachte die Polynome $f_1 := yx^3 - y^4x$, $f_2 := x^4 - y^2x^6$ und $f_3 := y^7x^3 - x^6y^6$.

Satz 2.1.4.5 (Gritzmann/Sturmfels, 1993). *Die Ecken von* $\mathrm{Ne\tilde{w}}(f)$ *entsprechen genau den Monomen von* f*, die als Leitterme in Frage kommen.*

Bemerkung 2.1.4.6. Der Satz von Robbiano besagt im $\mathbb{N}^2$: Sei $\leq$ eine Monomordnung auf $\mathbb{N}^2$, dann existiert ein $u_1 \in \mathbb{R}^2$ mit nichtnegativen Einträgen derart, dass

$$\alpha \leq \beta \Leftrightarrow \alpha\,{}^{\mathrm{t}}u_1 \leq \beta\,{}^{\mathrm{t}}u_1 \vee (\alpha\,{}^{\mathrm{t}}u_1 = \beta\,{}^{\mathrm{t}}u_1 \wedge \alpha \leq \beta).$$



Satz 2.1.4.7. *Seien* $f, g \in K[x_1, \ldots, x_n] \setminus \{0\}$*. Dann gilt*

(a) $\mathrm{New}(fg) = \mathrm{New}(f) + \mathrm{New}(g)$ *(Minkowski-Addition) und*

(b) $\mathrm{Ne\tilde{w}}(fg) = \mathrm{Ne\tilde{w}}(f) + \mathrm{Ne\tilde{w}}(g)$.

Beispiele 2.1.4.8.

(a) Beispiel zur Minksowski-Summe von Newtonpolytopen bzw. Newtonpolyedern.

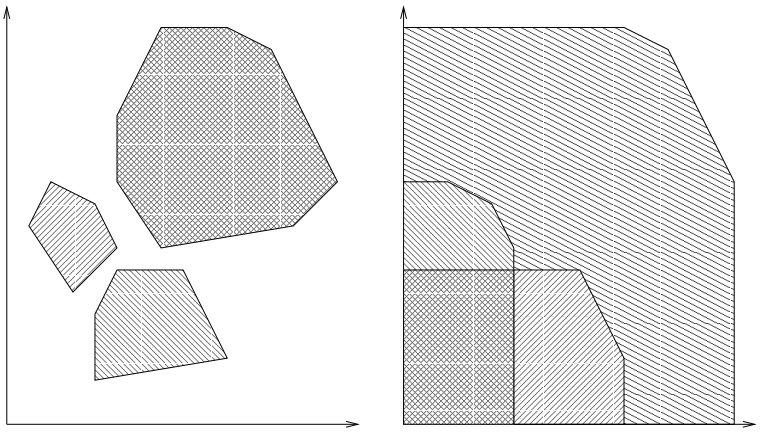
Betrachte die Polynome

$$f := x^5y^8 + x^4y^{10} + x^3y^6 + x^2y^11 + xy^9,$$
$$g := x^{10}y^3 + x^8y^7 + x^5y^7 + x^4y^5 + x^4y^2.$$

Es ist

$$\begin{aligned} fg = {} & x^{15}y^{11} + x^{14}y^{13} + x^{13}y^{15} + x^{13}y^9 + x^{12}y^{17} + x^{12}y^{14} + x^{11}y^{13} + x^{11}y^{12} \\ & + x^{10}y^{18} + x^{10}y^{15} + x^9y^{17} + x^9y^{16} + x^9y^{10} + x^8y^{15} + x^8y^{13} + x^8y^{12} \\ & + x^7y^{18} + x^7y^{11} + x^7y^8 + 2x^6y^{16} + x^6y^{13} + x^5y^{14} + x^5y^{11}. \end{aligned}$$

Die zugehörigen Newtonpoltope und Newtonpolyeder:



(b) Beispiel zur Minksowski-Summe von Newtonpolytopen bzw. Newtonpolyedern von ω-homogenen Polynomen. (Zur Definition vergleiche eine der späteren Übungsaufgaben.)

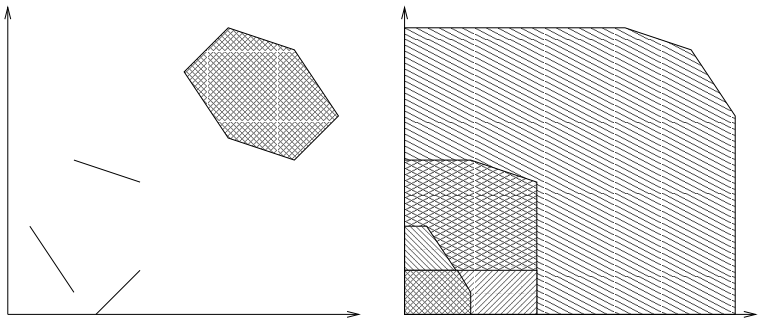
Betrachte die Polynome

$$\begin{aligned} f_1 &:= yx^3 - y^4x, \\ f_2 &:= x^4 - y^2x^6, \\ f_3 &:= y^7x^3 - x^6y^6. \end{aligned}$$

Es ist

$$f_1f_2f_3 = x^{10}y^8 - x^8y^{11} - x^{13}y^7 + x^{11}y^{10} - x^{12}y^{10} + x^{10}y^{13} + x^{15}y^9 - x^{13}y^{12}.$$

Die zugehörigen Newtonpoltope und Newtonpolyeder:



2.2 Manipulation und endliche Erzeugung von Polynommengen

2.2.0 Vorbemerkungen

Ziele:

1) jedes algebraische Gleichungssystem ist in Wirklichkeit ein endliches Gleichungssystem. → Hilbertscher Basissatz

   - Beweis stieß auf Ablehnung, da er nicht konstruktiv war.
   - Später fand Gordan einen konstruktiven Beweis.
   - Der kürzeste nicht-konstruktive Beweis wurde von Heidrun Sarges (siehe Kunz: Kommutative Algebra und Algebraische Geometrie) gefunden. Siehe auch Algebra I, Kapitel 7, die letzte Übungsaufgabe.
   - Hier: Konstruktiver Beweis.

2) Wie kann man ein endliches algebraisches Gleichungssystem vereinfachen?

   Naheliegender Ansatz: elementare Umformungen: $f_1, \ldots, f_r \to f_1 + af_k, f_2, \ldots, f_r$ mit a Polynom, $k > 1$.

   Aber: Hier treten Probleme auf!

2.2.1 Der Divisionsalgorithmus

Satz 2.2.1.1. *Seien $f_1, \ldots, f_s, f \in K[x_1, \ldots, x_n] \setminus \{0\}$, $\leq$ eine Monomordnung auf $\mathbb{N}^n$, $F = [f_1, \ldots, f_s]$. Dann gibt es $a_1, \ldots, a_s, r \in K[x_1, \ldots, x_n]$ derart, dass gilt*

(i) $f = a_1 f_1 + \cdots + a_s f_s + r$;

(ii) *entweder ist $r = 0$, oder $r \neq 0$ und kein Term von r wird geteilt durch einen Leitterm der $f_1, \ldots, f_s$;*

(iii) *es gilt $\max_{\leq}(f) \geq \max_{\leq}(a_i f_i)$ für alle $i = 1, \ldots, r$ mit $a_i \neq 0$.*

Schreibweise: *Schreibe $f \xrightarrow{F} r$ nur, wenn unser Algorithmus zu gegebenen f, F den "Rest" r ergibt.*

Beispiele 2.2.1.2.

(a) Sei $n = 1$, $s = 1$, und $f, f_1 \in K[x]$, $F = [f_1]$. Dann ist der Divisionsalgorithmus identisch zur normalen Division mit Rest in einer Variablen.

(b) Sei $n = 2$, $s = 1$ mit der Monomordnung $\leq_{grlex}$ und sei $x > y$. Ist $f = x^2y + x^2 + 2xy$ und $f_1 = x - y - 1$, so ist $\max_{\leq}(f) = (2, 1)$, $\max_{\leq}(f_1) = (1, 0)$ und der Algorithmus läuft wie folgt ab:

p	a_1	r
$x^2y + x^2 + 2xy$	0	0
$xy^2 + x^2 + xy + 2xy$	xy	0
$y^3 + x^2 + xy + y^2 + 2xy$	$xy + y^2$	0
$x^2 + xy + y^2 + 2xy$	$xy + y^2$	y^3
$4xy + y^2 + x$	$xy + y^2 + x$	y^3
$5y^2 + x + 4y$	$xy + y^2 + x + 4y$	y^3
$x + 4y$	$xy + y^2 + x + 4y$	$y^3 + 5y^2$
$5y + 1$	$xy + y^2 + x + 4y + 1$	$y^3 + 5y^2$
1	$xy + y^2 + x + 4y + 1$	$y^3 + 5y^2 + 5y$
0	$xy + y^2 + x + 4y + 1$	$y^3 + 5y^2 + 5y + 1$

(c) Sei $n = 2$, $s = 2$ mit der Monomordnung $\leq_{lex}$, und sei $x > y$. Sei weiter $f = x^3 + xy^3 + 1$, $f_1 = xy^2 - xy - 1$ und $f_2 = y - 1$. Der Algorithmus läuft wie folgt ab:

p	a_1	a_2	r
x^3+xy^3+1	0	0	0
xy^3+1	0	0	x^3
xy^2+y+1	y	0	x^3
$xy+y+2$	$y+1$	0	x^3
$x+y+2$	$y+1$	x	x^3
$y+2$	$y+1$	x	x^3+x
3	$y+1$	$x+1$	x^3+x
0	$y+1$	$x+1$	x^3+x+3

(d) Sei $n=3$, $s=3$, $f=x+y+z$, $f_1=x+y$, $f_2=y+z$, $f_3=x+z$ mit der Monomordnung $\leq_{lex}$, $x>y>z$.

Dann ist

- $f \xrightarrow{[f_1,f_2,f_3]} z$,
- $f \xrightarrow{[f_1,f_3,f_2]} z$,
- $f \xrightarrow{[f_2,f_1,f_3]} z$,
- $f \xrightarrow{[f_2,f_3,f_1]} -z$,
- etc.

"Trotzdem" gilt: $f=\frac{1}{2}(f_1+f_2+f_3)$ – unser Algorithmus ist also nicht optimal!

(e) Sei alles wie in (d), nur jetzt $f=x+y$.

- $f \xrightarrow{[f_1,f_2,f_3]} 0$,
- $f \xrightarrow{[f_3,f_2,f_1]} -2z$,
- etc.

(f) Sei $f_1=xy+1$, $f_2=xy^2-1$, $f=xy^2-x$, $R=K[x_1,x_2]$, und sei $\leq$ eine beliebige Monomordnung (die Leitterme sind hier unabhängig von $\leq$!). Dann gilt

- $f \xrightarrow{[f_1,f_2]} -x-y$ und
- $f \xrightarrow{[f_2,f_1]} -x+1$.

Analog siehe [CLO96].

Obwohl $f \in \langle f_1,f_2\rangle_R$ (das von f_1 und f_2 erzeugte Ideal) ist die Entscheidung hierüber für beliebige Monomordnungen alleine mit dem Divisionsalgorithmus nicht möglich.

Beweis zu Satz 1 mit Induktion/Wohlordnung.
Anfang: Sei $\max_{\leq}(f)=0$. Gilt $\max_{\leq}(f_i)=0$ für ein (minimal gewähltes) $i\in\{1,\ldots,s\}$, dann ist $f=\underbrace{\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)}}_{=:a_i}\mathrm{LT}(f_i)$, $r=0$, $a_j=0$ für $j\neq i$.

Ansonsten setze $a_i:=0$ für $i=1,\ldots,s$, $r:=f$ und es ist $f=\sum_{i=1}^s a_if_i+r$.
Es läßt sich leicht überprüfen, dass (ii) und (iii) in beiden Fällen gelten.
Annahme: Sei $\beta>0$ und sei der Satz richtig für alle $f\in K[x_1,\ldots,x_n]\setminus\{0\}$ mit $\alpha:=\max_{\leq}(f)<\beta$.

Wir zeigen: Dann gilt der Satz auch für Polynome f mit $\max_{\leq}(f)=\beta$. Dann folgt die Korrektheit des Satzes für alle $f\in K[x_1,\ldots,x_n]\setminus\{0\}$, denn sonst sei $M:=\{\alpha\in\mathbb{N}^n \mid \text{Satz ist falsch für ein } f\in K[x_1,\ldots,x_n]\setminus\{0\}\}\neq\emptyset$, und $\alpha:=\min M$ (existiert, da $\leq$ Wohlordnung). Nun gilt jedoch der Satz für alle f mit $\max_{\leq}(f)<\alpha$, Widerspruch.
Schluß: Sei $\max_{\leq}(f)=\beta$.
1. Fall: Es gibt ein $j\in\{1,\ldots,s\}$ (minimal gewählt) mit $\mathrm{LT}(f_j)\mid\mathrm{LT}(f)$.

Setze $p := f - \tilde{a}_j f_j$ mit $\tilde{a}_j := \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_j)}$. Ist $p = 0$, dann ist $f = \tilde{a}_j f + r$ mit $r := 0$, $\tilde{a}_i := 0$ für $i \neq j$, und (ii), (iii) gelten.

Ist $p \neq 0$, dann ist $\max_{\leq}(p) < \beta$. Nach Annahme gibt es $a_1, \ldots, a_s$ derart, dass $p = \sum_{i=1}^{s} a_i f_i + r$ und (ii), (iii) gelten (mit p anstelle von f). Damit ist

$$f = \sum_{i \neq j} a_i f_i + (a_j + \tilde{a}_j) f_j + r,$$

also gilt (i). Wegen der Annahme folgt (ii). Für $i \neq j$ gilt nach der Annahme $\max_{\leq}(f) > \max_{\leq}(p) \geq \max_{\leq}(a_i f_i)$ für $a_i \neq 0$, und für $i = j$ gilt auch

$$\max_{\leq}(f) \geq \max\{\max_{\leq}(a_j f_j), \max_{\leq}(\tilde{a}_j f_j)\} \geq \max_{\leq}(a_j f_j + \tilde{a}_j f_j).$$

2. Fall: Kein $\mathrm{LT}(f_i)$ teilt $\mathrm{LT}(f)$.

Setze $p := f - \mathrm{LT}(f)$. Dann ist $\max_{\leq}(p) < \max_{\leq}(f) = \beta$. Sei $p = \sum_{i=1}^{s} a_i f_i + r$ nach Annahme mit (ii), (iii) für p anstelle von f. Damit ist $f = \sum_{i=1}^{s} a_i f_i + (r + \mathrm{LT}(f))$, also gelten (i) und (iii). Ebenso gilt (ii) nach Wahl von r und mit $\mathrm{LT}(f_j) \nmid \mathrm{LT}(f)$, $j = 1, \ldots, s$. □

Ein weiterer Beweis findet sich in [CLO96, Seite 63].

Vorbemerkungen: Seien $f_1, \ldots, f_r, f_{r+1} \in R = K[x_1, \ldots, x_n]$, und betrachte das algebraische Gleichungssystem $f_1 = 0, \ldots, f_{r+1} = 0$.

Kann f_{r+1} weggelassen werden? Ja, wenn $f_{r+1} = \sum_{i=1}^{r} a_i f_i$, $a_i \in R$.

Problem: Divisionsalgorithmus kann nicht entscheiden, ob $f_{r+1} \in \langle f_1, \ldots, f_r \rangle_R \rightarrow$ Beispiele.

2.2.2 Monomideale und Dickson'sches Lemma

Sei im folgenden $R = K[x_1, \ldots, x_n]$.

Definition 2.2.2.1. *Ein Ideal I in R heißt* Monomideal*, wenn mit einer geeigneten Teilmenge $M \subseteq \mathbb{N}^n$ gilt $I = \langle \{x^\alpha \mid \alpha \in M\} \rangle_R$.*

Per Definition ist ein Monomideal ein Ideal. Zum Beispiel sind $\langle 1 \rangle = R$, $\langle x_1, x_2, \ldots, x_n \rangle$ Monomideale.

Beispiele 2.2.2.2. Sei $n = 2$, $M = \{(4,1), (2,3), (0,5)\}$. Siehe Abbildung 2.7.

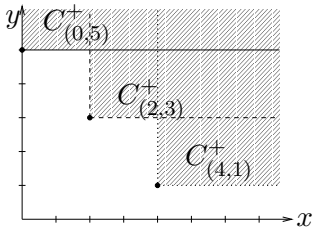


Abbildung 2.7: Das von M erzeugte Monomideal

Beobachtung 2.2.2.3.

(a) Für $\alpha \in \mathbb{N}^n$ gilt $\langle x^\alpha \rangle_R = \left\langle \{x^\beta \mid \beta \in C^+_\alpha\} \right\rangle_K$. Insbesondere ist $\{x^\beta \mid \beta \in C^+_\alpha\}$ genau die Menge der Monome von $\langle x^\alpha \rangle_R$.

Begründung: Sei $x^\gamma \in \langle x^\alpha \rangle_R$. Dann ist $x^\gamma = x^\alpha \cdot f$, $f \in R \setminus \{0\}$. Sei $f = f_1 x^{\beta(1)} + \cdots + f_t x^{\beta(t)}$, $f_1, \ldots, f_t \in K$. Es folgt $f = x^\beta$, $\beta \in \mathbb{N}^n$, $x^\gamma = x^\alpha x^\beta = x^{\alpha+\beta}$, also $\gamma \in C^+_\alpha$.

(b) Sei $\emptyset \neq M \subseteq \mathbb{N}^n$, dann gilt

$$\langle \{x^\alpha \mid \alpha \in M\} \rangle_R = \sum_{\alpha \in M} \langle x^\alpha \rangle_R \underset{(a)}{=} \sum_{\alpha \in M} \left\langle \{x^\beta \mid \beta \in C^+_\alpha\} \right\rangle_K = \left\langle \{x^\beta \mid \beta \in \overbrace{\bigcup_{\alpha \in M} C^+_\alpha}^{\in \mathcal{P}^+}\} \right\rangle_K.$$

Insbesondere ist die Menge $\{x^\beta \mid \beta \in \bigcup_{\alpha\in M} C_\alpha^+\}$ genau die Menge der Monome von I.

Begründung: Sei $x^\gamma \in I$. Dann ist $x^\gamma = \sum_{i=1}^r x^{\alpha^{(i)}} g_i =: g$, $\alpha^{(i)} \in M$, $g_i \in R$. Sortiere g: $g = \sum_{j=1}^t c_j x^{\beta^{(j)}}$, $\beta^{(j)}$ paarweise verschieden.

Beachte: Alle Terme in den g_i sind Vielfache gewisser x^α, $\alpha \in M$. Es folgt: Alle $c_j = 0$ bis auf ein c_{j^*} und $c_{j^*} = 1$. Dann ist $x^\gamma = x^{\beta^{(j^*)}}$, und $\beta^{(j^*)} \in \bigcup_{\alpha\in M} C_\alpha^*$.

Folgerung 2.2.2.4. *Sei $\emptyset \neq M \subseteq \mathbb{N}^n$, $I = \langle\{x^\alpha \mid \alpha \in M\}\rangle_R$, $\beta \in \mathbb{N}^n$ und $f \in R \setminus \{0\}$. Dann gilt*

(a) *Es ist $x^\beta \in I \Leftrightarrow \exists \alpha \in M : x^\alpha \mid x^\beta$;*

(b) *Es ist $f \in I \Leftrightarrow$ jeder Term aus f liegt in $I \Leftrightarrow f$ ist K-Linearkombination von Monomen aus I.*

Lemma 2.2.2.5 (Dickson). *[BW98, S. 184] Sei $\emptyset \neq M \subseteq \mathbb{N}^n$, $I = \langle\{x^\alpha \mid \alpha \in M\}\rangle_R$. Es gibt endlich viele $\alpha^{(1)}, \ldots, \alpha^{(r)} \in M$ derart, dass*

$$I = \left\langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(r)}} \right\rangle_R.$$

Beweis. Nach Beobachtung 2.2.3(b) ist $I = \left\langle\{x^\beta \mid \beta \in \bigcup_{\alpha\in M} C_\alpha^+ =: W\}\right\rangle_K$. Nun ist M abzählbar, also etwa $M = \{\alpha^{(1)}, \alpha^{(2)}, \ldots\}$. Dann wird

$$C^+_{\alpha^{(1)}} \subseteq C^+_{\alpha^{(1)}} \cup C^+_{\alpha^{(2)}} \subseteq \cdots \subseteq \bigcup_{i=1}^r C^+_{\alpha^{(i)}} \subseteq \ldots$$

nach Satz 2.1.2.9 konstant. □

2.2.3 Hilbertscher Basissatz und Gröbner-Basen

Kürzester nicht-konstruktiver Beweis von Heidrun Sarges, 1976 [BW98]. Siehe auch Algebra I, Kapitel 7, die letzte Übungsaufgabe. Wir benutzen den Divisionsalgorithmus und das Dicksonsche Lemma.

