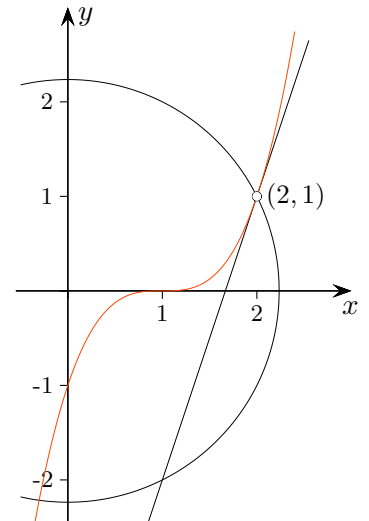


1. Gröbner Basis
2. Reduktion, verallgemeinerte Polynomdivision
3. Algorithmus für die reduzierte Gröbner Basis
4. Beispiel
5. Beispiel
6. Gröbner Basis Definition
7. Gröbner Basis
8. Reduzierte Gröbner Basis
9. Eindeutig bestimmte reduzierte Gröbner Basis, Normalform
10. Monomordnung
11. Schnitt von Ellipsen
12. Schnittmenge (Varietät) leer
13. Starke Form des Hilbertschen Nullstellensatzes
14. Elimination mit Gröbner Basen, Satz (nulldim. Ideal)
15. Implizite Darstellung
16. Formel von Heron
17. Resultante, Gröbner Basis
18. Einfärben von Landkarten
19. Polynom-Transformation
20. Schwache Form des Hilbertschen Nullstellensatzes
21. Nullstellensatz Erläuterungen
22. Lemma von Dickson
23. Hilbertscher Basissatz
24. Vektorraum der Normalformen
25. Multiplikation mod  $G$
26. Endlichkeitssatz
27.  $|V(I)| =$  Dimension des Vektorraums der Normalformen
28. Syzygie 5 Seiten
29. Polynomdivision (Reduktion) mit dem Gauss-Algorithmus
30. Gröbner Basis, einleitende Bemerkungen
31. Gröbner Basis, Integer Programming

32. Optimierungsproblem in  $\mathbb{N}$
33. Kompatible Monomordnung
34. Optimierungsproblem in  $\mathbb{Z}$

## ↑ Gröbner Basis

$$\begin{aligned} y - 3x + 5 &= 0 \\ x^2 + y^2 - 5 &= 0 \\ y - x^3 + 3x^2 - 3x + 1 &= 0 \end{aligned}$$



Mit [WolframAlpha](#)

```
GroebnerBasis[{y - 3x + 5, x^2 + y^2 - 5, y - x^3 + 3x^2 - 3x + 1}, {x, y}]
```

mit Maple

```
with(Groebner):
```

```
Basis([y - 3 * x + 5, x^2 + y^2 - 5, -x^3 + 3 * x^2 - 3 * x + y + 1], plex(x, y));
```

```
[y - 1, x - 2]
```

plex (oder lex) lexikographische Ordnung  $x > y$

Buchberger entwickelte 1965 ein über die [Resultanten-Methode](#) hinausreichendes Verfahren zur Lösung umfangreicher nichtlinearer Gleichungssysteme mit vielen Variablen. Sein Lehrer Gröbner hatte im Seminar ein damit zusammenhängendes Problem geschildert. Er erwähnte nicht, dass er sich schon über zwei Jahrzehnte vergeblich um eine Lösung bemüht hatte. Buchberger griff die Fragestellung begierig auf und seine intensiven Bemühungen - er war auch als Programmierer angestellt - waren nach eineinhalb Jahren erfolgreich. Der im Allgemeinen erhebliche Rechenaufwand seines Verfahrens konnte mit der zu dieser Zeit eingeführten Computertechnologie bewältigt werden. Ein Jahr zuvor entdeckte Hironaka algebraisch eng Verwandtes in der Geometrie, ohne jedoch einen Weg zur Berechnung aufzuzeigen.