Als Vorbereitungen:

Definition 2.2.3.1. *Sei $\emptyset \neq I \neq \{0\}$, $I \subseteq R = K[x_1, \ldots, x_n]$ und $\leq$ eine Monomordnung auf $\mathbb{N}^n$.*

(i) *Sei* $\mathrm{LM}_\leq(I) := \{\mathrm{LM}_\leq(f) \mid f \in I \setminus \{0\}\}$ *die* Menge der Leitmonome *der Menge I. Sei analog* $\mathrm{LT}_\leq(I) := \{\mathrm{LT}_\leq(f) \mid f \in I \setminus \{0\}\}$ *die* Menge der Leitterme *der Menge I.*

(ii) *Sei* $\mathrm{in}_\leq(I) = \langle \mathrm{LT}_\leq(I)\rangle_R = \langle \mathrm{LM}_\leq(I)\rangle_R$ *das* Anfangsideal von I bezüglich $\leq$ *(*in *steht für* initial ideal*).*

Bemerkung 2.2.3.2. Es ist $\mathrm{in}_\leq(I)$ immer ein Monomideal.

Beispiele 2.2.3.3.

(a) Sei $n = 1$, $R = K[x]$, $\emptyset \neq I \neq \{0\}$. Dann gilt stets $\mathrm{in}_\leq(I) = x^k R$, k geeignet.

(b) Sei $I = \langle f_1\rangle_R$ mit $f_1 := x - y - 1$, $R = K[x, y]$, $\leq_{grlex}$, $x > y$. Dann ist $\mathrm{in}_\leq(I) = \langle x\rangle_R$.

(c) Sei $I = \langle f_1, f_2\rangle_R$, $R = K[x, y]$, $\leq_{lex}$, $x > y$. Mit $f_1 = xy^2 - xy - 1$ und $f_2 = y - 1$ ist $I = R$ und $\mathrm{in}_\leq(I) = R \supsetneq \langle \mathrm{LM}(f_1), \mathrm{LM}(f_2)\rangle_R = \left\langle xy^2, y\right\rangle_R = \langle y\rangle_R \neq R$.

(d) Sei $I = \langle f_1, f_2, f_3\rangle_R$ mit $R = K[x, y, z]$, $\leq_{lex}$ mit $x > y > z$. Sei $I = \langle x + y, y + z, x + z\rangle_R$, $\mathrm{in}_\leq(I) \supsetneq \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(f_3)\rangle_R$.

Folgerung 2.2.3.4. *Sei $I \neq \emptyset$. Es gilt stets* $\mathrm{in}_\leq(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r)\rangle_R$ *mit geeigneten $g_1, \ldots, g_r \in I$.*

Satz 2.2.3.5 (Hilbertscher Basissatz). *Jedes Ideal I in $K[x_1, \ldots, x_n]$ ist endlich erzeugt, d. h. stets $I = \langle g_1, \ldots, g_s \rangle_R$ mit $g_1, \ldots, g_s \in I$.*

Beweis. Sei I ein Ideal in R, und sei ohne Einschränkung $I \neq \{0\}$. Es ist $\mathrm{in}_\leq(I)$ nach Dicksons Lemma endlich erzeugt von endlich vielen Leitmonomen von Polynomen aus I, etwa $\mathrm{in}_\leq(I) = \left\langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(s)}} \right\rangle$ und $x^{\alpha^{(i)}} = \mathrm{LM}(g_i)$, $1 \leq i \leq s$, $g_i \in I$.

Wir zeigen $I = \langle g_1, \ldots, g_s \rangle$. Sei $f \in I$. Der Divisionsalgorithmus liefert $r, a_1, \ldots, a_s \in R$ mit (i) $f = \sum_{i=1}^{s} a_i g_i + r$, (ii) kein Term von r wird durch ein $\mathrm{LM}(g_j)$ geteilt, und (iii) $\max_\leq f \geq \max_\leq a_i g_i$ für alle i mit $a_i \neq 0$.

Sei angenommen $r \neq 0$ (sonst $f \in I$). Betrachte $f - \sum_{i=1}^{s} a_i g_i \in I$, also $r \in I$. Daher $\mathrm{LM}_\leq(r) \in \mathrm{in}_\leq(I)$, Widerspruch zu (ii) und Wahl der g_i.

Es ist gezeigt $I \subseteq \langle g_1, \ldots, g_s \rangle_R \subseteq I$, also gilt die Behauptung. □

Definition 2.2.3.6. *Sei $I \neq \{0\}$ ein Ideal in R und $\leq$ eine Monomordnung auf $\mathbb{N}^n$. Die endliche Teilmenge $\{g_1, \ldots, g_n\} \subset I$ heißt* Gröbner-Basis (GB) von I bezüglich $\leq$, *falls gilt*

$$\langle \mathrm{LM}_\leq(g_1), \ldots, \mathrm{LM}_\leq(g_s) \rangle = \mathrm{in}_\leq(I).$$

Satz 2.2.3.7. *Jedes Ideal $I \neq \{0\}$ in R besitzt eine Gröbner-Basis (bezüglich jeder Monomordnung $\leq$).*

Beweis. Siehe Beweis des Basissatzes. □

Beispiele 2.2.3.8. (wie 2.3.3)

(a) Im Fall $n = 1$ ist jede Basis eine Gröbner-Basis.

(b) Es ist $\{f_1\}$ eine Gröbner-Basis von I.

(c) Seien $f_1 = xy^2 - xy - 1$, $f_2 = y - 1$, $\leq_{lex}$ mit $x > y$ die Monomordnung. Dann ist f_1, f_2 keine Gröbner-Basis, aber trotzdem ein Erzeugendensystem. $\{1\}$ ist eine Gröbner-Basis.

(d) Es ist $\{f_1, f_2, f_3\}$ keine Gröbner-Basis, und mit $g_1 = \frac{1}{2}(f_1 - f_2 - f_3)$, $g_2 = \frac{1}{2}(f_1 + f_2 - f_3)$ und $g_3 = \frac{1}{2}(-f_1 + f_2 + f_3)$ ist $\{g_1, g_2, g_3\}$ eine Gröbner-Basis.

Beobachtung 2.2.3.9. Eine endliche Monombasis eines (Monom-)Ideals I ist bereits eine Gröbner-Basis (da $\mathrm{in}_\leq(I) = I$) bezüglich jeder Monomordnung.

Definition 2.2.3.10. *Ein endliches Erzeugendensystem eines Ideals in R, das Gröbner-Basis bezüglich jeder Monom-Ordnung ist, heißt* universelle Gröbner-Basis.

Das jedes Ideal eine endliche universelle Gröbner-Basis besitzt, wurde erst 1987 bekannt. (Eventuell später mehr dazu.)

Zwei Konsequenzen aus dem Basissatz:

Satz 2.2.3.11. *Es ist R Noethersch, d. h. jede aufsteigende (Inklusions-)Kette von Idealen wird konstant.*

Beweis. (Siehe Übung.) Sei $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ eine aufsteigende Kette, $J = \bigcup_{k=1}^{\infty} I_k = \langle g_1, \ldots, g_s \rangle$ (Basissatz). Dann gibt es ein k^* mit $g_1, \ldots, g_s \in I_{k^*}$, und damit ist $I_{k^*} \subseteq I_k \subseteq \cdots \subseteq J \subseteq I_{k^*}$ für $k \geq k^*$, womit die Behauptung folgt. □

Beispiel 2.2.3.12. Es sei $f_1 = x^2 + y$, $f_2 = y^2 + z$, $f_3 = z^2 + x$, $f = x^4z^2 + zx \in \mathbb{Z}_2[x]$. Sei weiter $F = [f_1, f_2, f_3]$. (Beachte $-x = x$ und $2 = 0$ in $\mathbb{F}_2$!)

(a) Sei $\leq_{grlex}$ mit $x > y > z$ gegeben. Wir berechnen $f \xrightarrow{F} r$.

p	a_1	a_2	a_3	r
x^4z^2+xz	0	0	0	0
x^2yz^2+xz	x^2z^2	0	0	0
y^2z^2+xz	$x^2z^2+yz^2$	0	0	0
z^3+xz	$x^2z^2+yz^2$	z^2	0	0
0	$x^2z^2+yz^2$	z^2	z	0

(b) Sei $\leq_{lex}$ mit $x>y>z$ gegeben. Wir berechnen $f \xrightarrow{F} r$. (Bemerke: $f_3 = x+z^2$.)

p	a_1	a_2	a_3	r
x^4z^2+xz	0	0	0	0
x^2yz^2+xz	x^2z^2	0	0	0
$xz+y^2z^2$	$x^2z^2+yz^2$	0	0	0
$y^2z^2+z^3$	$x^2z^2+yz^2$	0	z	0
0	$x^2z^2+yz^2$	z^2	z	0

In beiden Fällen ergibt sich der Rest 0. Ist F eine Gröbner-Basis?

Bemerkung 2.2.3.13. Seien $f_1 = x^2y+1$, $f_2 = xy^3+1 \in \mathbb{Q}[x,y]$, und $h := y^2f_1 - xf_2 = y^2 - x \in \langle f_1, f_2\rangle_R$. Nun ist jedoch $\mathrm{LM}_\leq(h) \in \mathrm{in}_\leq(f_1,f_2) \neq \langle \mathrm{LM}_\leq(f_1), \mathrm{LM}_\leq(f_2)\rangle_R = \langle x^2y, xy^3\rangle_R \not\ni \mathrm{LM}_\leq(h)$ für jede Monomordnung $\leq$, also ist $\{f_1,f_2\}$ keine Gröbner-Basis.

Anmerkung für Lösungsmengen algebraischer Gleichungssysteme:

Satz 2.2.3.14. *Sei $P \subseteq K[x_1,\ldots,x_n] =: R$, $P \neq \emptyset$. Es gibt stets endlich viele Polynome $g_1,\ldots,g_s \in \langle P\rangle_R$ derart, dass für jeden Erweiterungskörper L von K gilt*

$$\begin{aligned} V_L(P) &:= \{v \in L^n \mid \forall f \in P : f(v) = 0\} \\ &= \{v \in L^n \mid g_1(v) = \cdots = g_s(v) = 0\} = V_L(g_1,\ldots,g_s). \end{aligned}$$

Beweis. Der Hilbertsche Basissatz besagt: Es gibt $g_1,\ldots,g_s$ mit $\langle P\rangle_R = \langle g_1,\ldots,g_s\rangle_R$. □

Bemerkung 2.2.3.15. Wesentlich für Satz 2.2.3.14 ist

$$\langle P\rangle_R = \langle Q\rangle_R \Rightarrow V_L(P) = V_L(Q),$$

wobei $P,Q \subseteq R$, $P \neq \emptyset \neq Q$. Die Rückrichtung

$$V_L(P) = V_L(Q) \Rightarrow \langle P\rangle_R = \langle Q\rangle_R$$

ist im allgemeinen falsch! Ein Beispiel für $n=1$ ist gegeben durch $P = \{x^2\}$ und $Q = \{x\}$.

Wichtig: Bisher kennen wir kein Verfahren zur Berechnung von Gröbner-Basen!

Wir wollen zuerst auf wichtige Spezialfälle von Gröbner-Basen eingehen, bevor wir uns dem Problem der Berechnung von Basen widmen.

Definition 2.2.3.16. *Seien $I \neq \{0\}$ ein Ideal in R, $\leq$ eine Monomordnung, $\emptyset \neq G \subseteq R \setminus \{0\}$.*
Schreibweise: Schreibe $M(g) = \{x^\alpha \mid \alpha \in \mathrm{supp}(g)\}$ für die Monome von g.

(a) *Die Menge G heißt* minimales Erzeugendensystem *bzw.* Basis *von I, wenn gilt*

(i) $I = \langle G\rangle_R$ *und*

(ii) $\forall g \in G : \langle G \setminus \{g\}\rangle_R \neq I$.

(b) *Die Menge G heißt* minimale Gröbner-Basis von I bzgl. $\leq$, *wenn gilt*

(i) *G ist Gröbner-Basis von I bzgl. $\leq$,*

(ii) *G ist normiert (d. h. $\forall g \in G : \mathrm{LK}_\leq(g) = 1$) und*

(iii) $\mathrm{LM}_\leq(G)$ *ist minimale Basis von* $\mathrm{in}_\leq(I)$.

(c) *Die Menge G heißt* reduzierte Gröbner-Basis von I bzgl. $\leq$, *wenn gilt*

(i) *G ist minimale Gröbner-Basis von I bzgl. $\leq$ und*

(ii) $\forall g \in G : M(g) \cap \mathrm{in}_{\leq}(I) = \{\mathrm{LM}_{\leq}(g)\}$.

Beispiele 2.2.3.17.

(a) Hauptideal: Es sei $I = \langle g \rangle_R$, $\mathrm{in}_{\leq}(I) = \langle \mathrm{LM}_{\leq}(g) \rangle_R$, und ohne Einschränkung sei $\mathrm{LK}_{\leq}(g) = 1$. Dann ist $\{g\}$ reduzierte Gröbner-Basis von I.

(b) Ab $n \geq 2$ sind minimale Gröbner-Basen im allgemeinen nicht eindeutig!

Beispiel: $R = \mathbb{Q}[x, y]$, $I = \langle x + ky, y \rangle_R$, $k \in \mathbb{Q}$, $x > y$. Mit $g_1 := x + ky$, $g_2 := y$ ist $\{g_1, g_2\}$ minimale Gröbner-Basis von I, und $\{g_1 - kg_2, g_2\}$ ist reduzierte Gröbner-Basis von $\langle x, y \rangle_R = \langle x + ky, y \rangle_R$ für alle $k \in \mathbb{Q}$.

Beobachtung 2.2.3.18. Für jedes Ideal I und bezüglich jeder Monomordnung $\leq$ gilt

(i) I besitzt eine minimale Gröbner-Basis;

(ii) $\{g_1, \ldots, g_s\}$ ist genau dann eine minimale Gröbner-Basis von I, wenn $\{\mathrm{LT}_{\leq}(g_1), \ldots, \mathrm{LT}_{\leq}(g_s)\}$ minimale Gröbner-Basis von $\mathrm{in}_{\leq}(I)$ ist;

(iii) Alle minimalen Gröbner-Basen von I bezüglich einer Monomordnung sind gleich lang.

Beweis. Klar. □

Satz 2.2.3.19. *Jedes Ideal $I \neq \{0\}$ besitzt bezüglich einer festen Monomordnung $\leq$ stets genau eine reduzierte Gröbner-Basis (als Menge geschrieben; als Liste geschrieben ist sie bis auf Permutationen eindeutig bestimmt).*

Lemma 2.2.3.20. *Sei $G = [g_1, \ldots, g_s]$ eine Gröbner-Basis von I, $i \in \{1, \ldots, s\}$. Dann ist $G' = [g'_1, \ldots, g'_s]$ mit $g'_j := g_j$ für $j \neq i$ und*

$$g'_i := g_i - \sum_{\substack{j=1, j\neq i \\ \mathrm{LM}(a_j g_j) < \mathrm{LM}(g_i)}}^{s} a_j g_j \qquad (*)$$

mit entsprechenden $a_j \in R$ eine Gröbner-Basis von I. Wenn G minimal ist, so auch G'.

Beweis. Der Leitterm von g_i ändert sich nicht durch $(*)$. □

Beweis von Satz 2.3.19.
Existenz: Sei $G = \{g_1, \ldots, g_s\}$ eine Gröbner-Basis, und G sei ohne Einschränkung normiert. Ist $s = 1$, so ist G bereits eine reduzierte Gröbner-Basis, und wir sind fertig.

Sei also $s \geq 2$. Ohne Einschränkung sei G minimal (andernfalls lasse überflüssige Elemente weg), und ohne Einschränkung gelte $\mathrm{LM}(g_1) > \cdots > \mathrm{LM}(g_s)$ (wegen der Minimalität). Weiterhin gilt $\mathrm{LM}(g_i) \nmid \mathrm{LM}(g_j)$ für $i \neq j$ wegen der Minimalität.

$$\begin{array}{lll}
g_1 \overset{[g_2,\ldots,g_s]}{\longrightarrow} r_1, & & \text{also } \mathrm{LT}(r_1) = \mathrm{LT}(g_1); \\
\vdots & \vdots & \\
g_i \overset{[g_{i+1},\ldots,g_s]}{\longrightarrow} r_i, & & \text{also } \mathrm{LT}(r_i) = \mathrm{LT}(g_i); \\
\vdots & \vdots & \\
g_s =: r_s, & & \text{also } \mathrm{LT}(r_s) = \mathrm{LT}(g_s).
\end{array}$$

Da $\mathrm{LT}(r_i) = \mathrm{LT}(g_i)$, $1 \leq i \leq s$ und da $r_1, \ldots, r_s \in I$ ist $[r_1, \ldots, r_s]$ minimale Gröbner-Basis von I bezüglich $\leq$.

Das obige Verfahren zeigt: Kein Term ausser den Leittermen der $r_1, \ldots, r_s$ kann von einem der Leitterme der $g_1, \ldots, g_s$ geteilt werden. Somit gilt $M(r_j) \cap \mathrm{in}_{\leq}(I) = \{\mathrm{LM}(r_j)\}$, $1 \leq j \leq s$.
Eindeutigkeit: Seien G, G' reduzierte Gröbner-Basen von I, $|G| = |G'|$, $G = \{g_1, \ldots, g_s\}$ und $G' = \{g'_1, \ldots, g'_s\}$. Sei ohne Einschränkung $\mathrm{LT}(g_i) = \mathrm{LT}(g'_i)$, $1 \leq i \leq s$.

Betrachte $g_i - g'_i \in I$. Falls gilt $g_i - g'_i \neq 0$, so ist $\max_{\leq}(g_i - g'_i) < \max_{\leq} g_i = \max_{\leq} g'_i$, Widerspruch, denn $\mathrm{LM}(g_i - g'_i) \in \mathrm{in}_{\leq}(I) = \langle \mathrm{LM}_{\leq}(g_1), \ldots, \mathrm{LM}_{\leq}(g_s) \rangle_R$. Also muss $g_i = g'_i$ sein, $1 \leq i \leq s$. □

Beispiel 2.2.3.21. Sei $f = x + yz$, $g = y + xz$, $F = [f, g]$.

(a) Für $\leq_{lex}$, $x > y > z$ ist $[x + yz, yz^2 - y]$ reduzierte Gröbner-Basis.

(b) Für $\leq_{lex}$, $z > y > x$ ist $[zy + x, zx + y, y^2 - x^2]$ reduzierte Gröbner-Basis.

Eine andere, verbreitete Bezeichnung für Gröbner-Basen ist *Standardbasis*.

2.3 Gröbner-Basen

2.3.1 Weitere Eigenschaften von Gröbner-Basen

Schreibweise: $\overline{f}^F$ sei der Rest von f bei Division mit F mit unserem Algorithmus, also $f \xrightarrow{F} \overline{f}^F$.

Satz 2.3.1.1. *Sei $I \neq \{0\}$ Ideal in R, $\leq$ feste Monomordnung.*

(a) *Sei G eine Gröbner-Basis, dann gilt für alle $f \in R$*

$$\overline{f}^G = 0 \Leftrightarrow f \in I.$$

(b) *Der Divisionsrest bei Division durch eine Gröbner-Basis ist eindeutig und unabhängig von der Reihenfolge der Basispolynome der Gröbnerbasis.*

Mit anderen Worten: Für Gröbner-Basen G, H von I bzgl. $\leq$ und alle $f \in R$ gilt $\overline{f}^G = \overline{f}^H$.

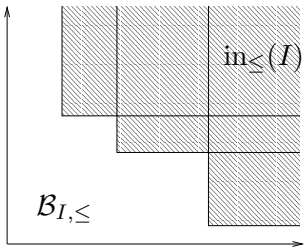


Abbildung 2.8: Die Mengen in$_\leq(I)$ und $\mathcal{B}_{I,\leq}$ aus Satz 2.3.1.1

(c) *Sei $\mathcal{B}_{I,\leq} := \{x^\alpha \mid x^\alpha \notin \text{in}_\leq(I)\}$ (oder einfach nur $\mathcal{B}$, falls I, $\leq$ fest sind) heißt die* Menge der Standardmonome *(bzgl. I, $\leq$) oder der* Basismonome. *Jedes $f \in R$ hat eine eindeutige Darstellung $f = g + r$ mit $g \in I$ und $r = 0$ oder r liegt in $\langle \mathcal{B}_{I,\leq} \rangle_K$. Man erhält r durch Division mit Rest mit einer Gröbner-Basis von I.*

Insbesondere ist $R = \langle \mathcal{B}_{I,\leq} \rangle_K \oplus \text{in}_\leq(I)$. Außerdem ist $\mathcal{B}_{I,\leq}$ eine K-Basis von $\langle \mathcal{B}_{I,\leq} \rangle_K$. Beachte dabei: $\text{in}_\leq(I) = \langle \{x^\alpha \mid x^\alpha \in \text{in}_\leq(I)\} \rangle_K$.

Beweis.

(a) **"⇒":** ✓

"⇐": Divisionsalgorithmus liefert $f = \sum_{i=1}^s a_i g_i + r =: g + r$. Wenn $f \in I$ ist, dann auch $r = f - g \in I$. Wäre $r \neq 0$, so müsste ein Leitmonom von einem g_i ein Teiler des Leitmonomes von r sein (da G Gröbner-Basis), Widerspruch zum Ergebnis des Divisionsalgorithmus. Also folgt $r = 0$ und damit die Behauptung.