Der Buchberger-Algorithmus führt für ein lineares Gleichungssystem zum selben Ergebnis wie der Gauss-Algorithmus, bei dem Gleichungen sukzessive durch Linearkombinationen mit anderen Gleichungen ersetzt werden, so dass sich an der Lösungsmenge nichts ändert.

$$\begin{array}{r} 2x + y - 4 = 0 \\ 4x - 3y + 2 = 0 \\ \hline 2x + y - 4 = 0 \\ -5y + 10 = 0 \\ \hline y = 2 \\ x = 1 \end{array}$$

$4x - 3y + 2$  wird hier durch  $(4x - 3y + 2) - 2(2x + y - 4) = -5y + 10$  ersetzt.

Dies kann weiterführend als Polynomdivision gelesen werden:

$$(4x - 3y + 2) : (2x + y - 4) = 2 \text{ Rest } -5y + 10 \quad \text{oder}$$

$$(4x - 3y + 2) = 2(2x + y - 4) + (-5y + 10)$$

Aus dieser Linearkombination ist ersichtlich, dass die Systeme  $\{2x + 4y - 4 = 0, 4x - 3y + 2 = 0\}$  und  $\{2x + 4y - 4 = 0, -5y + 10 = 0\}$  dieselbe Lösung haben.

Diese Strategie kann auf Systeme von Polynomgleichungen in mehreren Veränderlichen angewandt werden, um eine möglichst einfache polynomiale Beschreibung, die Gröbner Basis, der Schnittmenge (Varietät) zu erhalten. Wenden wir uns daher der Division mit mehreren Polynomen und dem Eingangsbeispiel zu.

## ↑ Reduktion, verallgemeinerte Polynomdivision

$f := -x^3 + 3x^2 - 3x + y + 1$  Die Summanden wurden nach Potenzen von  $x$  geordnet.

$g := x^2 + y^2 - 5$

$h := -3x + y + 5$

Mit [WolframAlpha](#)

PolynomialReduce $[-x^3 + 3x^2 - 3x + y + 1, \{x^2 + y^2 - 5, -3x + y + 5\}, \{x, y\}]$

$$\begin{array}{lcl}
 r_1 = f + xg & = & 3x^2 + xy^2 - 8x + y + 1 \\
 r_2 = r_1 - 3g & = & xy^2 - 8x - 3y^2 + y + 16 \\
 r_3 = r_2 + \frac{1}{3}y^2h & = & -8x - \frac{4}{3}y^2 + y + 16 + \frac{1}{3}y^3 \\
 r_4 = r_3 - \frac{8}{3}h & = & \frac{1}{3}(y^3 - 4y^2 - 5y + 8)
 \end{array}
 \quad \left| \quad \begin{array}{l}
 f = -xg + r_1 \\
 r_1 = r_2 + 3g \\
 r_2 = r_3 - \frac{1}{3}y^2h \\
 r_3 = r_4 + \frac{8}{3}h
 \end{array}
 \right.$$

Aus der Linearkombination  $f = (3 - x)g + \frac{1}{3}(8 - y^2)h + r_4$  ist erkennbar, dass die Polynommenge  $\{f, g, h\}$  dieselben gemeinsamen Nullstellen wie  $\{f, g, h, r_4\}$  hat. Beachte:  $r_4$  enthält nur Potenzen von  $y$ . Für  $r_4 = \frac{1}{3}(y - 1)(y^2 - 3y - 8) = 0$  ist auch  $y = 1$  eine Lösung. Durch Einsetzen erhalten wir (2, 1). Für Weiteres beachtenswert:  $f$  kann in  $\{f, g, h, r_4\}$  wegen der obigen Linearkombination entfallen, die gemeinsamen Nullstellen von  $\{g, h, r_4\}$  sind auch Nullstellen von  $f$ .

Bei der Polynomdivision in einer Variablen hat der Rest kleineren Grad als der Divisor. Hier können wir bei der Reduktion von  $f$  mit  $\{g, h\}$  nur feststellen, dass der Rest keine Monome enthält, die durch den führenden (in der Monomordnung größten) Term von  $g$  oder  $h$  teilbar sind.