(b) Bezüglich G sei $f = g + r$, r Divisionsrest, und bezüglich H sei $f = g' + r'$, r' Divisionsrest. Dann ist $0 = (g - g') + (r - r')$, also $I \ni g - g' = r' - r$. Da G und H Gröbner-Basen und in$_\leq(I)$ nur von $\leq$ abhängt, gilt: Kein Monom von $r - r'$ (falls $\neq 0$) wird geteilt durch eins der Leitmonome der g_i bzw. h_j (falls $G = [g_1, \ldots, g_s]$, $H = [h_1, \ldots, h_t]$). Da $g - g' \in I$ muss also $r = r'$ und $g = g'$ sein.

(c) Ergibt sich mit (a), (b) und Lineare Algebra I.

□

Erst mit Satz 2.3.1.1 ist eine vollständige Analogie zur Division mit Rest in einer Variablen erkennbar.

Die Ergebnisse führen zu einer kanonischen Darstellung für R/I:

Satz 2.3.1.2. *Bei festem Ideal $I \neq \{0\}$ und fester Monomordnung $\leq$ sei*

$$\varrho : R \to \langle \mathcal{B}_{I,\leq} \rangle_K \subseteq R, \qquad f \mapsto \overline{f}^G$$

für G eine Gröbner-Basis von I bezüglich $\leq$. (Eindeutig bestimmt nach Satz 2.3.1.1.)
Es gilt

(i) *$\varrho \circ \varrho = \varrho$;*

(ii) *ϱ ist K-linear, surjektiv und $\ker \varrho = I$;*

(iii) *für $f, h \in R$ gilt $\varrho(fh) = \varrho(\varrho(f)\varrho(h))$.*

Beweis.

(i) ✓ mit Divisionsalgorithmus.

(ii) Es ist $\varrho(cf) = c\varrho(f)$ klar, $c \in K$. Sei $f = g+r$, $h = g'+r'$. Dann ist $f+h = (g+g')+(r+r')$, $g + g' \in I$, $r + r' \in \langle \mathcal{B}_{I,\leq} \rangle_K$, womit die Behauptung folgt.

(iii) Ähnlich wie (ii).

□

Satz 2.3.1.3. *Führe in $\langle \mathcal{B}_{I,\leq} \rangle_K =: A$ die Multiplikation $r \odot r' := \varrho(rr')$ ein. Dann ist $(A, +, \odot, \cdot)$ eine kommutative K-Algebra[1], welche mit $R_{I,\leq}$ bezeichnet wird.*
Weiter ist $\varrho : R \to R_{I,\leq}$ ein surjektiver K-Algebra-Homomorphismus mit $\ker \varrho = I$. Weiter ist $R_{I,\leq} \cong R/I$, und $\varrho|_{R_{I,\leq}} = \mathbf{id}_{R_{I,\leq}}$.

Bemerkung 2.3.1.4. Wird R/I also beschrieben durch $\mathrm{in}_\leq(I)$ und ϱ (festgelegt durch I und $\leq$).

Wie kann man nun entscheiden, ob ein Erzeugendensystem eines Ideals eine Gröbner-Basis ist?

Satz 2.3.1.5 (Buchberger-Kriterium). *Sei $G = \{g_1, \ldots, g_s\} \subseteq R \setminus \{0\}$ ein Erzeugendensystem des Ideals $I \neq \{0\}$ in R. Dann ist für jede Monomordnung $\leq$ G eine Gröbner-Basis genau dann, wenn für alle $i, j \in \{1, \ldots, s\}$ gilt $\overline{S_\leq(g_i, g_j)}^G = 0$, wobei $S_\leq(f,g) = \frac{x^\gamma}{\mathrm{LT}_\leq(f)} f - \frac{x^\gamma}{\mathrm{LT}_\leq(g)} g$ mit $x^\gamma = \mathrm{kgV}(\mathrm{LM}_\leq(f), \mathrm{LM}_\leq(g))$. Das Polynom S wird als S-Polynom[2] bezeichnet.*
(Wichtig: $\max_\leq(S_\leq(f,g)) < \max_\leq \frac{x^\gamma}{\mathrm{LT}_\leq(f)} f = \max_\leq \frac{x^\gamma}{\mathrm{LT}_\leq(g)} g$.)

Bemerkung 2.3.1.6. Es ist $S_\leq(f,g) = -S_\leq(g,f)$.

Beispiel 2.3.1.7. Sei $f = x^2y^5 + y - 1$, $g = x^5y^2 + x - 1$, und sei $\leq_{grlex}$ mit $x > y$ die Monomordnung. Dann ist $S_\leq(f,g) = x^3 f - y^3 g = x^3y - xy^3 - x^3 + y^3$. Siehe auch Abbildung 2.9.

Beweis von Satz xx.
"⇒": ✓
"⇐": Sei $f \in I \setminus \{0\}$. Zu zeigen: $\mathrm{LM}(f) \in \langle \mathrm{LM}(G) \rangle_R$. Sei $f = \sum_{i=1}^s f_i g_i$, $f_i \in R$ (geht, da $f \in I$).
Fall 1: $\mathrm{LM}(f) = \mathrm{LM}(f_i g_i)$ für ein $i \Rightarrow$ fertig.
Fall 2: Für ein i ist $\mathrm{LM}(f_i g_i) > \mathrm{LM}(f)$. Dann gibt es $j \neq i$ mit $\mathrm{LM}(f_j g_j) = \mathrm{LM}(f_i g_i)$, insbesondere $s \geq 2$.

[1] D. h. A ist ein Ring, der Vektorraumeigenschaften hat.
[2] S kommt von dem griechischen Wort *'Syzygie'* (vergleiche Astronomie), was soviel wie Joch bedeutet.

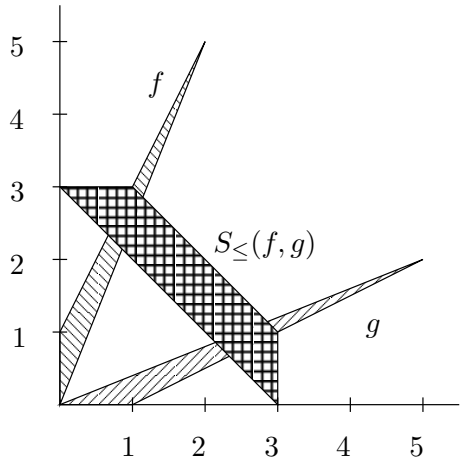


Abbildung 2.9: Die Polynome f, g und $S_\leq(f,g)$

Ohne Einschränkung sei $i=1$, $j=2$, und $\mathrm{LK}(g_1)=1=\mathrm{LK}(g_2)$. Sei etwa $f_1 = c_1 x^{\alpha^{(1)}} + \ldots$, $f_2 = c_2 x^{\alpha^{(2)}} + \ldots$,

$$f = (f_1 + c_2 x^{\alpha^{(1)}})g_1 + c_2(x^{\alpha^{(2)}} g_2 - x^{\alpha^{(1)}} g_1) + \underbrace{\cdots}_{\substack{\text{(restl. Terme}\\ \text{von } f_2)\cdot g_2}} + \sum_{i=3}^{s} f_i g_i. \qquad (*)$$

Dabei ist $x^{\alpha^{(2)}} g_2 - x^{\alpha^{(1)}} g_1 = x^\delta S_\leq(g_2, g_1)$. Der Divisionsalgorithmus liefert

$$0 = \overline{S_\leq(g_2,g_1)}^{G}, \qquad a_1 g_1 + \cdots + a_s g_s = S_\leq(g_2,g_1)$$

und $\mathrm{LM}(a_i g_i) \leq \mathrm{LM}(S_\leq(g_2,g_1)) < \mathrm{kgV}(\mathrm{LM}(g_2), \mathrm{LM}(g_1))$. Einsetzen in $(*)$ ergibt $f = \sum_{i=1}^{s} f_i' g_i$ und es gilt

$$\big|\{i \mid \mathrm{LM}(f_i' g_i) = \mathrm{LM}(f_1 g_1)\}\big| < |\{i \mid \mathrm{LM}(f_i g_i) = \mathrm{LM}(f_1 g_1)\}|.$$

Nun kann in endlich vielen Schritten erreicht werden, dass Fall 1 eintritt. □

Bemerkung 2.3.1.8. Der Beweis zeigt, dass das Buchberger-Kriterium unabhängig vom speziellen Divisionsalgorithmus ist.

Die Menge der Lösungen der linearen Gleichung

$$f_1 X_1 + \cdots + f_s X_s = 0, \qquad f_i \in R$$

wird mit $\mathrm{Syz}_R(f_1,\ldots,f_s)$ bezeichnet. Genauso im R^t, mit $(f_1,\ldots,f_s) \in R^{t\times s}$.

Satz 2.3.1.9 (Syzygiensatz von Hilbert). *Betrachte die Modulfolge*

$$\begin{aligned}
\Sigma_0 &:= I = \langle f_1,\ldots,f_s\rangle_R,\\
\Sigma_1 &:= \mathrm{Syz}_R(f_1,\ldots,f_s) = \left\langle f_1^{(1)},\ldots,f_{s_1}^{(1)}\right\rangle_R \subseteq R^S,\\
\Sigma_2 &:= \mathrm{Syz}_R(f_1^{(1)},\ldots,f_{s_1}^{(1)}) = \left\langle f_1^{(2)},\ldots,f_{s_2}^{(2)}\right\rangle_R \subseteq R^S,\\
&\cdots\cdots
\end{aligned}$$

Dann gibt es stets ein $k \geq 1$ so, dass Σ_k eine Basis besitzt. (Stichwort: freie Auflösung.)

Satz 2.3.1.10. *Seien $f_1,\ldots,f_s \in R\setminus\{0\}$, $\leq$ eine Monomordnung,*

$$\mathrm{ggT}(\mathrm{LM}(f_i),\mathrm{LM}(f_j)) = 1 \qquad (1)$$

für $1 \leq i < j \leq s$. Dann ist $F := [f_1,\ldots,f_s]$ eine Gröbner-Basis von $I := \langle F\rangle_R$.

Beweis. Es gelte ohne Einschränkung $\mathrm{LM}(f_1) > \cdots > \mathrm{LM}(f_s)$ und es sei $\tilde{f}_i := \overline{f_i}^{[f_{i+1},\ldots,f_s]}$ für $1 \leq i < s$ das Ergebnis des Divisionsalgorithmus mit $[f_{i+1}, \ldots, f_s]$ und $\tilde{f}_s := f_s$ (vergleiche Beweis von Satz 2.2.3.19). Nach Lemma 2.2.3.20 ist F genau dann eine Gröbner-Basis von I, wenn $\tilde{F} = [\tilde{f}_1, \ldots, \tilde{f}_s]$ eine Gröbner-Basis von I ist. Dieses Reduktionsverfahren zusammen mit (1) garantiert uns

$$\mathrm{LT}(f_i) = \mathrm{LT}(\tilde{f}_i) \tag{2}$$

für $1 \leq i \leq s$, und für $1 \leq j \leq s$, $j \neq i$ gilt

$$\text{kein } \mathrm{LM}(\tilde{f}_j) \text{ teilt ein Monom aus } \tilde{f}_i. \tag{3}$$

Ab jetzt gelte ohne Einschränkung (1)—(3) schon für F.

Wir zeigen nun mit Hilfe des Buchbergerkriteriums, dass F eine Gröbnerbasis von I ist. Seien dafür $i \neq j$ fest gewählt. Zu zeigen ist $\overline{S(f_i, f_j)}^F = 0$. Wir benutzten dabei folgende Bezeichnungen für $f \in K[x_1, \ldots, x_n]$:

Sei $f^{(0)} := f$ und für $k \geq 0$ sei $f^{(k+1)} := f^{(k)} - \mathrm{LT}(f^{(k)})$, falls $f^{(k)} \neq 0$, andernfalls $f^{(k+1)} := 0$. Weiter sei für $k, \ell \in \mathbb{N}_{>0}$ definiert $S_{k,\ell} := f_j f_i^{(k)} - f_i f_j^{(\ell)}$ insbesondere ist $S_{1,1} = S(f_i, f_j)$. Auf Grund von (1)—(3) gilt für $k, \ell \in \mathbb{N}_{>0}$ und mit $f_i^{(k)} \neq 0 \neq f_j^{(\ell)}$

$$\mathrm{LM}(f_j f_i^{(k)}) \neq \mathrm{LM}(f_i f_j^{(\ell)}). \tag{4}$$

Falls $S_{k,\ell} \neq 0$ gilt daher

$$\text{entweder } \mathrm{LM}(S_{k,\ell}) = \mathrm{LM}(f_j f_i^{(k)}) \text{ oder } \mathrm{LM}(S_{k,\ell}) = \mathrm{LM}(f_i f_j^{(\ell)}). \tag{5}$$

Mit diesen Bezeichnungen verfolgen wir die Berechnung von $\overline{S(f_i, f_j)}^F$ mit dem Divisionsalgorithmus der Vorlesung. Zunächst stellt man als Konsequenz von (1)–(5) fest, dass für $i \neq \nu \neq j$ und $k, \ell \in \mathbb{N}_{>0}$ *niemals* $\mathrm{LM}(f_\nu) \mid \mathrm{LM}(S_{k,\ell})$ gelten kann.

Solange aber $S_{k,\ell} \neq 0$ ist, gilt stets wegen (5) entweder $\mathrm{LM}(f_j) \mid \mathrm{LM}(S_{k,\ell})$ oder $\mathrm{LM}(f_i) \mid \mathrm{LM}(S_{k,\ell})$. Im ersten Fall wird vom Divisionsalgorithmus wie folgt reduziert:

$$S_{k,\ell} = (f_j f_i^{(k)} - f_i f_j^{(\ell)}) \to (S_{k,\ell} - \mathrm{LT}(f_i^{(k)}) f_j) = (f_j f_i^{(k+1)} - f_i f_j^{(\ell)}) = S_{k+1,\ell}, \tag{6}$$

und im zweiten Fall so:

$$S_{k,\ell} \to (S_{k,\ell} + \mathrm{LT}(f_j^{(\ell)}) f_i) = (f_j f_i^{(k)} - f_i f_j^{(\ell+1)}) = S_{k,\ell+1}. \tag{7}$$

Entweder wird dadurch $S_{k+1,\ell} = 0$ oder $S_{k,\ell+1} = 0$ und der Divisionsalgorithmus bricht ab, oder es werden wieder Reduktionsschritte der Form (6) oder (7) durchgeführt. Nach endlich vielen Schritten muss aber mit gewissen k', ℓ' gelten $S_{k',\ell'} = 0$. Der Divisionsalgorithmus ergibt also wie gewünscht $\overline{S(f_i, f_j)}^F = 0$. □

Folgerung 2.3.1.11. *Ist* $s = 2$, $\mathrm{ggT}(\mathrm{LM}(f_1), \mathrm{LM}(f_2)) = 1$, *dann ist* $\overline{S(f_1, f_2)}^{[f_1,f_2]} = 0$.

2.3.2 Der Buchberger-Algorithmus

Gegeben sei $F = [f_1, \ldots, f_s]$ und eine Monomordnung $\leq$.

- Setze $G := F$.
- Wiederhole:
  - Setze $G' := G$.
  - Für jedes Paar $\{p, q\} \subseteq G'$ mit $p \neq q$:
    - Setze $S := \overline{S(p,q)}^{G'}$.
    - Ist $S \neq 0$, so setze $G := G \cup \{S\}$.

  Solange bis $G = G'$.

- Ergebnis: G ist Gröbner-Basis von $\langle F \rangle_R$.

Satz 2.3.2.1. *Der Buchberger-Algorithmus ist korrekt.*

Beweis. Wenn der Algorithmus abbricht, liegt wegen dem Buchberger-Kriterium eine Gröbner-Basis vor.

Sei $I = \langle f_1, \ldots, f_r \rangle_R$. Stets bleibt $G \subseteq I$. Sei $J_0 = \langle \mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_r) \rangle_R \subseteq \mathrm{in}_{\leq}(I)$. Bei jeder Erweiterung von G um ein Polynom S im Algorithmus wird $\langle \mathrm{LM}(G) \rangle_R$ *echt* größer. Da jede aufsteigende Kette von Idealen abbricht, muss auch der Algorithmus abbrechen. □

Folgerung 2.3.2.2. *Für ein Ideal $I = \langle f_1, \ldots, f_s \rangle_R$ in $R = K[x_1, \ldots, x_n]$ und gegebener Monomordnung $\leq$ lässt sich (wenn K effektiv) in endlich vielen Schritten eine reduzierte Gröbner-Basis berechnen.*

Wir streben Verbesserungen des Algorithmus in zwei Richtungen an:

- Verbesserung des Divisionsalgorithmus;
- Verbesserung der Auswahl der Paare.

Beispiel 2.3.2.3. Das folgende Beispiel stammt aus: Peter Gritzmann und Bernd Sturmfels: Minkowski Addition of Polytopes, SIAM Journal of Discrete Math, Volume 6, No. 2, pp 246–269 (1993) auf Seite 261.

Sei $f := x^5 + yu^3 + z^2 - 1$, $g := x^2 + y^2 + z - 1$ und $h := x^6 + y^5 + z^3 - 1$.

Berechnen Sie Gröbner-Basen bezüglich verschiedener $\leq_{lex}$- und $\leq_{gradlex}$-Ordnungen.

Namen:

- Teo Mora, Stichwort “sugar”;
- Lorenzo Robbiano;
- Patricia Cianni;
- Computer-Algebra-Systeme:
  - CoCoA;
  - Singular (aus Kaiserslautern);
  - Macaulay 2.

2.3.3 Universelle Gröbnerbasen

Wieviele verschiedene reduzierte Gröbnerbasen lässt ein Ideal zu?

- Universelle Gröbnerbasen;
- $\bigcup\{$ Gröbnerbasen zu verschiedenen Monomordnungen $\}$ = Gröbnerbasis zu all diesen Monomordnungen.

Beispiele 2.3.3.1.

(1) Ist $n = 1$, so ist jede Basis universell.

(2) Monomialbasen sind universell.

(3) Siehe Aufgabe 44.

(4) Sei $f \in K[x] \setminus K$, $G = [f(x_1), \ldots, f(x_n)]$ ist universelle Gröbnerbasis von $\langle G \rangle_{K[x_1,\ldots,x_n]}$.

(5) Sei $n = 6$, $R = K[x_{11}, \ldots, x_{13}, x_{21}, \ldots, x_{23}]$. Setze

$$D_{12} = x_{11}x_{22} - x_{21}x_{12},$$
$$D_{23} = x_{12}x_{23} - x_{12}x_{22},$$
$$D_{13} = x_{11}x_{23} - x_{13}x_{21}.$$

Dann ist $G = [D_{12}, D_{23}, D_{13}]$ universelle Gröbnerbasis von $\langle G \rangle_R$.

Vergleiche [Stu96, Seite 2].

Beobachtung 2.3.3.2. Sei I ein Ideal in $K[x_1, \ldots, x_n]$. Dann sind äquivalent:

(1) Es existiert eine universelle Gröbnerbasis;

(2) $|\{G_\leq \mid G_\leq \text{ reduzierte Gröbnerbasis bezüglich der Monomordnung } \leq\}| < \infty$;

(3) $|\{\text{in}_\leq(I) \mid \leq \text{ Monomordnung }\}| < \infty$.

Beweis. Zeige (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1). □

Satz 2.3.3.3. *Es ist $J_0 := \{\text{in}_\leq(I) \mid \leq$ Monomordnung $\}$ endlich. (Ca. 1987/88.)*

Beweis (nach Logar). Sei $I \neq \{0\}$. Wir nehmen an $|J_0| = \infty$.

Sei $f_1 \in I \setminus \{0\}$. Sei $x^{\alpha^{(1)}}$ ein Monom aus f_1, das in unendlich vielen Idealen aus J_0 enthalten ist. Sei $J_1 := \{H \in J_0 \mid x^{\alpha^{(1)}} \in H\}$. Es existiert $H \in J_1$ mit $\left\langle x^{\alpha^{(1)}} \right\rangle \neq H$. Sei $x^\beta \in H \setminus \left\langle x^{\alpha^{(1)}} \right\rangle$.

Division mit Rest liefert $x^\beta = g + r$ mit $g \in I$, $r \in \langle B_H \rangle_K$. Setze $f_2 := x^\beta - r \in I \setminus \{0\}$ (nach Konstruktion). Sei $x^{\alpha^{(2)}}$ Monom von f_2, das in unendlich vielen Idealen aus J_1 vorkommt. Wichtig: $x^{\alpha^{(2)}} \notin \left\langle x^{\alpha^{(1)}} \right\rangle$.

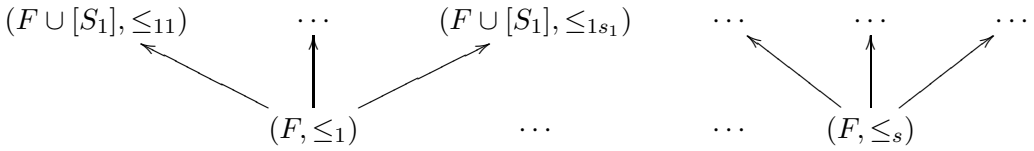
Führe dieses Verfahren weiter.

Am Ende entsteht (unter der Annahme $|J_0| = \infty$) eine echte Kette von Monomidealen, Widerspruch. □

Skizze eines 'anschaulichen Beweises'. Gegeben sei $F = [f_1, \ldots, f_r]$.

Ist $G \subseteq R \setminus \{0\}$ und $\leq$ eine Monomordnung, dann ist $(G, \leq)$ eine geordnete Menge, wobei $\leq = \leq|_{\text{supp}\, G}$ mit $\text{supp}\, G := \bigcup_{f \in G} \text{supp}\, f$.

Aufbau eines Multibaumes:



Hier sind die $\leq_i$ die endlich vielen Einschränkungen von Monomordnungen auf $\text{supp}\, F$.

"Weiche" den Divisionsalgorithmus so auf, dass er unabhängig von $\leq$ wird (nachdem die Leitterme festgelegt wurden); vergleiche Übungsaufgabe dazu.

Wir schreiben nun $(F, \leq_i) \to (G, \leq)$, falls es einen endlichen 'Pfad' $(F, \leq_i) \to (F \cup [S_1], \leq_{ij}) \to \cdots \to (G, \leq)$ gibt.

Eigenschaften:

- Für alle $(G, \leq)$ im Multibaum existiert $(F, \leq_i) \to (G, \leq)$.
- Jedes $(G, \leq)$ im Multibaum hat nur endlich viele obere Nachbarn. (Die Wurzel befindet sich unten.)

Ist der Multibaum endlich? Ja, nach dem Lemma von König! Dies kann angewendet werden, da der Buchbergeralgorithmus korrekt funktioniert. □

Lemma 2.3.3.4 (König). *Sei M eine mit $\leq$ geordnete Menge mit den Eigenschaften*

(i) *Es gibt endlich viele $m_1, \ldots, m_s \in M$ mit $\forall m \in M \exists i : m_i < m$.*

(ii) *Jedes $m \in M$ hat nur endlich viele obere Nachbarn (direkte Nachfolger).*

Gilt dann $|M| = \infty$, so gibt es eine aufsteigende unendliche Kette.

2.3.4 Schlussbemerkungen

Was fehlt:

- Gröbner-Spaziergang (Gröbner-Walk)
- Gröbner-Basen von Moduln
- Anwendungen von Gröbner-Basen in der kommutativen Algebra: Berechnung von
  - Schnitt zweier Ideale $I \cap J$,
  - Kernen von Abbildungen,
  - Bilder von Abbildungen.

(Vergleiche Übungsaufgaben und Seminar.)

Etwas zur Geschichte von Gröbner-Basen findet sich in Abschnitt 15.6 in [Eis95a, S. 341f].

2.4 Algebraische Gleichungssysteme insbesondere mit endlich vielen Lösungen

2.4.1 Elimination und Dimension

Definition 2.4.1.1. *Seien $X = \{x_1, \ldots, x_n\}$, $U \subseteq X$, $S = K[X \setminus U]$, und $\leq$ eine Monomordnung für $R = K[X]$. Dann heißt* $\leq$ Eliminierordnung bezüglich U *oder* eine U eliminierende Monomordnung, *falls für alle $f \in R \setminus \{0\}$ gilt*

$$\mathrm{LM}_{\leq}(f) \in S \Rightarrow f \in S.$$

Beispiele 2.4.1.2.

(a) Es ist $\leq_{lex}$ mit $x_1 > \cdots > x_n$ eine Eliminationsordnung bezüglich $\{x_1, \ldots, x_r\}$ für $0 \leq r \leq n$.

(b) Sei $\leq_r$ eine Monomordnung auf $\mathbb{N}^r$ und $\leq_s$ eine Monomordnung auf $\mathbb{N}^s$ mit $r + s = n$ und $r \neq 0 \neq s$. Für $\alpha, \beta \in \mathbb{N}^n$ setze

$$\alpha \leq \beta :\Leftrightarrow \begin{cases} \alpha_{(r)} <_r \beta_{(r)} & \text{oder} \\ \alpha_{(r)} = \beta_{(r)} \text{ und} & \alpha^{(r)} \leq_s \beta^{(r)} \end{cases}$$

mit $\alpha_{(r)} = (\alpha_1, \ldots, \alpha_r)$ und $\alpha^{(r)} = (\alpha_{r+1}, \ldots, \alpha_n)$.

(c) Bezeichner wie in (b). Sei $w \in \mathbb{R}^r_{>0}$ und $\leq$ eine Monomordnung auf $\mathbb{N}^n$. Für $\alpha, \beta \in \mathbb{N}^n$ setze

$$\alpha \leq^* \beta :\Leftrightarrow \begin{cases} {}^{\mathrm{t}}w\alpha_{(r)} <_r {}^{\mathrm{t}}w\beta_{(r)} & \text{oder} \\ {}^{\mathrm{t}}w\alpha_{(r)} = {}^{\mathrm{t}}w\beta_{(r)} \text{ und} & \alpha \leq \beta \end{cases}.$$

In (a), (b) und (c) liegen Eliminationsordnungen für $\{x_1, \ldots, x_r\}$ vor.

Satz 2.4.1.3. *Seien $X = \{x_1, \ldots, x_n\}$, $U \subseteq X$, $S = K[X \setminus U]$, und $\leq$ eine U eliminierende Monomordnung und I ein Ideal in R.*

(a) *Es ist* $\mathrm{in}_{\leq|_S}(I \cap S) = (\mathrm{in}_{\leq} I) \cap S$ *und*

(b) *ist G eine Gröbner-Basis von I bezüglich $\leq$, dann ist $G \cap S$ eine Gröbner-Basis von $I \cap S$ bezüglich $\leq|_S$.*

Beweis.

(a) **"$\supseteq$":** Sei $h \in (\mathrm{in}_{\leq} I) \cap S$. Dann ist $h \in S$ und alle Monome von h sind Leitmonome gewisser Polynome aus I. Da $\leq$ eine Eliminationsordnung bezüglich U ist, müssen alle diese Polynome in S liegen, also in $I \cap S$. Es folgt $h \in \mathrm{in}_{\leq|_S}(I \cap S)$.

"$\subseteq$": Sei x^α Monom aus $\mathrm{in}_{\leq|_S}(I \cap S)$. Dann gibt es ein $f \in I \cap S$ mit x^α als Leitmonom ($x^\alpha \in S$). Es folgt $x^\alpha \in (\mathrm{in}_{\leq} I) \cap S$.

(b) Sei $f \in I \cap S$, und sei $G = [g_1, \ldots, g_r]$. Es ist $0 = \overline{f}^G = f - \sum_{i=1}^r a_i g_i$ mit $\max_{\leq} a_i g_i \leq \max_{\leq} f$, womit $\mathrm{LM}_{\leq}(g_i) \in S$ ist falls $a_i \neq 0$. Damit folgt $g_i \in S$, falls $a_i \neq 0$, also $f \in \langle G \cap S \rangle_S$. Setze $G_S := G \cap S$, und sei ohne Einschränkung $G_S = [g_1, \ldots, g_s]$. Nach dem Buchbergerkriterium ist G_S eine Gröbner-Basis, da die S-Polynome in $I \cap S$ liegen und Division mit Rest mit G_S den Rest 0 ergibt.

□

Folgerung 2.4.1.4. *Sei I ein Ideal in R, G eine Gröbner-Basis von I bezüglich $\leq_{lex}$ mit $x_1 > \cdots > x_n$. Dann gilt für $0 \leq r < n$*

$$G \cap K[x_{r+1}, \ldots, x_n] \text{ Gröbner-Basis in } K[x_{r+1}, \ldots, x_n] \text{ von } I \cap K[x_{r+1}, \ldots, x_n].$$

Beispiele 2.4.1.5.

(a) Das Ideal I sei erzeugt von $f_1 = 1+xy+x^2y^2+x^3y^3$, $f_2 = 1+xyz+z^2+y^2$ und $f_3 = 1+xyz$. Man berechnet folgende Gröbner-Basen:

	Variablen	Ordnung	reduzierte Gröbner-Basis von I	Länge
(1)	$[x,y,z]$	$\leq_{lex}$	$[x-yz, y^2+z^2, z^3-z^2+z-1]$	3
(2)	$[y,x,z]$	$\leq_{lex}$	$[y-xz^2+xz-x, x^2+1, z^3-z^2+z-1]$	3
(3)	$[z,x,y]$	$\leq_{lex}$	$[z-xy+y^2-1, x^2+1, xy^2-x-y^3+y, y^4-1]$	4
(4)	$[x,z,y]$	$\leq_{lex}$	$[x-zy, z^2+y^2, zy^2-z-y^2+1, y^4-1]$	4
(5)	$[y,z,x]$	$\leq_{lex}$	$[y-z^2x+zx-x, z^3-z^2+z-1, x^2+1]$	3
(6)	$[z,y,x]$	$\leq_{lex}$	$[z+y^2-yx-1, y^3-y^2x-y+x, x^2+1]$	3
(7)	$[x,y,z]$	$\leq_{grlex}$	$[z^2+y^2, z^3-z^2+z-1, x^2+1, z^2+yx-z+1, xz^2-xz-y+x, zy-x]$	6

(Eine solch lange Gröbner-Basis wie in (7) ist untypisch für $\leq_{grlex}$.)

Anmerkung: In MAPLE werden die Ordnungen $\leq_{grlex}$ mit *tdeg* und $\leq_{lex}$ mit *plex* bezeichnet.

(b) Lösung eines algebraischen Gleichungssystem in "Dreiecksform" (Definition später!):

Seien $g_1 = x-yz$, $g_2 = y^2+z^2$, $g_3 = z^3-z^2+z+1 = (z-1)(z^2+1)$ und das Gleichungssystem $\{g_1 = 0, g_2 = 0, g_3 = 0\}$ gegeben.

Sei $K = \mathbb{Q}[\mathbf{i}]$. Es hat g_3 die Nullstellen $\{1, \mathbf{i}, -\mathbf{i}\}$, womit es sechs Lösungen gibt:

$$(\mathbf{i}, \mathbf{i}, 1), (-\mathbf{i}, \mathbf{i}, 1), (\mathbf{i}, 1, \mathbf{i}), (-\mathbf{i}, -1, \mathbf{i}), (-\mathbf{i}, 1, -\mathbf{i}) \text{ und } (\mathbf{i}, -1, -\mathbf{i}).$$

(c) "Dimensionsbegriff" (siehe unten). In (a) gilt mit $I = \langle f_1, f_2, f_3\rangle$

$$I \cap K[x_1] \neq \{0\}, I \cap K[x_2] \neq \{0\} \text{ und } I \cap K[x_3] \neq \{0\}.$$

(Sieht man mit den jeweils passenden Gröbner-Basen aus (a).) Weiterhin ist $I \cap K = \{0\}$, da wir Lösungen haben.

(d) Das Ideal I sei erzeugt von $f_1 = 9x^2+6xy+60x+y^2+20y+100$, $f_2 = 6x^2-xy+35x-y^2-5y+50$, $f_3 = 4x^2-4xy+20x+y^2-10y+25$. Man berechnet die folgende reduzierte Gröbner-Basis mit $\leq_{lex}$ und $[x,y,z]$:

$$G = [x^2+6x+9, xy+x+3y+3, y^2+2y+1].$$

Definition 2.4.1.6. *Es ist $G = [g_1, \ldots, g_s]$ in (*normierter, starker*)* Dreiecksform *(vergleiche Buch von Mishra), wenn $s \geq n$ ist und bei geeigneter Nummerierung gilt*

(i) $g_i \in K[x_i, \ldots, x_n]$,

(ii) g_i *enthält Term* $x_i^{d_i}$ *mit* $d_i \in \mathbb{N}_+$,

(iii) $\mathrm{LT}(g_i) = x_i^{d_i}$.

Definition 2.4.1.7. *Sei I ein Ideal in R*

(a) *Es heißt $U \subseteq X = \{x_1, \ldots, x_n\}$* unabhängig von I, *wenn $I \cap K[U] = \{0\}$.*

(b) *Für $I \neq R$ sei*

$$\dim I := \max\{|U| \mid U \subset X, U \text{ unabhängig von } I\}.$$

In Beispiel 5(c) ist $\dim I = 0$.

Beobachtung 2.4.1.8. Es ist $\dim I = 0$ äquivalent zu

$$I \cap K[x_i] \neq \{0\}, \quad 1 \leq i \leq n \qquad \text{und} \qquad I \cap K = \{0\}.$$

Bemerkung 2.4.1.9.

(a) Ein primitives Verfahren zur Entscheidung, ob $\dim I = 0$ ist:

Berechne eine Gröbner-Basis bezüglich $\leq_{lex}$ mit $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n > x_i$ und sehe nach, ob ein Polynom $\neq 0$ aus $K[x_i]$ vorkommt.

(b) Bei Polynomidealen äquivalente Dimensionen:

- Krulldimension,
- Transzendenzgrad von R/I.

Satz 2.4.1.10 (Hauptsatz über 0-dimensionale Ideale, ihre Lösungsmenge und Gleichungssysteme). *Sei I ein Ideal in R. Dann sind äquivalent:*

(1) *Es ist $0 < |\mathcal{V}_L(I)| < \infty$ in einem algebraisch abgeschlossenen Erweiterungskörper L von K.*

(2) *Es ist $\dim I = 0$.*

(3) *Für jede Monomordnung $\leq$ gilt $0 < \dim_K R_{I,\leq} < \infty$.*

(4) *Für $1 \leq i \leq n$ gilt:*

Jede Gröbner-Basis von I bezüglich einer Monomordnung $\leq$ enthält ein Polynom g_i mit $\mathrm{LM}(g_i) = x_i^{d_i}$ mit $d_i \in \mathbb{N}_+$.

(Insbesondere ist $|G| \geq n$ und $I \neq R$.)

(5) *Die reduzierte Gröbner-Basis von I bezüglich $\leq_{lex}$ mit $x_1 > \cdots > x_n$ ist in Dreiecksform (Definition 2.4.1.6).*

Insbesondere ist wieder $I \neq R$ und $|G| \geq n$.

Bemerkung 2.4.1.11. Die Äquivalenzen von (1) zu (i) $(1 < i \leq 5)$ benötigen den Hilbertschen Nullstellensatz, während (2) $\Leftrightarrow \cdots \Leftrightarrow$ (5) so gezeigt werden kann.

Satz 2.4.1.12 (Hilberts Nullstellensatz, starke Form). *Sei L ein algebraisch abgeschlossener Erweiterungskörper von K, I ein Ideal in R und $f \in R$. Dann gilt*

$$\mathcal{V}_L(I) \subseteq \mathcal{V}_L(f) \Rightarrow \exists q \in \mathbb{N}_+ : f^q \in I.$$

Definition 2.4.1.13. *Sei I ein Ideal in R. Setze*

$$\sqrt{I} = \{f \in R \mid \exists q \in \mathbb{N}_+ : f^q \in I\}.$$

Dann heißt $\sqrt{I}$ das Radikalideal *oder* Radikal *von I.*

Beobachtung 2.4.1.14. Es ist $\sqrt{I}$ ein Ideal, $I \subseteq \sqrt{I}$, $\sqrt{\sqrt{I}} = \sqrt{I}$ und $\mathcal{V}_L(I) = \mathcal{V}_L(\sqrt{I})$.

Beweis. Übungsaufgabe 48. □

Bemerkung 2.4.1.15. Die starke Form des Hilbertschen Nullstellensatz besagt

$$\sqrt{I} = \{f \in R \mid f|_{\mathcal{V}_L(I)} = 0\},$$

wobei L wie gerade ein algebraisch abgeschlossener Erweiterungskörper von K ist.

Beispiele 2.4.1.16. Sei $\mathbb{Q} \subseteq K$ oder sei K perfekt[3].

[3]Ein Körper K heißt *perfekt*, falls $\mathrm{Char}\, K = 0$ oder $\mathrm{Char}\, K = p$ und $K^p = K$. Eine alternative Definition ist K perfekt $\Leftrightarrow \forall f \in K[x] \setminus K : (f$ quadratfrei $\Leftrightarrow \mathrm{ggT}(f, \frac{d}{dx} f) = 1)$. Literatur: [BW98, p. 311 ff].

(a) $n = 1$: Sei $f \in K[x] \setminus K$. Dann ist

$$\sqrt{\langle f \rangle_R} = \{g \in K[x] \mid \exists p \in \mathbb{N}_+ : g^p \in \langle f \rangle\} = \left\langle \frac{f}{\mathrm{ggT}(f, \frac{d}{dx} f)} \right\rangle_R .$$

Zum Beispiel $K = \mathbb{Q}$, $f = (x-a)^2$, dann ist $\sqrt{\langle f \rangle_R} = \langle x - a \rangle_R$.

(b) Sei $I = \langle f_1, f_2 \rangle_R \subseteq K[x_1, x_2]$ mit $f_1 \in K[x_1]$, $f_2 \in K[x_2]$. Dann ist

$$\sqrt{I} = \left\langle \frac{f_1}{\mathrm{ggT}(f_1, \frac{d}{dx} f_1)}, \frac{f_2}{\mathrm{ggT}(f_2, \frac{d}{dx} f_2)} \right\rangle_R .$$

(Nachrechnen!)

Allgemein für $\dim I = 0$ später.

Satz 2.4.1.17 (Hilberts Nullstellensatz, schwache Form). *Sei L ein algebraisch abgeschlossener Erweiterungskörper von K und I ein Ideal in $R = K[x_1, \ldots, x_n]$. Dann gilt*

$$\mathcal{V}_L(I) = \emptyset \Rightarrow I = R.$$

Bemerkung 2.4.1.18. Die beiden Nullstellensätze sind äquivalent (hier ohne Beweis).

Vergleiche zum Beispiel [BW98], Kapitel 7, oder Lang: Algebra, Kunz: Kommutative Algebra und Algebraische Geometrie, van der Waerden (erste Ausgabe, ca. 1950, elementarer Beweis).

Bemerkung 2.4.1.19. Folgerung aus dem Nullstellensatz:

$$\mathcal{V}_L(I) = \emptyset \Leftrightarrow \{1\} \text{ ist reduzierte Gröbner-Basis von } I.$$

Nun zum

Beweis von Satz 2.4.1.10. **(1) ⇒ (2):** Sei etwa $\mathcal{V}_L(I) = \{v_1, \ldots, v_r\} \subseteq L^n$. Sei v_{ij} die j-te Komponente von v_i. Sei ohne Einschränkung $L = \overline{K}$. Dann sind alle v_{ij} algebraisch über K. Sei $f_j \in K[x_j] \setminus K$ derart, dass $v_{1j}, \ldots, v_{rj}$ (unter anderem) Nullstellen von f_j sind, und $f_j \in K[x_j] \subseteq R$; dann gilt $\mathcal{V}_L(I) \subseteq \mathcal{V}_L(f_j)$, $1 \leq j \leq r$. Hilberts Nullstellensatz liefert $\exists q_j \in \mathbb{N}_+ : f_j^{q_j} \in I$. Damit ist $I \cap K[x_j] \neq \{0\}$, $1 \leq j \leq n$, und da $\mathcal{V}_L(I) \neq 0$ folgt $1 \notin I$, also $K \cap I = \{0\}$. Damit gilt $\dim I = 0$.
(2) ⇒ (3): Sei $f_j \in (K[x_j] \cap I) \setminus K$, $1 \leq j \leq n$. Für jede Monomordnung ist $\mathrm{LM}(f_j) = x_j^{d_j}$, $d_j \in \mathbb{N}_+$ und damit

$$\mathcal{B}_{I,\leq} = \underbrace{(R \setminus \mathrm{in}_{\leq} I)}_{\neq \emptyset} \subseteq \underbrace{R \setminus \{x^{d_j e_j + \beta} \mid 1 \leq j \leq n, \beta \in \mathbb{N}^n\}}_{|\cdot| < \infty},$$

womit (3) folgt, da $\mathcal{B}_{I,\leq}$ K-Basis für $R_{I,\leq}$ ist.
(3) ⇒ (4): Klar.
(4) ⇒ (5): Folgt direkt mit Hilfe der Eliminier-Eigenschaft von $\leq_{lex}$.
(5) ⇒ (1): Sei L algebraisch abgeschlossene Körpererweiterung von K. Wäre $I = R$, so wäre $1 \in I$ und $\{1\}$ reduzierte Gröbner-Basis, Widerspruch zu (5). Sei also $I \neq R$. Mit dem schwachen Nullstellensatz folgt $|\mathcal{V}_L(I)| > 0$. Zu zeigen ist $|\mathcal{V}_L(I)| < \infty$.

Nun hat $g_n \in K[x_n] \setminus K$ endlich viele Nullstellen. Seien $g_{n-1} = x_{n-1}^{d_{n-1}} + \tilde{g}_{n-1}$ mit $\tilde{g}_{n-1} \in K[x_{n-1}, x_n]$ und $\mathrm{LT}(g_{n-1}) = \mathrm{LM}(g_{n-1}) = x_{n-1}^{d_{n-1}}$, $d_{n-1} \geq 1$. Einsetzen der endlich vielen Lösungen von $g_n = 0$ ergibt endlich viele nichttriviale Polynome aus $K[x_{n-1}]$, die alle in L endlich viele Lösungen besitzen.

Induktion liefert die Behauptung. □

Wie viele Lösungen gibt es?