Der Divisions-Algorithmus endet nach endlich vielen Schritten:

Bei jedem Divisionsschritt wird der führende Term  $r_i$  mit dem ihn teilenden führenden Term des Divisors  $g$  bzw.  $h$  eliminiert. Alle Monome, die eventuell neu dazukommen, sind daher kleiner oder gleich dem führenden Monom des Divisors. Die führenden Monome der  $r_i$  bilden daher eine absteigende, schließlich abbrechende Kette.

Die von  $\{f, g, h\}$  und  $\{f, g, h, r_4\}$  bzw.  $\{g, h, r_4\}$  im Polynomring  $\mathbb{Q}[x, y]$  mit den Variablen  $x$  und  $y$  erzeugten Ideale sind identisch, Schreibweise  $\langle f, g, h \rangle = \langle g, h, r_4 \rangle$ , da ein von  $\{f_1, f_2, f_3\}$  erzeugtes Ideal aus allen Linearkombinationen von  $f_1, f_2, f_3$  mit Koeffizienten aus  $\mathbb{Q}[x, y]$  besteht. Es gilt:  $\{f_1, f_2, f_3\}$  und  $\{g_1, g_2, g_3, g_4\}$  erzeugen dasselbe Ideal (mit gleicher Schnittmenge), wenn sich jedes Polynom der einen Menge als Linearkombination der anderen darstellen lässt. Gesucht sind Erzeugende minimalen Grades. Diese algebraische Formulierung kommt ohne die Schnittmenge aus, sie kann auch leer sein.

Buchberger verwendet in seinem Algorithmus Linearkombinationen von jeweils zwei Polynomen, wie z. B.  $r_1$ , so dass sich der größte Summand heraushebt ( $S$ -Polynom, Syzygie gr.-lat. Zusammenfügung, Gespann, in der Astronomie: Sonne, Erde und Mond in einer geraden Linie aufgereiht). Beim  $S$ -Polynom  $S(f, g)$  werden  $f$  und  $g$  so multipliziert, dass die jeweils führenden Terme wie im linearen Fall auf das kleinste gemeinsame Vielfache gebracht werden, damit sie bei der Subtraktion herausfallen,

$$f = x^3 - 2xy, \quad g = x^2y - 2y^2 + x, \quad S(f, g) = yf - xg = -x^2.$$

Maple with(Groebner): SPolynomial( $x^3 - 2 * x * y, x^2 * y - 2 * y^2 + x, \text{plex}(x, y)$ );

Die Polynomdivision hängt von der Monomordnung (und der Reihenfolge der Divisoren ab), alternative Berechnung:

$$\begin{aligned} r_1 &:= y^2x + y + 3x^2 - 8x + 1 && \text{Siehe oben, die Summanden wurden nach Potenzen von } y \text{ geordnet.} \\ g &:= y^2 + x^2 - 5 \\ h &:= y - 3x + 5 \end{aligned}$$

$$\begin{aligned} r_2 &= r_1 - xg = y - x^3 + 3x^2 - 3x + 1 \\ r_3 &= r_2 - h = -x^3 + 3x^2 - 4 \\ &= (1-x)(x-2)^2 \end{aligned} \quad \left| \begin{array}{l} r_1 = xg + r_2 \\ r_2 = h + r_3 \\ r_1 = xg + h + r_3 \end{array} \right. \quad \text{Das führt zu (2,1).}$$

### ↑ Algorithmus für die reduzierte Gröbner Basis

In einem Eliminationsschritt des Gauss-Algorithmus wird ein Polynom durch ein  $S$ -Polynom ersetzt. Hier kann sich jedoch die Lösungsmenge ändern:

$$f = x^2y + xy^2 + 1, \quad g = x^3 - xy, \quad S(f, g) = xf - yg = x^2y^2 + xy^2 + x.$$

$(0, 0)$  ist Nullstelle von  $S(f, g)$ , aber nicht von  $f$ , das somit nicht durch  $S(f, g)$  ersetzt werden kann.