Beobachtung 2.4.1.20. Sei $\dim I = 0$ und $G = [g_1, \ldots, g_s]$ reduzierte Gröbner-Basis von I in Dreiecksform mit $\mathrm{LT}(g_i) = x_i^{d_i}$. Dann gilt

$$|\mathcal{V}_L(I)| \leq \prod_{i=1}^{s} d_i.$$

Beweis. Siehe Beweis zu Satz 2.4.1.10, Teil "(5) ⇒ (1)". □

Wie erhält man genauere Informationen über $|\mathcal{V}_L(I)|$?

Beispiele 2.4.1.21.

(a) Beispiel 2.4.1.5(b): Dort ist $d_1 d_2 d_3 = 6 = |\mathcal{V}_L(I)|$.

(b) $n = 1$: Sei $f = x^k$, $|\mathcal{V}_L(f)| = 1$, $d = k$, $k \in \mathbb{N}$.

(c) $n = 2$: Sei $f_1 = x_1 + x_2 - 2$, $f_2 = x_1^2 - 2x_2 + 1$ und $I = \langle f_1, f_2 \rangle$, $\mathcal{V}_L(I) = \{(1,1)\}$. Jedoch ist $d_1 d_2 = 2$.

Hier ist $\sqrt{I} = \langle x_1 - 1, x_2 - 1 \rangle_R$. (Es ist $x_2 - 1 \in \sqrt{I}$, da $(x_2 - 1)^2 \in I$, und damit $f_1 - (x_2 - 1) = x_1 - 1 \in \sqrt{I}$. Da weiterhin $\langle x_1 - 1, x_2 - 1 \rangle$ ein maximales Ideal ist, muss $\sqrt{I} = \langle x_1 - 1, x_2 - 1 \rangle$ sein.)

Es ist $|\mathcal{V}_L(I)| = 1$ und $d_1^{(\sqrt{I})} d_2^{(\sqrt{I})} = 1$.

Das Beispiel (a) zeigt, dass die obere Schranke aus der Beobachtung scharf ist, und Beispiel (b) zeigt, dass sie auch sehr ungenau sein kann.

Satz 2.4.1.22. *Sei L algebraisch abgeschlossener Erweiterungskörper von K, $\dim I = 0$ und $\leq$ Monomordnung.*

(a) *Es ist* $|\mathcal{V}_L(I)| \leq \dim_K R/I = \dim_K R_{I,\leq} = |\mathcal{B}_{I,\leq}|$.

(b) *Ist $K = L$, so gilt*

$$|\mathcal{V}_L(I)| = |\mathcal{B}_{I,\leq}| \Leftrightarrow \sqrt{I} = I.$$

Anmerkung (ohne Beweis): Die Bedingung $K = L$ aus (b) ist nicht nötig, wenn K perfekt ist.

Beweis.

(a) Sei $I_L = \langle I \rangle_S$, $S = L[x_1, \ldots, x_n]$. Dann ist $\dim_K R/I \geq \dim_L S/I_L$. (Denn: Sei G eine Gröbner-Basis von I in R, dann gilt $G \subseteq I_L$. Es folgt $\{x^\alpha \mid x^\alpha \in \mathrm{in}_\leq I_L\} \supseteq \{x^\alpha \mid x^\alpha \in \mathrm{in}_\leq I\}$ und $\mathcal{B}_{L,I_L,\leq} \subseteq \mathcal{B}_{I,\leq}$, womit $\dim_L S/I_L \leq \dim_K R/I$ folgt.)

Außerdem ist $\mathcal{V}_L(I) = \mathcal{V}_L(I_L)$. Wir zeigen jetzt $\dim_L S/I_L \geq |\mathcal{V}_L(I_L)| =: m$. Es gilt $\dim I = 0$, also $0 < m < \infty$ nach Satz 2.4.1.10. Betrachte die lineare Abbildung

$$\varphi : \langle \mathcal{B}_{L,I_L,\leq} \rangle \to L^m, \quad r \mapsto (r(v_1), \ldots, r(v_m))$$

mit $\mathcal{V}_L(I_L) = \{v_1, \ldots, v_m\}$. Es ist φ L-linear.

Wir zeigen nun φ surjektiv: Mehrdimensionale Lagrange-Interpolation (siehe unten) ergibt Polynome $g_1, \ldots, g_m$ aus S mit $g_i(v_j) = \delta_{ij}$. Dann ist $\varphi(g_i) = e_i$ (wobei φ auf S ausgedehnt wird) und zu $(c_1, \ldots, c_m) \in L^m$ ist

$$\varphi(\sum_{i=1}^{m} c_i g_i) = \sum_{i=1}^{m} c_i \varphi(g_i) = (c_1, \ldots, c_m).$$

Sei $g = \sum_{i=1}^m c_i g_i$. Dann ist $\overline{g}^{G_L} \in \langle \mathcal{B}_{L,I_L,\leq} \rangle_L$, wobei G_L eine Gröbner-Basis von I_L ist. Sei etwa $g = h + \overline{g}^{G_L} =: h + r$, dann gilt $\varphi(g) = \varphi(r) = (c_1, \ldots, c_m)$, womit φ surjektiv ist.

Damit folgt die Abschätzung.

(b) Gelte $\sqrt{I} = I$. Wir zeigen φ aus (a) injektiv. Sei $r \in \langle \mathcal{B}_{I,\leq} \rangle$ (es ist $I = I_L$, da $K = L$) und sei $\varphi(r) = 0$. Damit verschwindet r auf $\mathcal{V}_L(I)$ und der Nullstellensatz liefert $r \in \sqrt{I} = I$. Da G eine Gröbner-Basis ist, folgt $r = 0$.

Sei nun $|\mathcal{B}_{I,\leq}| = m$ (wie in (a)). Dann ist φ injektiv, also gilt $f \in \sqrt{I} \Rightarrow f \in I$ (da $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$), womit $\sqrt{I} \subseteq I$ ist. Da $I \subseteq \sqrt{I}$ folgt $I = \sqrt{I}$.

□

Bemerkung 2.4.1.23. Genauere Informationen bei (a) mit Hilfe von Vielfachheit. Vergleiche Seminar, lokale Ringe.

Hilfssatz 2.4.1.24 (Mehrdimensionale Lagrange-Interpolation). *Seien $|K| = \infty$ und $v_1, \ldots, v_m \in K^n$ paarweise verschieden.*

(a) *Es gibt Polynome $g_1, \ldots, g_m \in K[x_1, \ldots, x_n]$ derart, dass*

$$g_i(v_j) = \delta_{ij} \qquad (*)$$

ist. Man findet sie durch Lagrange-Interpolation.

(b) *Es gibt ein $\ell \in K^{1\times n}$ so, dass $\ell^{\,t} v_i \neq \ell^{\,t} v_j$ gilt für $i \neq j$.*

(c) *Mit einem ℓ aus (b) und mit*

$$g_i = \prod_{\substack{j=1 \\ j\neq i}}^{m} \frac{\ell^{\,t}(x - v_j)}{\ell^{\,t}(v_i - v_j)}$$

gilt (∗). Dabei sei $x = (x_1, \ldots, x_n)$.

(d) *Seien $c_1, \ldots, c_m \in K$ vorgegeben. Dann gibt es ein $g \in K[x_1, \ldots, x_n]$ so, dass für $1 \leq i \leq m$ gilt*

$$g(v_i) = c_i.$$

(e) *Zur Eindeutigkeit in (d):*

Sei $J(v_1, \ldots, v_m) = \{f \in K[x_1, \ldots, x_n] : f(v_1) = \cdots = f(v_m) = 0\}$. Dann ist $g + J(v_1, \ldots, v_m)$ die Menge aller *Polynome h mit $h(v_1) = c_1, \ldots, h(v_m) = c_m$.*

Beweis. Die Implikationen (b) ⇒ (c) ⇒ (a) ⇒ (d) sind klar, und dem Leser sei (e) zur Übung überlassen. Nun zum Beweis von (b).

Sei $U = \bigcup_{\substack{i,j=1 \\ i\neq j}}^{m} (v_i - v_j)^{\perp}$.

Beachte: Es existiert ℓ in (b) genau dann, wenn $K^n \setminus U \neq \emptyset$.

Sei $f_{ij} = (v_i - v_j)^{\perp} x \in K[x_1, \ldots, x_n]$, und $f = \prod_{\substack{i,j=1 \\ i\neq j}}^{m} f_{ij}$. Dann ist $U \neq K^n \Leftrightarrow \mathcal{V}(f) \neq K^n$. Nun ist $f \neq 0$, und nach folgendem Lemma ist $\mathcal{V}(f) \neq K^n$, da $|K| = \infty$: □

Lemma 2.4.1.25. *Sei $|K| = \infty$ und $f \in K[x_1, \ldots, x_n] \setminus \{0\}$. Dann gibt es ein $v \in K^n$ mit $f(v) \neq 0$.*

Beweis. Induktion (Übung). Vergleiche auch unsere Lösung zu Aufgabenblatt 14. :-) □

Zur Bedeutung von $\sqrt{I}$.

Satz 2.4.1.26. *Unter der Voraussetzung* $\dim I = 0$ *gilt $\sqrt{I} = I$ genau dann, wenn $|\mathcal{V}_L(I)| = |\mathcal{B}_{I,\leq}|$.*

Weitere Informationen liefert das Shape-Lemma. Dazu erst folgende Definition:

Definition 2.4.1.27. *Sei I ein Ideal mit* $\dim I = 0$. *Dann ist I* in regulärer Position, *wenn für je zwei verschiedene Nullstellen $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n)$ über einem algebraisch abgeschlossenen Körper gilt $v_n \neq w_n$.*

Bemerkung 2.4.1.28. Über $\mathbb{Q}$ sind "fast" alle 0-dimensionalen Ideale in regulärer Position.
(Ohne Beweis.)

Lemma 2.4.1.29 (Shape-Lemma). *Sei K algebraisch abgeschlossen oder perfekt. Sei I in regulärer Position und $\sqrt{I} = I$. Dann gibt es $g_1, \ldots, g_n \in K[x_n]$ so, dass*

(i) *g_n quadratfrei ist,*

(ii) $\deg g_i < \deg g_n$ *für $i < n$ gilt und*

(iii) *die reduzierte Gröbner-Basis von I bezüglich $\leq_{lex}$ mit $x_1 > \cdots > x_n$ die Gestalt*

$$[x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)]$$

hat.

Beweis. In der Übung. □

Der Nachteil des Shape-Lemmas ist, dass es auf $\leq$ beruht.

Bemerkung 2.4.1.30. Es kann eine affin-lineare Variablentransformation ($x \mapsto A\,{}^{\mathrm{t}}x + b$ mit $A \in GL_n(K)$, $b \in K^n$) zur Herbeiführung der regulären Position genutzt werden.
Vergleiche [CCS99, Bd. 2, p. 26 f].

Ein Beispiel findet sich in dem MAPLE-Worksheet `MapleDemoÜbung`.

2.4.2 Zur Problematik algebraischer Gleichungssysteme

Hier den Beginn aus Kapitel 2 aus [CLO98] einfügen (Seiten 23 bis 34).

2.4.3 Berechnung von $\mathcal{B}_{I,\leq}$ und $\sqrt{I}$

Sei $\dim I = 0$. Zur Berechnung von $\mathcal{B}_{I,\leq}$ siehe Aufgabe 51 bzw. [CLO98]. Nun zur Berechnung von $\sqrt{I}$.

Satz 2.4.3.1. *Sei K perfekt und* $\dim I = 0$. *Dann ist für $1 \leq i \leq n$*

$$\{0\} \neq I \cap K[x_i] = \langle f_i \rangle_{K[x_i]} \neq K[x_i]$$

mit geeigneten $f_i \in K[x_i]$. Sei $\overline{f_i} = \frac{f_i}{\mathrm{ggT}(f_i, \frac{d}{dx_i} f_i)}$ der quadratfreie Anteil von f. Dann ist

$$\sqrt{I} = I + \left\langle \overline{f_1}, \ldots, \overline{f_n} \right\rangle_R .$$

Bemerkung: Die Formel ist einfach, jedoch ist der Beweis erstaunlich schwer.

Beweis. Sei $J := I + \left\langle \overline{f_1}, \ldots, \overline{f_n} \right\rangle$. Es gilt $I \subseteq J \subseteq \sqrt{I} \neq R$, wobei $J \subseteq \sqrt{I}$ durch Vergleich der Nullstellenmengen und $\sqrt{I} \neq R$ aufgrund $\dim I = 0$ folgt. Insbesondere gilt $\sqrt{J} = \sqrt{I}$. Wir zeigen nun $\sqrt{J} = J$ indem wir zeigen, dass J *Durchschnitt endlich vieler maximaler Ideale ist.*

Beachte: Ein maximales Ideal ist prim, und jedes Primideal ist radikal, und der Durchschnitt endlich vieler radikaler Ideale ist ebenfalls radikal (vergleiche Übung).

Der Beweis erfolgt durch Induktion nach n.

Anfang ($n = 1$): Sei $J = I + \left\langle \overline{f} \right\rangle$ mit $\overline{f}$ quadratfrei. Dann ist $J = \langle h \rangle$, h quadratfrei; es ist h assoziiert zu $\mathrm{ggT}(\overline{f}, g)$ wenn $I = \langle g \rangle$. Sei etwa $h = p_1 \cdots p_r$, wobei die p_i paarweise verschiedene Primelemente sind. Dann ist $J = \bigcap_{i=1}^{r} \langle p_i \rangle$, und da $K[x_i]$ Hauptidealbereich sind die $\langle p_i \rangle$ maximal.

Schluß ($n > 1$): Sei $\overline{f_n} = p_1 \cdots p_s$ in $K[x_n]$ mit p_i paarweise verschiedenen Primelementen.

Zwischenbehauptung: Es ist $J = J + \left\langle \overline{f_n} \right\rangle_R = \bigcap_{i=1}^{s} (J + \langle p_i \rangle_R)$. Der erste Teil ist auf Grund der Definition von J klar, und der zweite wird in Aufgabe 53 bewiesen.

Wir zeigen jetzt, dass $J + \langle p \rangle_R$ mit $p \in K[x_n]$ prim Durchschnitt endlich vieler maximaler Ideale ist. Zusammen mit der Zwischenbehauptung folgt dann die eigentliche Behauptung.

Beachte $A = \left\langle B_{\langle p \rangle, \leq} \right\rangle_K \cong K[x_n]/pK[x_n]$, wobei $A \subset K[x_n]$. (Es ist $A = \left\langle 1, x_n, \ldots, x_n^{d-1} \right\rangle_K$ wobei $d = \deg p$.) Betrachte nun die kanonische Abbildung $\varrho : K[x_n] \to A$, $f \mapsto \varrho(f) =$ Rest bei Division mit p.

Setze nun ϱ fort zu einem K-linearen surjektiven Ringhomomorphismus $\varrho : R = (K[x_1, \ldots, x_{n-1}])[x_n] \to A[x_1, \ldots, x_{n-1}]$ mit

$$\varrho\left(\sum_{i=0}^{\delta} c_n x_n^i\right) = \sum_{i=0}^{\delta} c_i \varrho(x_n^i).$$

Dann ist $\ker \varrho = pR$.

Nun liefert der Homomorphiesatz unter anderem eine Bijektion (genauer: einen Verbandsisomorphismus) zwischen

$$\{ \text{ Ideale in } R, \text{ die } pR \text{ enthalten } \} \qquad \text{und} \qquad \{ \text{ Ideale in } A[x_1, \ldots, x_{n-1}] \}$$

(vergleiche Jacobson: Basic Algebra 1).

Beachte, dass $\varrho(\overline{f_n}) = 0$ ist und $\varrho(\overline{f_i}) = \overline{f_i}$ für $1 \leq i \leq n-1$.

Nun sind $\varrho(I)$ und $H = \varrho(J + \langle p \rangle_R)$ Ideale in $A[x_1, \ldots, x_{n-1}]$. Dann ist $H = \varrho(I) + \left\langle \overline{f_1}, \ldots, \overline{f_{n-1}} \right\rangle$ mit $\overline{f_1}, \ldots, \overline{f_{n-1}} \in A[x_1, \ldots, x_{n-1}]$ quadratfrei.

Mit der Induktionsannahme ist nun $H = \bigcap_{j=1}^{r} \mathcal{M}_j$ mit maximalen Idealen $\mathcal{M}_j \subseteq A[x_1, \ldots, x_{n-1}]$. Nun sind ebenfalls $\varrho^{-1}(\mathcal{M}_j)$ maximale Ideale, da ϱ ein Verbandsisomorphismus zwischen den Idealverbänden ist. Da nun $\bigcap_{j=1}^{r} \varrho^{-1}(\mathcal{M}_j) = \varrho^{-1}(H) = J + \langle p \rangle_R$ ist nach dem Homomorphiesatz folgt die Behauptung. □

Bemerkung 2.4.3.2. Satz 2.4.3.1 liefert eine einfache Methode zur Berechnung von $\sqrt{I}$, wenn $\dim I = 0$ und K perfekt:

Bestimme $I \cap K[x_i] = \langle f_i \rangle$ und benutze die Formel aus Satz 2.4.3.1.

Beispiel 2.4.3.3. Ein MAPLE-Beispiel:

```
> restart:
> with(Groebner): read `zdimradi_neu.txt`;
```

Erzeuger des Ideals I:

```
> f1 := y^4 * x + 3 * x^3 - y^4 - 3 * x^2:
  f2 := x^2 * y - 2 * x^2 + 1 + z:
  f3 := 2 * y^4 * x - x^3 - 2 * y^4 + x^2:
  f4 := x^2 * y^2 * z^2:
> F := [f1, f2, f3, f4]:
```

Reduzierte Gröbner-Basis von I bezüglich $\leq_{gradlex}$:

```
> gbasis(F, tdeg(x,y,z));
```

$$[z^2-1+y+zy, x+xz-1-z, x^2y-2x^2+1+z, x^3-x^2, z^4-2z^3+4x^2+z^2-4, y^4+2z^3-12x^2-5z^2+4z+11]$$

Reduzierte Gröbner-Basis des Radikals von I bezüglich $\leq_{gradlex}$.

```
> gbasis(zdimradical(F,[x,y,z]),tdeg(x,y,z));
```

$$[-1 - z + 2x - y, z^2 + y - 1, zy, -y + y^2]$$

2.4.3.1 Basiskonversion

Wir betrachten nun den FGLM-Algorithmus (FGLM steht für die Namen Faugère, Gianni, Lazard und Mora). Dieser ist z. B. via `fglm` in MAPLE verfügbar.

Gegeben sei ein 0-dimensionales Ideal I in $R = K[x_1, \ldots, x_n]$, und zwei Monomordnungen $\leq$ und $\leq'$ auf $\mathbb{N}^n$. Sei weiter G eine Gröbner-Basis bezüglich $\leq$. Gesucht ist nun eine Gröbner-Basis G' bezüglich $\leq'$.

Dazu wird folgende Eigenschaft benutzt:

$$x^\alpha \in \mathrm{in}_\leq(I) \Leftrightarrow \exists c_1, \ldots, c_r \in K\ \exists \alpha^{(1)}, \ldots, \alpha^{(r)} \in \mathbb{N}^n : \alpha^{(i)} < \alpha \wedge x^\alpha - \sum_{i=1}^{r} c_i x^{\alpha^{(i)}} \in I$$

$$\Leftrightarrow \exists c_1, \ldots, c_r \in K\ \exists \alpha^{(1)}, \ldots, \alpha^{(r)} \in \mathbb{N}^n : \alpha^{(i)} < \alpha \wedge \overline{x^\alpha}^G = \sum_{i=1}^{r} c_i \overline{x^{\alpha^{(i)}}}^G.$$

Nun zur Beschreibung des Algorithmus:

1. Setze $G' := \emptyset$, $\mathcal{B}' := \{0\}$, $In' := \emptyset$, $\gamma := 0$, wobei $G' \subseteq R$, $\mathcal{B}', In' \subseteq \mathbb{N}^n$, $\gamma \in \mathbb{N}^n$.
2. Solange $M := \{\beta \in \mathbb{N}^n \mid \gamma < \beta\} \cap (\mathbb{N}^n \setminus \bigcup_{\alpha \in In'} C_\alpha^+) \neq \emptyset$ ist, tue folgendes:
   (a) Setze $\beta^* := \min_{\leq'} M$.
   (b) Ist $\overline{x^{\beta^*}}^G \in \left\langle \{\overline{x^\alpha}^G \mid \alpha \in \mathcal{B}'\} \right\rangle_K$, so tue folgendes:
      (i) Bestimmte $c_\alpha \in K$ mit $\overline{x^{\beta^*}}^G = \sum_{\alpha \in \mathcal{B}'} c_\alpha \overline{x^\alpha}^G$.
      (ii) Setze $g := x^{\beta^*} - \sum_{\alpha \in \mathcal{B}'} c_\alpha x^\alpha$,
      (iii) $G' := G' \cup \{g\}$ und
      (iv) $In' := In' \cup \{\beta^*\}$.
   (c) Ansonsten setze
      (i) $\mathcal{B}' := \mathcal{B}' \cup \{\beta^*\}$ und
      (ii) $\gamma := \beta^*$.

Korrektheit des FGML-Algorithmus:

- Der Algorithmus terminiert:
  - Da $\dim I = 0$ muss $\mathcal{B}'$ konstant werden.
  - Es wird $\bigcup_{\alpha \in In'} C_\alpha^+$ konstant.
- Also wird M nach endlich vielen Schritten berechnet.
- Per Konstruktion gilt: $\langle \{\mathrm{LM}_{\leq'}(g) \mid g \in G'\} \rangle = \mathrm{in}_{\leq'}(I)$:

  "$\subseteq$": Klar.

  "$\supseteq$": Sei $h \in I$, $x^\beta = \mathrm{LM}_{\leq'}(h)$. Annahme $x^\beta \notin \mathrm{in}_{\leq'}(I)$, Widerspruch zur Abbruchbedingung!

Beispiel 2.4.3.4. Das folgende Beispiel stammt aus einem Vorlesungsskript von Beatrice Amrheim, Tübingen 1995. Die Bearbeitung des Beispiels folgt allerdings dem FGLM-Algorithmus, wie er in der Vorlesung behandelt wurde.

Ein umfangreiches Beispiel wird in der MAPLE-Hilfedatei zu `fglm` (`fglm_algo` ab MAPLE 9) angeboten.

Gegeben: Eine $\leq_{gradlex}$-Gröbner-Basis $G = [x^2 + 2y^2, xy^2 - \frac{1}{2}y, y^4 + \frac{1}{4}xy]$.
Gesucht: Eine $\leq_{lex}$-Gröbner-Basis.

Die folgende Tabelle gibt die wichtigsten vom Algorithmus berechneten Größen an:

bearbeitete Monome	zugehörige Reste	G'	B'	In'
1	1	—	$[1]$	—
y	y	—	$[1, y]$	—
y^2	y^2	—	$[1, y, y^2]$	—
y^3	y^3	—	$[1, y, y^2, y^3]$	—
y^4	$-\frac{1}{4}xy$	—	$[1, y, y^2, y^3, y^4]$	—
y^5	$-\frac{1}{8}y$	$[y^5 + \frac{1}{8}y]$	—	$[y^5]$
x	x	—	$[1, y, y^2, y^3, y^4, x]$	—
xy	xy	$[y^5 + \frac{1}{8}y, 4y^4 + xy]$	—	$[y^5, xy]$
x^2	$-2y^2$	$[y^5 + \frac{1}{8}y, 4y^4 + xy, x^2 + 2y^2]$	—	$[y^5, xy, x^2]$

Damit ist

$$G' = [y^5 + \tfrac{1}{8}y, 4y^4 + xy, x^2 + 2y^2]$$

das Ergebnis, also eine $\leq_{lex}$-Gröbner-Basis von $\langle G \rangle_R$.

2.4.4 Eingenwert/-vektor-Methoden zur Lösung algebraischer Gleichungssysteme

Untersucht wird hier die "Feinstruktur von R/I." Sei nun stets K ein algebraisch abgeschlossener Unterkörper von $\mathbb{C}$.

Sei $\dim I = 0$ in $R = K[x_1, \ldots, x_n]$, $\leq$ eine Monomordnung auf $\mathbb{N}^n$, $\mathcal{B}_{I,\leq}$, G, $\mathcal{V}(I) = \mathcal{V}_K(I) = \{v^{(1)}, \ldots, v^{(k)}\}$ mit $k \in \mathbb{N}^+$ wie bisher. Sei weiter $A = \langle \mathcal{B}_{I,\leq} \rangle_K \cong R/I$. Sind $r, s \in A$, so ist $r \odot s := \varrho(rs) := \overline{rs}^G$.

Zu $f \in R$ sei $M_f : A \to A$, $r \mapsto \varrho(fr) = \overline{fr}^G$. Es ist M_f K-linear. Betrachte die Matrix von M_f (in $K^{m \times m}$, wobei $m = |\mathcal{B}_{I,\leq}|$) bezüglich der kanonischen Basis $\mathcal{B}_{I,\leq}$ geordnet mit $\leq$.

Erinnere: $\mathrm{End}_K(A) \cong K^{m \times m}$ bei fester Basis.

Beispiel 2.4.4.1. Es geht darum, in einem ganz einfachen Fall zu zeigen, wie man eine Matrixdarstellung M_f gewinnt für die Multiplikation mit f in R/I.

Das Ideal I sei gegeben durch die Polynomliste $F = [f_1, f_2, f_3]$ in den Variablen $X = [x, y]$ mit rationalen Koeffizienten:

$$f_1 = xy^2 + x^2 - xy - 2y^2 - 3x + 2y + 2, f_2 = xy - x - 2y + 2, f_3 = -2xy + y^2 + 4x - y - 2.$$

Die Basis $\mathcal{B}$ von R/I bezüglich $\leq_{gradlex}$ (`tdeg` in MAPLE) – in aufsteigender Reihenfolge bezüglich $\leq_{gradlex}$ sortiert – ist

$$B = [1, y, x].$$

Sei nun als willkürliches Beispiel f wie folgt gegeben:

$$f := x^2 + y^2.$$

Die Bilder der Basispolynome bei Multiplikation mit f können über den Divisionsalgorithmus mit einer $\leq_{gradlex}$-Gröbner-Basis des von $[f_1, f_2, f_3]$ erzeugten Ideals bestimmt werden. Im Beispiel ist

$$G = [y^2 + 2x - 5y + 2, xy - x - 2y + 2, x^2 - 3x + 2].$$

Damit berechnet man

$$\overline{f \cdot 1}^G = 5y + x - 4, \quad \overline{f \cdot y}^G = -9x + 23y - 12, \quad \overline{f \cdot x}^G = 4x + 10y - 12.$$

Die Matrix M_f lautet daher

$$M_f = \begin{pmatrix} -4 & -12 & -12 \\ 5 & 23 & 10 \\ 1 & -9 & 4 \end{pmatrix}.$$

Im Kontext von Abschnitt 2.4.4 sind die Matrizen M_x und M_y wichtiger. Zur Bestimmung von M_x: Es ist

$$\overline{x \cdot 1}^G = x, \quad \overline{x \cdot y}^G = x + 2y - 2, \quad \overline{x \cdot x}^G = 3x - 2.$$

Die Matrix M_x lautet daher

$$M_x = \begin{pmatrix} 0 & -2 & -2 \\ 0 & 2 & 0 \\ 1 & 1 & 3 \end{pmatrix}.$$

Nun zur Bestimmung von M_y: Es ist

$$\overline{y \cdot 1}^G = y, \quad \overline{y \cdot y}^G = -2x + 5y - 2, \quad \overline{y \cdot x}^G = x + 2y - 2.$$

Die Matrix M_y lautet daher

$$M_y = \begin{pmatrix} 0 & -2 & -2 \\ 1 & 5 & 2 \\ 0 & -2 & 1 \end{pmatrix}.$$

Natürlich kann man diesen Prozess auch automatisieren.

Beobachtung 2.4.4.2.

(a) Die Abbildung $M : R \to \mathrm{End}_K(A)$, $f \mapsto M_f$ ist ein Ringhomomorphismus (und K-linear).

(b) Es ist $\operatorname{Ker} M = I$.

(c) Es ist $M|_{\langle \mathcal{B}_{I,\leq} \rangle_K}$ injektiv. (D. h. Bild M ist isomorph zu einem kommutativen Unterring von $K^{m \times m}$.)

(d) Mit $h \in K[t]$ und $f \in R$ gilt $M_{h(f)} = h(M_f)$.

Beweis.

(a) Es sind $M_0 = 0$ und $M_1 = \mathbf{id}$. Weiterhin ist $M_{f+g}(r) = \varrho((f+g)r) = \varrho(fr + gr) = \varrho(fr) + \varrho(gr) = M_f(r) + M_g(r)$, und $M_{fg}(r) = \varrho(fgr) = \varrho(f\varrho(gr)) = M_f(M_g(r))$ für $r \in A$. Weiterhin ist $M_{\lambda f}(r) = \varrho(\lambda f r) = \lambda \varrho(fr) = \lambda M_f(r)$ für $\lambda \in K$.

(b) **"$\supseteq$":** Sei $f \in I$. Es ist $M_f(r) = \varrho(fr) = 0$, da $fr \in I$, womit $M_f = 0$ ist.
"$\subseteq$": Ist $M_f = 0$, so ist $M_f(1) = \varrho(f) = 0$, womit $f \in I$ ist.

(c) Es ist $\langle \mathcal{B}_{I,\leq} \rangle_K \cap I = \{0\}$.

(d) Folgt aus (a): Ist $h = \sum_{i=0}^{\ell} c_i t^i$, so gilt $M_{h(f)}(r) = M_{\sum c_i f^i}(r) = \sum c_i (M_f(r))^i = h(M_f(r))$, $r \in A$.

□

Betrachte die Minimalpolynome der M_f: $f \mapsto M_f \mapsto h_f :=$ Minimalpolynom von f.
Erinnere: Das Minimalpolynom teilt das charakteristische Polynom.

Satz 2.4.4.3. *Seien $f \in R$ und h_f das Minimalpolynom von M_f. Dann sind äquivalent:*

(a) *Es ist $\lambda \in K$ eine Nullstelle von h_f;*

(b) *Es ist λ ein Eigenwert von M_f;*

(c) *Es ist $\lambda \in f(\mathcal{V}(I))$.*

Hilfssatz 2.4.4.4. *Mit $g \in R$ gilt $0 \notin g(\mathcal{V}(I)) \Leftrightarrow \varrho(g)$ invertierbar in A.*

Beweis. **"$\Leftarrow$":** Sei $g^* \in A \setminus \{0\}$ mit $\varrho(gg^*) = 1$. Dann ist $g^*g - 1 \in I$, und somit $0 \notin g(\mathcal{V}(I))$.
"$\Rightarrow$": Sei $0 \notin g(\mathcal{V}(I))$, $g(v^{(i)}) \neq 0$, $1 \leq i \leq k$. Sei g^* (Interpolation) ein Polynom mit $g^*(v^{(i)}) = \frac{1}{g(v^{(i)})}$. Dann ist $(g^*g - 1)(v^{(i)}) = 0$, womit mit Hilfe des Nullstellensatzes $g^*g - 1 \in \sqrt{I}$ folgt. Sei etwa $(g^*g - 1)^\ell \in I$, $\ell \in \mathbb{N}_+$. Ausmultiplizieren liefert $(g^*g - 1)^\ell = \tilde{g}g - 1$ mit $\tilde{g} \in R$. Damit folgt $\varrho(\tilde{g}g - 1) = 0$, und damit ist $\varrho(g)$ invertierbar in A. □

Beweis von Satz 2.4.4.3. **(a) ⇔ (b):** Klar nach Lineare Algebra II.
(b) ⇒ (c): Koordinatenform: λ ist ein Eigenwert des Endomorphismus M_f genau dann, wenn es ein $r \in A \setminus \{0\}$ gibt mit $(M_f - \lambda \mathbf{id})(r) = 0$. Es gilt dann $M_{(f-\lambda)}(r) = \varrho((f-\lambda)r) = 0$. Setze $g := f - \lambda$.

Annahme: Es ist $g(v^{(i)}) \neq 0$ für alle i. Nach Hilfssatz 2.4.4.4 gibt es dann ein $g^* \in R$ mit $\varrho(g^* g) = 1$. Nun ist $\varrho(g^* g r) = \varrho(r) = r$ für $r \in A$ und $\varrho(g^* g r) = \varrho(\varrho(g^*)\varrho(gr)) = \varrho(\varrho(g^*)0) = 0$, Widerspruch zu $r \in A \setminus \{0\}$.

Also muss $g(v^{(i)}) = 0$ sein für ein i, womit $f(v^{(i)}) = \lambda$ folgt.
(c) ⇒ (a): Sei $v \in V(I)$ mit $f(v) = \lambda$. Es ist $h_f(M_f) = 0$ (Cayley-Hamilton), also (Beobachtung 2.4.4.2(d)) gilt $M_{h_f(f)} = 0$, womit $h_f(f) \in I$ ist. Damit gilt $0 = h_f(f)(v) = h_f(f(v)) = h_f(\lambda)$. □

Satz 2.4.4.5. *Die Eigenwerte von M_{x_i} sind die i-ten Komponenten v_i der Lösungen $v \in \mathcal{V}(I)$. Außerdem ist*

$$\langle h_{x_i}(x_i) \rangle_{K[x_i]} = I \cap K[x_i], \qquad 1 \leq i \leq n.$$

Beweis. Der erste Teil ist klar (folgt direkt aus Satz 2.4.4.3), und für den zweiten Teil benutze $0 = h(M_{x_i}) = M_h(x_i) \Leftrightarrow h(x_i) \in I$ für alle $h \in K[t]$. □

Bemerkung 2.4.4.6. Satz 2.4.4.5 liefert zweierlei:

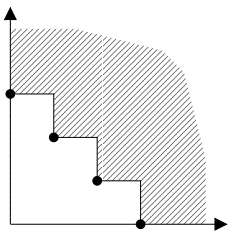
- Ein Verfahren zur Lösung algebraischer Gleichungssysteme;
- Ein Verfahren zur Berechnung von $I \cap K[x_i]$.

Beispiele 2.4.4.7.

(a) $n = 1$

(b) Siehe Übung, Form nach Shape-Lemma.

(c) Monomideal, $n = 2$, $\dim I = 0$, $\leq_{lex}$, $x > y$. Sei $I = \langle y^3, x^3, xy^2, x^2 y \rangle$ und $\mathcal{B}_{I,\leq} = [1, y, y^2, x, xy, x^2]$.



Es ist

$$M_x = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$\mathcal{V}(I) = \{0\}$, $\sqrt{I} = \{f \in K[x,y] \mid f(0) = 0\} = \langle x, y \rangle_K$.

Zur Bestimmung von $\mathcal{V}(I)$ für Ideale mit $\dim I = 0$ vergleiche [CLO98], "Hilbertpolynom".

Bemerkung 2.4.4.8. Für ein Verfahren mit Hilfe von Satz 2.4.4.5 siehe das MAPLE-Demo. Vorteil gegenüber Elimination:

- $\leq$ beliebig;
- nicht rekursiv.

Nachteile vielleicht bei grossen n:

- Rekonstruktion der Lösungen.

Letzters entfällt, wenn man zuerst $\sqrt{I}$ bestimmt und dann die Eigenvektoren von ${}^{\mathrm{t}}M_{x_i}$ benutzt.

Satz 2.4.4.9. *Sei $I = \sqrt{I}$ und $f \in R$. Sei $f|_{\mathcal{V}(I)}$ injektiv, $\mathcal{B}_{I,\leq} = \{x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}\}$ mit $x^{\alpha^{(1)}} = 1$ (ohne Einschränkung), und sei $\dim I = 0$. Dann gilt*

$$\mathrm{Eig}({}^{\mathrm{t}}M_f, f(v)) = \left\langle {}^{\mathrm{t}}\left(v^{\alpha^{(1)}}, \ldots, v^{\alpha^{(m)}}\right) \right\rangle_K, \quad v \in \mathcal{V}(I),$$

wobei $v^\alpha = \prod v_i^{\alpha_i}$, und

$$K^m = \bigoplus_{v \in \mathcal{V}(I)} \mathrm{Eig}({}^{\mathrm{t}}M_f, f(v)).$$

Beweis. Sei etwa $M_f = (a_{ij})$. Es entspricht M_f der Multiplikation mit f in A:

$$\varrho(f x^{\alpha^{(j)}}) = \sum_{i=1}^{m} a_{ij} x^{\alpha^{(i)}}, \quad 1 \leq j \leq m.$$

Einsetzen von $v \in \mathcal{V}(I)$ liefert

$$f(v) v^{\alpha^{(j)}} = \sum_{i=1}^{m} a_{ij} v^{\alpha^{(i)}}$$

und somit

$$f(v)(v^{\alpha^{(1)}}, \ldots, v^{\alpha^{(m)}}) = (v^{\alpha^{(1)}}, \ldots, v^{\alpha^{(m)}}) M_f,$$

und da $v^{\alpha^{(1)}} = 1$ folgt $(v^{\alpha^{(1)}}, \ldots, v^{\alpha^{(m)}}) \neq 0$. Also ist $(v^{\alpha^{(1)}}, \ldots, v^{\alpha^{(m)}})$ Eigenvektor von ${}^{\mathrm{t}}M_f$ zum Eigenwert $f(v)$. Da $\sqrt{I} = I$ (also $|\mathcal{B}| = |\mathcal{V}(I)|$) und $f|_{\mathcal{V}(I)}$ injektiv folgt der Rest mit Linearer Algebra I/II. □

Hinweis: Die Eigenwerte von M_f sind gerade die Eigenwerte von ${}^{\mathrm{t}}M_f$.

Wir betrachten nun ein

EW/EV-Verfahren zur Lösung 0-dimensionaler algebraischer Gleichungssysteme:

1. Lege $\leq$ fest mit $x_1 > \cdots > x_n$.
2. Berechne eine reduzierte Gröbner-Basis von $\sqrt{I}$ mit $\mathcal{B} = \{x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}\}$, wobei $\alpha^{(1)} = 0$.
3. Wähle $f = c_1 x_1 + \cdots + c_n x_n$ mit zufälligen $c_i \in \mathbb{Z}$. (Es ist sehr wahrscheinlich, dass f injektiv auf $\mathcal{V}(I)$ ist. Siehe dazu auch weiter unten.)
4. Berechne M_f.
5. Berechne Eigenraumzerlegung für ${}^{\mathrm{t}}M_f$. Hier zeigt sich, ob f "gut" war (gegebenenfalls Wiederholen).
6. Ergebnis zu gutem f: m linear unabhängige Eigenvektoren $w^{(1)}, \ldots, w^{(m)}$ von ${}^{\mathrm{t}}M_f$ zu paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_m$.

   Etwa zu $w^{(1)}$ existiert ein $v \in \mathcal{V}(I)$ derart, dass $w^{(1)} = c_1(v^{\alpha^{(1)}}, \ldots, v^{\alpha^{(m)}})$ ist. Da $\alpha^{(1)} = 0$ folgt $w_1^{(1)} = c_1$. Ersetze $w^{(1)}$ durch $w^{(1)}(w_1^{(1)})^{-1}$.

   Fallunterscheidung:

   (a) $x_i \in \mathcal{B}$ für alle $i = 1, \ldots, n$, d. h. zu jedem i gibt es ein $\alpha \in \{\alpha^{(1)}, \ldots, \alpha^{(m)}\}$ mit $x^\alpha = x_i$. Dann ist $v^{\alpha^{(i)}} = v_i$. Man erhält so alle v_i.

(b) Sei $x_i \notin \mathcal{B}$ für ein $1 \leq i \leq n$. Sei $J := \{i \in \{1, \ldots, n\} \mid x_i \notin \mathcal{B}\} = \{i_1, \ldots, i_\ell\} \neq \emptyset$. Ohne Einschränkung sei $i_1 > \cdots > i_\ell$. Zu x_{i_k} mit $i_k \in J$ gibt es $g_k \in I$ mit

$$g_k = x_{i_k} + \tilde{g}_k, \qquad \mathrm{LT}(g_k) = x_{i_k}.$$

Behauptung: Es ist $\tilde{g}_k \in K[\{x_i \mid i > i_k\}]$. Annahme: $\tilde{g}_k$ enthält Monom der Form $x_j x^\alpha$, $j < i$. Dann kann nicht gelten $x_j > x_i$. Also folgt die Behauptung.

Nun wird wie folgt iteriert:

$$g_1 = x_{i_1} + \tilde{g}_1 \text{ mit } \tilde{g}_1 \in K[\{x_j \mid j > i_1\}].$$

Ist $i_1 = n$, so gilt $\tilde{g}_1 \in K$, ansonsten bestimme v_i wie in (a) und dann $v_{i_1} = -\tilde{g}_1(v_{i+1}, \ldots, v_n)$.

Beispiel 2.4.4.10. Siehe MAPLE-Demo.

Bemerkung 2.4.4.11 (zu f). Veranschaulichung im $\mathbb{R}^n$, Spezialfall $n = 2$.

Sei $V = \{v^{(1)}, v^{(2)}\}$, $f_\omega(x) = {}^{\mathrm{t}}\omega x$ mit $\|\omega\| = 1$, etwa $\omega = e^{\mathbf{i}\varphi}$ (es wird $\mathbb{C}$ mit $\mathbb{R}^2$ identifiziert). Sei

$$\Omega = \{\varphi \in [0, 2\pi[\mid f_\omega|_{\mathcal{V}(I)} \text{ nicht injektiv } \}.$$

Bei einer Gleichverteilung auf $[0, 2\pi]$ gilt $P(\Omega) = 0$. Vergleiche Abbildung 2.10.

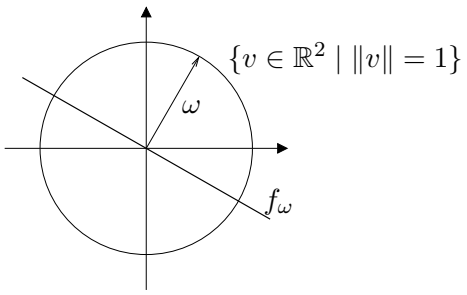


Abbildung 2.10: Veranschaulichung der fast sicheren Injektivität im $\mathbb{R}^2$

(Unser Verfahren wird dadurch bestätigt.)