Der Algorithmus von Buchberger ist im Gegensatz zu den erforderlichen Begründungen einfach zu formulieren. Sei eine Monomordnung festgelegt, z.B. eine lexikographische.

1.  $G = \{f_1, f_2, \dots, f_n\}$
2.  $G' = G$   
Ermittle für jedes Paar  $f_i, f_j \in G'$  ( $i < j$ ) den Rest  $r$  bei der Division von  $S(f_i, f_j)$  durch die Elemente von  $G'$  (Reduktion mit  $G'$ ). Falls  $r \neq 0$ , füge  $r$   $G$  hinzu ( $G = G \cup \{r\}$ ).
3. Falls  $G \neq G'$ , so gehe zu 2. Diese Polynome ergeben die Gröbner Basis.
4. Streiche alle Elemente aus  $G$ , dessen führendes Monom durch ein führendes Monom eines der restlichen Elemente aus  $G$  teilbar ist.  $g \in G$  normieren, minimale Gröbner Basis (siehe Satz S. 6)
5. Eliminiere durch Multiplikation und Subtraktion aus den Elementen von  $G$  Terme, die durch das führende Monom eines anderen Elements aus  $G$  teilbar sind. reduzierte Gröbner Basis

Der Algorithmus kann optimiert werden.

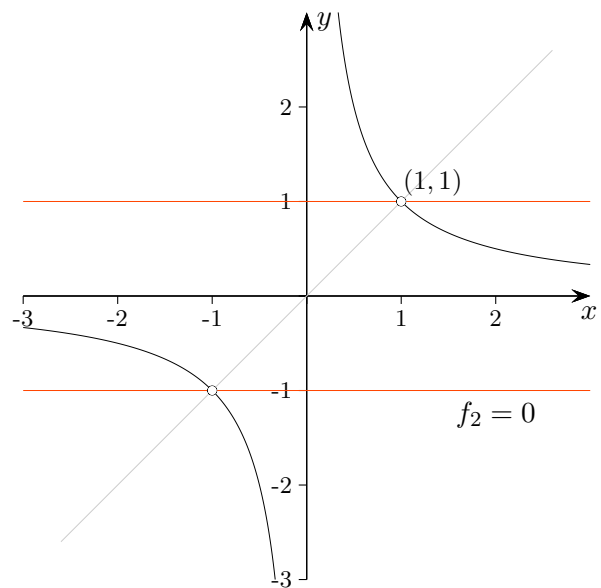
$S$ -Polynome, die im 2. Schritt den Divisionsrest null ergeben, müssen nicht weiter berücksichtigt werden. Der Divisionsrest bleibt bei jedem weiteren Durchgang null, da durch dieselben Polynome (plus einiger neuer) dividiert wird.

Wenn im 2. Schritt ein Divisionsrest  $r \neq 0$  auftaucht, ist dessen führendes Monom durch kein führendes Monom eines Polynoms  $g \in G$  teilbar. Wir erhalten daher eine Folge  $m_1, m_2, \dots$  von Monomen mit der Eigenschaft, dass für alle  $i < j$  gilt:  $m_i$  teilt nicht  $m_j$ . Die Folge muss endlich sein. Es gibt z.B. für  $m_i = x^2y^3$  oder  $m_i = y^3$  für  $m_j$  nur die Möglichkeiten  $y, y^2, x, xy, xy^2, xy^3, xy^4$ , usw., so dass  $m_i$  nicht  $m_j$  teilt. Wenn z.B.  $m_j = xy^3$  in der Folge erscheint, ist das für  $xy^k, k \geq 3$ , nicht mehr möglich. Also kann der zweite Schritt nur endlich oft durchlaufen werden.

## ↑ Beispiel

Aus der folgenden vereinfachten Formulierung ist unmittelbar zu ersehen, dass die Schnittmenge stets gleich (invariant) bleibt. Sei eine Monomordnung festgelegt.