Jedoch ist f deterministisch bestimmbar mit

Lemma 2.4.4.12. *Sei $\mathcal{V}$ eine endliche Teilmenge von $\mathbb{C}^n$, etwa $|\mathcal{V}| = d > 0$. Die endliche Menge*

$$\mathcal{F} := \{x_1 + ix_2 + \cdots + i^{n-1}x_n \mid 0 \leq i \leq \tfrac{1}{2}(n-1)d(d-1), i \in \mathbb{N}\}$$

enthält ein f mit $f|_{\mathcal{V}}$ injektiv.

Beweis. Sei $f_i := x_1 + ix_2 + \cdots + i^{n-1}x_n \in \mathcal{F}$. Seien $u, v \in V$, $u \neq v$ und es gelte $f_i(u) = f_i(v)$. Dann folgt

$$0 = \sum_{k=1}^{n} (u_k - v_k) i^{k-1},$$

also ist i Nullstelle von $\sum_{k=1}^{n}(u_k - v_k)x^{k-1}$. Es gibt $\frac{1}{2}d(d-1)$ Teilmengen $\{u, v\} \subseteq V$ mit $u \neq v$. Jedes Polynom $\sum(u_k - v_k)x^{k-1}$ hat höchstens $n-1$ Nullstellen. Insgesamt gibt es höchstens $\frac{1}{2}(n-1)d(d-1)$ Wahlen von i, die ungeeignet sind. Aber: $|\mathcal{F}| > \frac{1}{2}(n-1)d(d-1)$! $\square$

2.4.5 Eingrenzung reeller Lösungen

Sei nun stets $K \subseteq \mathbb{R}$. Sei $\mathcal{V}_{\mathbb{R}}(I) = \mathcal{V}_{\mathbb{C}}(I) \cap \mathbb{R}^n$.

Beispiele von Gebieten, die wir zulassen wollen:

Sei $0 \neq h \in R$, dann ist

$$\mathbb{R}^n = H_h^- \dot\cup \mathcal{V}_{\mathbb{R}}(h) \dot\cup H_h^+, \qquad (*)$$

wobei $H_h^+ = \{v \in \mathbb{R}^n \mid h(v) > 0\}$ und $H_h^- = \{v \in \mathbb{R}^n \mid h(v) < 0\}$.

Beispiele 2.4.5.1.

(a) Sei $n = 1$, $h = (x-a)(x-b)$ mit $a < b$. Dann ist $\mathcal{V}_{\mathbb{R}}(h) = \{a, b\}$, $H_h^+ = \mathbb{R} \setminus [a, b]$ und $H_h^- =]a, b[$.

(b) Sei $n = 2$, $h = \underbrace{(x^2+y^2-1)}_{=:h_1}\underbrace{(x^2+y^2-2)}_{=:h_2}$. Dann ist $\mathcal{V}_{\mathbb{R}}(h) = \mathcal{V}_{\mathbb{R}}(h_1) \cup \mathcal{V}_{\mathbb{R}}(h_2)$. Weiterhin ist $H_h^+ = \{v \in \mathbb{R}^2 \mid \|v\|_2 < 1 \vee \|v\|_2 > \sqrt{2}\}$ und $H_h^- = \{v \in \mathbb{R}^2 \mid 1 < \|v\|_2 < \sqrt{2}\}$. (Siehe Abbildung 2.11.)

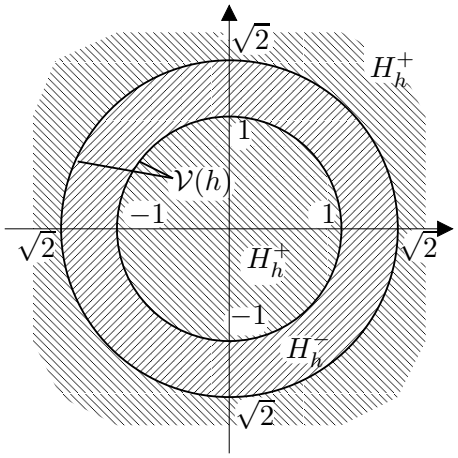


Abbildung 2.11: Die Mengen H_h^+, H_h^- und $\mathcal{V}(h)$ zu $h = h_1 h_2$

(c) Seien $n = 2$, $a < b$ und $c < d$. Setze $h_1 = (x-a)(x-b)$ und $h_2 = (y-c)(y-d)$. Es ist $H_{h_1}^- \cap H_{h_2}^- = \{(u, v) \in \mathbb{R}^2 \mid a < u < b \wedge c < v < d\}$. (Siehe Abbildung 2.12.)

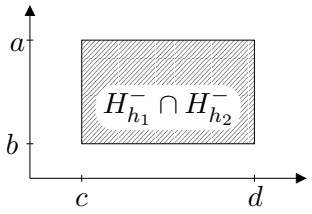


Abbildung 2.12: Die Menge $H_{h_1}^- \cap H_{h_2}^-$ zwei Polynomen h_i wie in (a)

Eine symmetrische Bilinearform auf R und A: Zu $f, g \in R$ sei

$$S(f, g) := \operatorname{Spur}(M_f M_g) = \operatorname{Spur}(M_{fg}) \in K$$

eine symmetrische Bilinearform. Über $\mathbb{C}$ gilt

$$\operatorname{Spur} A = \sum_{\lambda \text{ EW von } A} \lambda \cdot \underbrace{\nu_\lambda(p_A)}_{\text{Vielfachheit}} .$$

Beachte: Ist A symmetrisch, so sind die Eigenwerte reell.

Zu $h \in R$ und $f, g \in R$ sei

$$S_h(f,g) := \operatorname{Spur} M_{fgh}$$

eine symmetrische Bilinearform. Es ist $S_1 = S$.
Beachte: Eigentlich ist S_h Bilinearform auf A, da die Funktionswerte bei Änderungen modulo I konstant bleiben.

Wir betrachten nun die Matrix von S_h auf A bezüglich $\mathcal{B}_{I,\leq}$:

$$MS_h := \left(S_h(x^{\alpha(i)}, x^{\alpha(j)})\right)_{1\leq i,j\leq m},$$

wobei $m = |\mathcal{B}_{I,\leq}|$ und $\mathcal{B}_{I,\leq} = \{x^{\alpha(1)}, \ldots, x^{\alpha(m)}\}$.
Erinnerung: Sei S symmetrische Matrix über K und p die Anzahl der positiven Eigenwerte (mit Vielfachheiten) und q die Anzahl der negativen Eigenwerte (mit Vielfachheiten). Dann heißt p der *Trägheitsindex*, q der *Morseindex* und $\sigma(S) := p - q$ die *Signatur* von S. Es ist $p + q = \operatorname{rang} S$.

Satz 2.4.5.2 (Sylvesterscher Trägheitssatz). *Seien S, p und q wie gerade. Dann sind p und q invariant bei Transformationen der Art $M \to PM\,{}^{\mathrm{t}}P$ mit $P \in GL_m(K)$.*

Beispiele 2.4.5.3. Beispiele von Matrizen MS_h verschiedener Bilinearformen S_h und deren Signaturen. Als Basis dient jeweils die aufsteigend geordnete Standardmonombasis $\mathcal{B}$.

(a) Mit dem Ideal aus Beispiel 4.4.1. Sei $I := \langle f_1, f_2, f_3\rangle$ mit $f_1 = xy^2+x^2-xy-2y^2-3x+2y+2$, $f_2 = xy - x - 2y + 2$ und $f_3 = -2xy + y^2 + 4x - y - 2$, und $F = [f_1, f_2, f_3]$, $X = [x, y]$.

Die Gröbner-Basis G von I ist

$$G = [y^2 + 2x - 5y + 2, xy - x - 2y + 2, x^2 - 3x + 2],$$

und die nach der Monomordnung $\leq_{gradlex}$ (`tdeg` in MAPLE) sortierte Standardmonombasis ist

$$\mathcal{B} = [1, y, x].$$

Die Matrizen MS_h der Bilinearformen S_h für $h = 1, f, f^2$ mit $f = x(x-1)$ und deren Signaturen:

(i) Für $h = 1$ ist

$$MS_h = \begin{pmatrix} 3 & 6 & 5 \\ 6 & 14 & 11 \\ 5 & 11 & 9 \end{pmatrix},$$

und das charakteristische Polynom lautet

$$t^3 - 26t^2 + 13t - 1.$$

Es ist 0 kein Eigenwert, alle Nullstellen müssen reell sein, es finden drei Vorzeichenwechsel statt, also ist $\sigma(M_h) = 3$.

(ii) Für $h = f$ ist

$$MS_h = \begin{pmatrix} 4 & 10 & 8 \\ 10 & 26 & 20 \\ 8 & 20 & 16 \end{pmatrix},$$

und das charakteristische Polynom lautet

$$t^3 - 46t^2 + 20t.$$

Es ist 0 ein Eigenwert, alle Nullstellen müssen reell sein, es finden zwei Vorzeichenwechsel statt, also ist $\sigma(M_h) = 2$.

(iii) Für $h = f^2$ ist

$$MS_h = \begin{pmatrix} 8 & 20 & 16 \\ 20 & 52 & 40 \\ 16 & 40 & 32 \end{pmatrix},$$

und das charakteristische Polynom lautet

$$t^3 - 92t^2 + 80t.$$

Wie gerade stellt man fest, dass ebenfalls $\sigma(M_h) = 2$ ist.

(b) Für ein weiteres Beispiel siehe Aufgabe 60.

Satz 2.4.5.4. *Es sei I ein Ideal in R mit $\dim I = 0$ (beachte $K \subseteq \mathbb{R}$), und sei $h \in R$. Dann gilt*

(a) $\sigma(S_h) = \left|\mathcal{V}_{\mathbb{R}}(I) \cap H_h^+\right| - \left|\mathcal{V}_{\mathbb{R}}(I) \cap H_h^-\right|$ *und*

(b) $\operatorname{rang} MS_h = |\{v \in \mathcal{V}(I) \mid h(v) \neq 0\}|$.

Wir benutzten einen Satz von Stickelberger (1850–1936):

Satz 2.4.5.5 (Stickelberger). *Sei I ein 0-dimensionales Ideal in R und sei $h \in R$. Dann gilt*

(a) *Die Eigenwerte von MS_h sind die Elemente von $h(\mathcal{V}(I))$.*

(b) *Es ist* $\det MS_h = \prod_{v \in \mathcal{V}(I)} h(v)^{\mu(v)}$.

(c) *Weiter ist* $\operatorname{Spur} MS_h = \sum_{v \in \mathcal{V}(I)} \mu(v) h(v)$.

(d) *Es ist* $\operatorname{CharPoly}(MS_h) = \prod_{v \in \mathcal{V}(I)} (t - h(v))^{\mu(v)}$.

Dabei ist $\mu(v)$ die "Vielfachheit" der Nullstelle v; vergleiche [CLO98].

Eine ganz anders aussehende Version (in Wirklichkeit äquivalent) findet sich zum Beispiel in [CCS99, p. 47]. Die obige Version findet sich etwa in [BPR03, p. 128]. Vergleiche auch [SS88, S. 795 ff].

Beweis von Satz 2.4.5.4. Seien $\mathcal{B}_{I,\leq} = \{x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}\}$ mit $m = |\mathcal{B}_{I,\leq}|$, $\mathcal{V}(I) = \{v^{(1)}, \ldots, v^{(d)}\}$ mit $d = |\mathcal{V}(I)|$. Es ist $d \leq m$.

zu (b) Stickelberger Teil (c) für $hx^{\alpha^{(i)}} x^{\alpha^{(k)}}$ ergibt für den (i,k)-Eintrag von MS_h

$$\begin{aligned} &\operatorname{Spur} M_{hx^{\alpha^{(i)}} x^{\alpha^{(k)}}} \\ &= \sum_{v \in \mathcal{V}(I)} \mu(v) h(v) v^{\alpha^{(i)}} v^{\alpha^{(k)}} \\ &= \sum_{j=1}^{d} \mu(v^{(j)}) h(v^{(j)}) (v^{(j)})^{\alpha^{(i)}} (v^{(j)})^{\alpha^{(k)}}. \end{aligned}$$

Man sieht, dass mit

$$D = \begin{pmatrix} \mu(v^{(1)}) h(v^{(1)}) & & 0 \\ & \ddots & \\ 0 & & \mu(v^{(d)}) h(v^{(d)}) \end{pmatrix}$$

und

$$P = \left((v^{(j)})^{\alpha^{(i)}} \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq d}} \in \mathbb{C}^{m \times d}$$

gilt

$$P D\, {}^{\mathrm{t}}P = MS_h.$$

Es ist $\operatorname{rang} D = |\{v \in \mathcal{V}(I) \mid h(v) \neq 0\}|$. Wir zeigen $\operatorname{rang} P D\, {}^{\mathrm{t}}P = \operatorname{rang} D$.

Erinnere: Es ist $I \subseteq \sqrt{I}$, $\mathrm{in}_\leq(\sqrt{I}) \supseteq \mathrm{in}_\leq(I)$, aber $\mathcal{B}_{\sqrt{I},\leq} \subseteq \mathcal{B}_{I,\leq}$. Sei ohne Einschränkung $\mathcal{B}_{\sqrt{I},\leq} = \{x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(d)}}\}$. Sei weiterhin $P = \begin{pmatrix} P_d \\ \tilde{P} \end{pmatrix}$ mit $P_d \in \mathbb{C}^{d\times d}$. Wir zeigen $P_d \in GL_d(K)$.

Sei $c \in \mathbb{C}^d$ mit ${}^{\mathrm{t}}cP_d = 0$. Mit anderen Worten: $\sum_{i=1}^d c_i (v^{(j)})^{\alpha^{(i)}} = 0$ für $1 \leq j \leq d$. Nun gilt

$$\begin{aligned} 0 &= \sum_{i=1}^d c_i (v^{(j)})^{\alpha^{(i)}} \\ &= \sum_{i=1}^d c_i x^{\alpha^{(i)}}(v^{(j)}) \\ &= \left(\sum_{i=1}^d c_i x^{\alpha^{(i)}}\right)(v^{(j)}), \end{aligned}$$

womit nach dem Nullstellensatz, starke Variante, gilt $\sum_{i=1}^d c_i x^{\alpha^{(i)}} \in \sqrt{I}$. Da die $x^{\alpha^{(i)}} \in \mathcal{B}_{\sqrt{I},\leq}$ sind folgt $c_i = 0$, also $c = 0$.

Damit ist $\operatorname{rang} P_d = d$. Nun gibt es ein $U \in GL_m(\mathbb{C})$ mit $UP = \begin{pmatrix} E_d \\ 0 \end{pmatrix}$ und

$$(UP)D\,{}^{\mathrm{t}}(UP) = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

womit die Behauptung folgt.

zu (a) **Fall 1:** Alle Nullstellen sind reell, d. h. $\mathcal{V}(I) \subseteq \mathbb{R}^n$. Dann sind P und D aus (b) reelle Matrizen, und $\sigma(S_h) = \sigma(D)$ nach dem Trägheitssatz, womit die Behauptung folgt.

Fall 2: Sei $\mathcal{V}(I) \setminus \mathbb{R}^n \neq \emptyset$. Ohne Einschränkung sei $v^{(1)}, \ldots, v^{(2s)} \in \mathbb{C}^n \setminus \mathbb{R}^n$ und $v^{(2i)} = \overline{v^{(2i-1)}}$, $i \leq s$, und $v^{(i)} \in \mathbb{R}^n$ für $i > 2s$. Sei $p^{(j)}$ die j-te Spalte von P. Dann ist

$$p^{(j)} = {}^{\mathrm{t}}\Big((v^{(j)})^{\alpha^{(1)}}, \ldots, (v^{(j)})^{\alpha^{(m)}}\Big).$$

Nach obiger Nummerierung gilt $p^{(2i)} = \overline{p^{(2i-1)}}$, $i \leq s$.

Fall eines einzigen konjugierten Paars: Es ist

$$[p, \overline{p}] \underbrace{\begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\mathbf{i} \\ \frac{1}{2} & \frac{1}{2}\mathbf{i} \end{pmatrix}}_{=:Q} = [\Re p, \Im p],$$

und $Q^{-1} = \begin{pmatrix} 1 & 1 \\ \mathbf{i} & -\mathbf{i} \end{pmatrix}$, und

$$(Q^{-1}) \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix} {}^{\mathrm{t}}(Q^{-1}) = \begin{pmatrix} 2a & -2b \\ -2b & -2a \end{pmatrix} =: W,$$

falls $z = a + \mathbf{i}b$, $a, b \in \mathbb{R}$.

Im Produkt $PD\,{}^{\mathrm{t}}P$ angewendet ergibt sich

$$(P \underbrace{\begin{pmatrix} Q^{(1)} & & & & & \\ & \ddots & & & & \\ & & Q^{(s)} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}}_{=:U})U^{-1}D\,{}^{\mathrm{t}}U^{-1}\,{}^{\mathrm{t}}(PU) = (PU)(U^{-1}D\,{}^{\mathrm{t}}U^{-1})\,{}^{\mathrm{t}}(PU),$$

wobei PU und $U^{-1}D^{\mathrm{t}}U^{-1}$ reell sind.

Weiter ist $\mathrm{CharPoly}(W) = t^2 - 4(a^2+b^2)$ mit $a^2+b^2 = |z|^2 \neq 0$, also $\sigma(W) = 0$. (W hat die Eigenwerte $2\sqrt{a^2+b^2}$ und $-2\sqrt{a^2+b^2}$.)

□

Um Satz 2.4.5.4 anzuwenden, brauchen die Eigenwerte nicht berechnet zu werden:

Sonderfall der Regel von Descartes: Die Anzahl der positiven Eigenwerte von MS_h ist die Anzahl der Vorzeichenwechsel bei den Koeffizienten von $\mathrm{CharPoly}(MS_h)$ (ohne die 0-Koeffizienten).

Beispiel 2.4.5.6. Siehe Aufgabe 60.

Schlussbemerkungen: Andere Methoden der Nullstelleneingrenzung:

- Shape Lemma → Eingrenzungsmethode für eine Variable (z. B. Sturmsche Ketten, Thom-Codes, etc.)
- Einvariablenmethoden anwenden auf Erzeuger von $I \cap K[x_i]$, siehe [BW98, Ch. 8.8].

2.4.6 μ-Auflösung und univariate Darstellungen 0-dimensionaler Ideale

Beginn entsprechender Untersuchungen ab ca. 1995. Siehe zum Beispiel Fabricia Rouillier, "Applied Algebra in Engineering, Communications and Computing" [Rou99], oder auch [CCS99, Ch. 2], [BPR03, Ch. 11] und die Diplomarbeit von J. Peeken, 2002.

Seien die Bezeichnungen wie bisher, und sei $K \subseteq \mathbb{C}$. Wir benutzten ohne Beweis oder Begründung für die Vielfachheiten insbesondere

$$\sum_{v \in \mathcal{V}(I)} \mu(v) = \dim_K A \qquad (\dim I = 0).$$

Wir betrachten Morphismen von Nullstellenmengen (Varietäten). Dazu betrachten wir K-Algebra-Morphismen

$$\phi : K[x_1, \ldots, x_n] \to K[y_1, \ldots, y_m]$$

(bestimmt durch $\phi(x_1), \ldots, \phi(x_n)$) und dazu

$$\phi^* : \mathbb{C}^m \to \mathbb{C}^n, \quad w \mapsto (\phi(x_1)(w), \ldots, \phi(x_n)(w)).$$

Genauere Informationen zu der entsprechenden Dualität finden sich zum Beispiel in [CLO96].

Definition 2.4.6.1. *Seien $V \subseteq \mathbb{C}^n$, $W \subseteq \mathbb{C}^m$.*

(a) *Es heißt $\varphi : W \to V$ ein* (polynomialer) K-Morphismus, *wenn mit einem K-Algebra-Morphismus $\phi : K[x_1, \ldots, x_n] \to K[y_1, \ldots, y_m]$ gilt*

$$\phi^*|_W = \varphi.$$

Unser Szenario:

$$\begin{array}{ccc} K[x_1, \ldots, x_n] & \xrightarrow{\quad\phi\quad} & K[y_1, \ldots, y_m] \\ I & & J \\ V = \mathcal{V}(I) & \xleftarrow[\phi^*|_W]{} & W = \mathcal{V}(J) \end{array}$$

(b) *Es heißt $\varphi : W \to V$ ein K-*Isomorphismus, *wenn*

(i) *φ bijektiv ist und*

(ii) *φ, φ^{-1} K-Morphismen sind.*

*In diesem Fall heissen W und V K-*isomorph.

Beispiele 2.4.6.2.

(a) Sei $I = \langle x_1^2, x_1x_2, x_2^2\rangle$ und $J = \langle y_1^3\rangle$. Sei weiter $V := \mathcal{V}(I) = \{(0,0,0)\}$ (wobei $\mu((0,0,0)) = 3$) und $W := \mathcal{V}(J) = \{0\}$ (wobei $\mu(0) = 3$).

Betrachte die folgenden Abbildungen:

$$\begin{aligned}
\phi &: K[x_1, x_2] \to K[y_1], & x_1 &\mapsto y_1, x_2 \mapsto 0,\\
\phi^* &: \mathbb{C} \to \mathbb{C}^2, & c &\mapsto (\phi(x_1)(c), \phi(x_2)(c)) = (c, 0),\\
\psi &: K[y_1] \to K[x_1, x_2], & x_1 &\mapsto y_1, x_2 \mapsto 0,\\
\psi^* &: \mathbb{C}^2 \to \mathbb{C}, & (c_1, c_2) &\mapsto \psi(y_1)(c_1, c_2) = c_1.
\end{aligned}$$

Bestätige: V und W sind K-isomorph. Ausserdem bleiben die Vielfachheiten erhalten.

(b) Für weniger triviale Beispiele siehe [CCS99], Example 3.11, Seite 35.

(c) Situation des Shape-Lemmas: reguläre Position bezüglich x_n, $\sqrt{I} = I$, $\leq_{lex}$, und sei $[x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n)]$ eine Gröbner-Basis.

Betrachte $\phi : K[x_1, \ldots, x_n] \to K[y]$ und $\psi : K[y] \to K[x_1, \ldots, x_n]$ mit $\phi(x_i) = h_i(y)$, $1 \leq i < n$ und $\phi(x_n) = y$, $\psi(y) = x_n$.

Dann induzieren $\phi^*(\lambda) = (h_1(\lambda), \ldots, h_{n-1}(\lambda), \lambda)$ und $\psi^*((v_1, \ldots, v_n)) = v_n$ einen K-Isomorphismus zwischen $\mathcal{V}(I)$ und $\mathcal{V}(h_n(y))$. Die Vielfachheiten sind alle 1.

Definition 2.4.6.3. *Seien $I \subseteq K[x_1, \ldots, x_n]$, $J \subseteq K[y_1, \ldots, y_m]$ beides 0-dimensionale Ideale. Dann heissen I, J μ-*äquivalent*, wenn es einen K-Isomorphismus $\varphi : \mathcal{V}(I) \to \mathcal{V}(J)$ gibt mit*

$$\forall v \in \mathcal{V}(I) : \mu(\varphi(v)) = \mu(v).$$

Kurz: $I \cong_\mu J$.

Satz 2.4.6.4. *Seien I, J wie in der Definition. Dann sind I und J genau dann μ-äquivalent, wenn es einen K-Algebra-Homomorphismus $\phi : K[x_1, \ldots, x_n] \to K[y_1, \ldots, y_m]$ gibt mit*

(i) *$\phi^*|_{\mathcal{V}(J)}$ ist ein K-Isomorphismus auf $\mathcal{V}(I)$,*

(ii) *für alle $g \in K[x_1, \ldots, x_n]$ gilt*

$$\sum_{v \in \mathcal{V}(I)} \mu(v) g(v) = \sum_{w \in \mathcal{V}(J)} \mu(w) \phi(g(w)).$$

Beweis. Siehe etwa [??? Ro ???] (... ...). □

Bemerkung 2.4.6.5. Beachte: $I \cong_\mu J$ impliziert im allgemeinen nicht $K[x_1, \ldots, x_n]/I \cong K[y_1, \ldots, y_m]/J$ als K-Algebra. Jedoch sind sie als K-Vektorräume isomorph.

Etwa in Beispiel 2.4.6.2(a) sind die Algebren nicht isomorph.

Im Fall $I \cong_\mu J$ gilt jedoch $K[x_1, \ldots, x_n]/\sqrt{I} \cong K[y_1, \ldots, y_m]/\sqrt{J}$ als K-Algebra.

Definition 2.4.6.6. *Sei* $\dim I = 0$. *Dann heißt I μ-*aufgelöst mit einem Ideal J *mit $J \subseteq K[t]$, wenn $I \cong_\mu J$.*

*Ist I μ-aufgelöst und ϕ ein K-Algebra-Homomorphismus, der eine Isomorphie nach Definition 2.4.6.1 herstellt so, dass gilt $I \cong_\mu J$ mit $J \subseteq K[t]$, dann heißt (J, ϕ) μ-*Auflösung von I.

Satz 2.4.6.7 (Rouillier). *Seien $h, \ell \in K[x_1, \ldots, x_n]$ und h injektiv auf $\mathcal{V}(I)$, und seien*

$$f_h := \prod_{v \in \mathcal{V}(I)} (t - h(v))^{\mu(v)}, \qquad g_{\ell h} := \sum_{v \in \mathcal{V}(I)} \mu(v)\ell(v) \prod_{\substack{\lambda \in h(\mathcal{V}(I)) \\ \lambda \neq h(v)}} (t - \lambda).$$

Dann gilt

(a) *Es ist*

$$\varphi : \mathcal{V}(f_h) \to \mathcal{V}(I), \quad \lambda \mapsto \frac{1}{g_{1,h}(\lambda)}(g_{x_1,h}(\lambda), \ldots, g_{x_n,h}(\lambda))$$

wohldefiniert und ein K-Isomorphismus.

(b) *Außerdem gilt $f_h \in K[t]$, $g_{\ell,h} \in K[t]$ und*

$$f_h = \mathrm{CharPoly}(M_h), \qquad g_{\ell,h} = \frac{-\frac{\partial}{\partial s}\,\mathrm{CharPoly}(M_{h+s\ell})\big|_{s=0}}{\mathrm{ggT}(f_h, \frac{\partial}{\partial t} f_h')}.$$

Anhang A

Kommentiertes Literaturverzeichnis

A.1 Algebra II: Algebraische Gleichungen in einer Variablen

Die Literaturauswahl und Kommentare stammen von Prof. Dr. Wiland Schmale.

A.1.1 Kapitel 0

- [Rus00] `www.math-atlas.org`

  Unvollständig, es fehlen große Gebiete, wie z. B. die algebraische Geometrie.

- [ADNF$^+$03] H.-W. Alten, A. Djafari-Naini, M. Folkerts, H. Schlosser, K.-H. Schlote, H. Wußing, *4000 Jahre Algebra; Geschichte, Kulturen, Menschen.*

  Nicht die Algebra, sondern "nur" die Geschichte wird dargestellt; erfasst auch bereits neuere Gebiete, wie etwa Computer-Algebra.

- [Bew02] J. Bewersdorff, *Algebra für Einsteiger, Von der Gleichungsauflösung zur Galois-Theorie.*

  Schön beschriebene Einführung und Hinführung zur Algebra und insbesondere zur Galoistheorie. Geht mit vielen Beispielen und Kommentaren entlang des historischen Ablaufs vor und setzt anfangs nur Schulmathematik voraus. Trotzdem kommt er am Ende u. a. auch zum Hauptsatz der Galoistheorie. Dafür müssen dann natürlich algebraische Strukturen eingeführt werden.

- [Soc97] *Notices of the AMS*, März 1997,

  `http://www.ams.org/notices/199703/199703-toc-ps.html`

  Dort befindet sich ein Interview mit Bartel Leendert van der Waerden von Yvonne Dold-Samplonius:

  > *"The life and experiences of van der Waerden spanned twentieth-century mathematics in Europe, as revealed in this interview with him in 1993"*

  und der Artikel von Saunders Mac Lane: *Van der Waerden's Modern Algebra, The major changes in algebra wrought over 70 years ago were brought to the mathematical world by van der Waerden's seminal texts.* Beides aus *Notices of the AMS*, März 1997. Eine neuere Auflage des dabei angesprochenen Algebra-Werks wird weiter unten aufgeführt.

- [Tig02] Jean-Pierre Tignol, *Galois Theory of algebraic equations.* World Scientific, 2002.

  > *"[...] to convey to [...] undergraduate students in mathematics of how mathematics is made [...]"*

  Breit historisch-genetisch ausgerichtete Entwicklung der Galoistheorie und der zugehörigen Algebra, mathematisch viel breiter und vollständiger angelegt als das oben erwähnte Buch von Bewersdorff.

A.1.2 Kapitel 1 und 2

Viele einführende Texte zur Algebra enthalten auch einen unterschiedlich umfangreichen, oft auch nur kurzen Abschnitt zur Galoistheorie. Methodisch wird unterschiedlich vorgegangen, so dass sie zwar ergänzend zur Vorlesung z. T. interessant sind, aber deren Erarbeitung nicht ersetzen können. So z. B. die folgenden Bücher:

- [Kun94] Ernst Kunz, *Algebra.*
- [Bos04] Siegfried Bosch, *Algebra.*
- [Bac90] Friedrich Bachmann, *Algebra.*

Nach wie vor empfehlenswert ist der Klassiker *Algebra* von Bartel L. van der Waerden [Wae03], in Englisch neuaufgelegt. Es gab fast ununterbochen Neuauflagen auch in Deutsch, siehe Bibliotheksbestände. Die Galoistheorie in diesem Buch ist beeinflusst von deren Darstellung durch Emil Artin, die später und weiterentwickelt eigenständig in Buchform erschien [Art04].

Einflussreich und weit verbreitet waren und sind die Texte

- *Algebra* von Serge Lang [Lan84] (sehr systematisch, aber m. E. nicht zu schwer zum Lesen),
- *Basic Algebra I* von Nathan Jacobson [Jac85] (sehr gut lesbares Kapitel zur Galoistheorie und ihren Anwendungen, die nur relativ wenig Vorkenntnisse aus der Einführung in die Algebra erfordert; enthält als Kapitel 8 eine exzellente Einführung in die Verbandstheorie) und
- *Fields and Rings* von Irving Kaplanski [Kap72] (meine Vorlesung ist methodisch am stärksten von diesem Text beeinflusst).

Zur Verbandstheorie sei das Werk *Lattice Theory* von Garret Birkhoff [Bir73] erwähnt.

Laut Computer-Algebra-Rundbrief, Oktober 2003, befinden sich nun noch 20.000 Körper mehr in der Datenbank algebraischer Zahlenkörper und transitiver Galoisgruppen bis zur Ordnung 15 von J. Klüners, G. Malle [KM03].

Eine Orchidee aus dem Internet-Dschungel ist das Skript *Fields and Galois Theory* von J. S. Milne [Mil03].

A.1.3 Weitere in der Vorlesung erwähnte Literatur

Zur Umkehrung des Kriteriums "f auflösbar $\Rightarrow$ G_f auflösbar" im Fall $\operatorname{Char} K = 0$ empfehle ich Jacobson's *Basic Algebra*, [Jac85, Seiten 247/248], aber natürlich auch van der Waerden und viele andere. Jacobson verwendet die gleiche Definition von "auflösbar". Es werden dabei noch mehr Ergebnisse aus der Gruppentheorie herangezogen (Seiten 241/242). Das vollständige Kriterium in beiden Richtungen heisst *Galois-Kriterium.* Die Umkehrung auch im Fall von 0 verschiedenen Charakteristiken wird z. B. bei Lang [Lan84, S. 326–328] behandelt. Die Definition der Auflösbarkeit muss dann modifiziert werden, um die sogenannten Artin-Schreier-Polynome $x^p - x - c$ bei von 0 verschiedener Charakteristik p zuzulassen.

Viel Material ist wie immer zu finden bei *Lehrbuch der Algebra: Unter Einschluß der linearen Algebra, Band 2* von Scheja/Storch [SS88], insbesondere auf den Seiten 770 ff.

Mehr zu speziellen Gleichungen gibt es z. B. bei den oben aufgeführten Werken von Bewersdorff [Bew02], Tignol [Tig02] und Scheja/Storch [SS88].

Mehr und Interessantes zu nicht auflösbaren Gleichungen ist in dem eigenwilligen Büchlein *Field Theory and its Classical Problems* von Charles Hadlock [Had78] ausgearbeitet. Dort wird u. a. ausführlich der Hilbertsche Irreduziblitätssatz bewiesen und benutzt, um für alle $n \geq 5$ nicht auflösbare Polynome zu konstruieren.

Ein interessantes Lehrbuch ist m. E. auch *Classical Galois Theory with Examples* von Lisl Gaal [Gaa79]. Dort werden viele Beispiele einbezogen. Eine Besonderheit im Vergleich mit vielen anderen Abhandlungen der Galoistheorie ist, dass auch gezeigt wird, wie zumindest prinzipiell die wichtigsten Objekte der Galoistheorie berechnet werden können. Außerdem wird z. B. der Körper $\mathbb{W}$ aller Wurzeln aus ganzen Zahlen über $\mathbb{Q}$ untersucht und vergleichen mit dem Körper $\mathbb{E}$,

der alle Einheitswurzeln über $\mathbb{Q}$ enthält. Es gilt erstaunlicherweise $\mathbb{W} \subseteq \mathbb{E}$. Auch der Körper der mit Zirkel und Lineal konstruierbaren Zahlen wird dort verglichen mit $\mathbb{E}$ (Seite 241).

In dem Buch *Introduction to the Galois correspondence* von Marueen Fenrick [Fen92] wird am Ende die Galoistheorie benutzt, um wichtigste Resultate der Mathematik zu gewinnen: Ein Satz von Wedderburn, der besagt, dass jeder endliche Schiefkörper ein Körper ist (vergleiche die Übungsaufgaben zu Kapitel 10 in der Einführung in die Algebra), Existenz von Galois-Erweiterungen von $\mathbb{Q}$ zu gegebenen abelschen Galoisgruppen.

Zur Realisierung endlicher abelscher Gruppen als Galoisgruppen über $\mathbb{Q}$ kann auch auf das Buch von Kunz [Kun94, S 182] verwiesen werden.

Die Galoistheorie ist auch heute ein Gebiet aktiver mathematischer Forschung. Insbesondere sind beim sogenannten inversen Problem der Galoistheorie noch viele Fragen offen. Dabei geht es darum, zu gegebenem Körper K (insbesondere iom Fall $K = \mathbb{Q}$) und gegebener Gruppe G eine Galoiserweiterung zu finden mit G als Galoisgruppe. Z. B. Ihara et al, *Galoisgroups over* $\mathbb{Q}$, oder Arbeiten von Gunter Malle, um nur Beispiele zu nennen. Dies ist Spezialliteratur, die auch für Mathematiker anderer Spezialgebiete nicht mehr so leicht zugänglich ist. Lesenswert, auch wenn man nicht weiterlesen will, ist die Einleitung zu *Konstruktive Galoistheorie* von Heinrich Matzat [Mat87].

Im Zusammenhang mit modularen Methoden in der berechnenden Algebra sind außerdem Ergebnisse über den Zusammenhang der Galoisgruppe eines Polynoms aus z. B. $\mathbb{Z}[x]$ mit denen der entsprechenden reduzierten Polynome aus $\mathbb{Z}_p[x]$ von Interesse.

Vieles haben wir nicht behandelt: allgemeine Diskriminanten, Normalbasen, Hilbert's Satz 90 (siehe z. B. das oben erwähnte Skript von Milne [Mil03]), unendliche Galoiserweiterungen, etc.

Ein Standardwerk der "computational algebra" ist *A Course in Computational Number Theory* von H. Cohen [Coh03]. Dort werden auch einige Themen, die die Vorlesung betreffen, bearbeitet. Mit Überraschungen ist zu rechnen, denn gerechnet wird manchmal ganz anders, als es die Theorie zunächst vermuten lässt.

A.2 Algebra II: Algebraische Gleichungen in mehreren Variablen

- [AL94] W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases.*
- [BPR03] S. Basu, R. Pollack, M. Roy, *Algorithms in Real Algebraic Geometry.*
- [BW98] Th. Becker, V. Weispfennig, *Gröbner Bases, A Computational Application.*
- [Buc98] B. Buchberger, F. Winkler (Hrsg.), *Gröbner Bases and Applications.*
- [CCS99] A. Cohen, H. Cuypers, H. Sterk, *Some Tapas of Computer Algebra.*
- [CLO96] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.*
- [CLO98] D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry.*
- [Eis95b] D. Eisenbud, *Commutative Algebra with a View Towards Algebraic Geometry.*
- [GG03] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra.*
- [KR00] M. Kreuzer, L. Robbiano, *Computational Commutative Algebra.*
- [Mis93] B. Mishra, *Algorithmic Algebra.*
- [Stu96] B. Sturmfels, *Gröbner Bases and Convex Polytopes.*
- [Win96] F. Winkler, *Polynomial Algorithms in Computer Algebra.*

Literaturverzeichnis

[ADNF+03] Alten, H.-W. ; Djafari-Naini, A. ; Folkerts, M. ; Schlosser, H. ; Schlote, K.-H. ; Wussing, H.: *4000 Jahre Algebra; Geschichte, Kulturen, Menschen.* Springer, 2003

[AL94] Adams, W. ; Loustaunau, P.: *An Introduction to Gröbner Bases.* American Math Society, 1994

[Art04] Artin, E.: *Galoissche Theorie.* Harri Deutsch, 2004

[Bac90] Bachmann, F.: *Algebra.* Wissenschaftliche Buchgemeinschaft, 1990

[Bew02] Bewersdorff, J.: *Algebra für Einsteiger. Von der Gleichungsauflösung zur Galois-Theorie.* Vieweg, 2002

[BG00] Bainville, E. ; Genèves, B.: Constructions Using Conics. In: *Mathematical Intelligencer* 3 (2000), S. 59–72

[Bir73] Birkhoff, G.: *Lattice Theory.* American Math Society, 1973

[Bos04] Bosch, S.: *Algebra.* Fünfte. Springer, 2004

[Bou59] Bourbaki, N.: *Elements de Mathematiques, Algebra Ch. 4, 5, Notes historiques.* Herman, 1959

[BPR03] Basu, S. ; Pollack, R. ; Roy, M.: *Algorithms in Real Algebraic Geometry.* Springer, 2003

[Buc98] Buchberger, B. ; Winkler, F. (Hrsg.): *Gröbner Bases and Applications.* Cambridge University Press, 1998

[BW98] Becker, Th. ; Weispfennig, V.: *Gröbner Bases. A Computational Application.* Zweite. Springer, 1998

[CCS99] Cohen, A. ; Cuypers, H. ; Sterk, H.: *Some Tapas of Computer Algebra.* Springer, 1999

[CLO96] Cox, D. ; Little, J. ; O'Shea, D.: *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, 1996

[CLO98] Cox, D. ; Little, J. ; O'Shea, D.: *Using Algebraic Geometry.* Springer, 1998

[Coh03] Cohen, H.: *A Course in Computational Number Theory.* Springer, 2003

[Ebb92] Ebbinghaus, H. D. (Hrsg.): *Zahlen.* Springer, 1992

[Eis95a] Eisenbud, David: *Commutative Algebra: with a View Toward Algebraic Geometry.* New York : Springer-Verlag, 1995 (Graduate Texts in Mathematics 150)

[Eis95b] Eisenbud, David: *Commutative Algebra with a View Towards Algebraic Geometry.* Springer, 1995

[Fen92] Fenrick, M. H.: *Introduction to the Galois correspondence.* Birkhäuser, 1992

[FS83] Fischer, G. ; Sacher, R.: *Einführung in die Algebra*. Teubner, 1983

[Gaa79] Gaal, L.: *Classical Galois Theory with Examples*. Chelsea, 1979

[GG03] von zur Gathen, J. ; Gerhard, J.: *Modern Computer Algebra*. Cambridge University Press, 2003

[Had78] Hadlock, C.: *Field Theory and its Classical Problems*. Mathematical Association of America, 1978

[HG86] h. H. Garling, D.: *A course in Galois Theory*. Cambridge University Press, 1986

[Jac85] Jacobson, N.: *Basic Algebra I*. Second. W. H. Freeman, 1985

[Kap72] Kaplanski, I.: *Fields and Rings*. University of Chicago Press, 1972

[Kap76] Kaplanski, I.: *An Introduction to Differential Algebra*. Paris : Herrmann, 1976

[KM03] Klüners, J. ; Malle, G. *A Database for Number Fields*. `http://www.mathematik.uni-kassel.de/~klueners/minimum/`. 2003

[KR00] Kreuzer, M. ; Robbiano, L.: *Computational Commutative Algebra*. Springer, 2000

[Kun94] Kunz, E.: *Algebra*. Zweite überarbeitete. Vieweg, 1994

[Lan84] Lang, S.: *Algebra*. Zweite. Addison Wesley, 1984

[Mag94] Magid, A. R.: *Lectures on Differential Galois Theory*. American Math Society, 1994

[Mat87] Matzat, H.: *Konstruktive Galoistheorie*. Springer, 1987 (Springer Lecture Notes Nr. 1284)

[Mil03] Milne, J. S. *Fields and Galois Theory*. `http://www.jmilne.org/`. 2003

[Mis93] Mishra, B.: *Algorithmic Algebra*. Springer, 1993

[Rot90] Rotmann, J.: *Galois Theory*. Springer, 1990

[Rou99] Rouillier, F.: In: *Applied Algebra in Engineering, Communications and Computing* 9(5) (1999), S. 433–461

[Rus00] Rusin, D. *Mathematical Atlas*. `http://www.math-atlas.org/`. 2000

[Soc97] Society, American M. *Notices of the AMS*. `http://www.ams.org/notices/199703/199703-toc-ps.html`. März 1997

[SS88] Scheja, G. ; Storch, U.: *Lehrbuch der Algebra: Unter Einschluß der linearen Algebra*. Bd. 2. Teubner, 1988

[Ste73] Stewart, I.: *Galois Theory*. Chapman Hall (open university text), 1973

[Stu96] Sturmfels, B.: *Gröbner Bases and Convex Polytopes*. American Math Society, 1996

[Tig02] Tignol, J.-P.: *Galois Theory of Algebraic Equations*. World Scientific, 2002

[Wae85] van der Waerden, B. L.: *A history of Algebra*. Springer, 1985

[Wae03] van der Waerden, B. L.: *Algebra*. Springer, 2003

[Win96] Winkler, F.: *Polynomial Algorithms in Computer Algebra*. Springer, 1996

Index