1.  $G = \{f_1, f_2, \dots, f_n\}$
2.  $G' = G$   
Ermittle für jedes Paar  $f_i, f_j \in G'$  ( $i < j$ ) den Rest  $r$  bei Reduktion von  $S(f_i, f_j)$  mit  $G'$ .  
Falls  $r \neq 0$ , dann  $G = G \cup \{r\}$ .
3. Reduziere jedes  $f \in G$  (Ergebnis  $r$ ) mit  $G \setminus \{f\}$ .  
Falls  $r = 0$ , dann  $G = G \setminus \{f\}$ , sonst ersetze in  $G$   $f$  durch  $r$ .
4. Falls  $G \neq G'$ , gehe zu 2.



$$f_1 = xy - 1$$

$$f_2 = y^2 - 1$$

$$G = \{f_1, f_2\}$$

2.	$G' = \{g_1, g_2\}$	$S(g_1, g_2) = 0 \cdot g_1 + 0 \cdot g_2 + x - y$ (Reduktion mit $G'$ )	$G = \{g_1, g_2, g_3 = x - y\}$
3.		$g_1 = g_2 + yg_3 + 0, g_2 = 0 \cdot g_1 + 0 \cdot g_3 + g_2, g_3 = \dots g_3$	$G = \{g_2, g_3\}$
2.	$G' = \{g_2, g_3\}$	$S(g_2, g_3) = yg_2 - g_3 + 0$ (Reduktion mit $G'$ )	$G = \{g_2, g_3\}$

$$G = \{g_1 = x - y, g_2 = y^2 - 1\}$$

Schnittpunkte  $(1, 1), (-1, -1)$

Probe, die Gröbner Basis erzeugt das Ideal  $\langle f_1, f_2 \rangle$ .

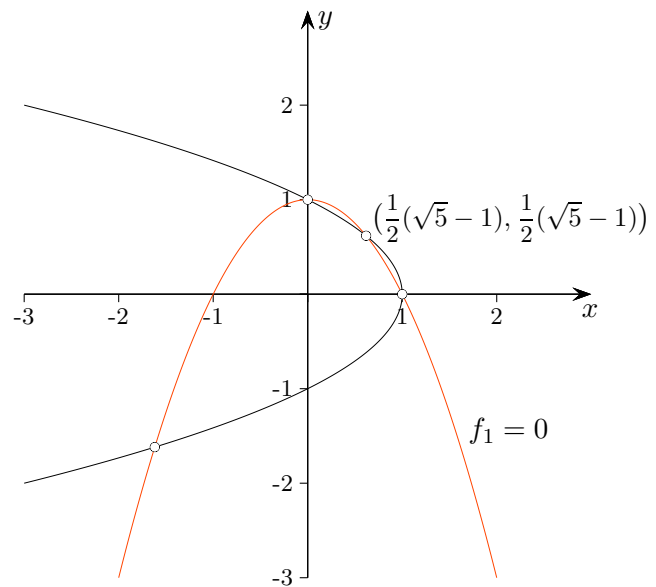
$$f_1 = yg_1 + g_2$$

$$f_2 = g_2$$

↑

## ↑ Beispiel

1.  $G = \{f_1, f_2, \dots, f_n\}$
2.  $G' = G$   
Ermittle für jedes Paar  $f_i, f_j \in G'$  ( $i < j$ ) den Rest  $r$  bei Reduktion von  $S(f_i, f_j)$  mit  $G'$ .  
Falls  $r \neq 0$ , dann  $G = G \cup \{r\}$ .
3. Reduziere jedes  $f \in G$  (Ergebnis  $r$ ) mit  $G \setminus \{f\}$ .  
Falls  $r = 0$ , dann  $G = G \setminus \{f\}$ , sonst ersetze in  $G$   $f$  durch  $r$ .
4. Falls  $G \neq G'$ , gehe zu 2.



$$f_1 = x^2 + y - 1$$

$$f_2 = x + y^2 - 1$$

$$G = \{f_1, f_2\}$$

2.	$G' = \{f_1, f_2\}$	$S(f_1, f_2) = 0 \cdot f_1 + (1 - y^2) \cdot f_2 + y^4 - 2y^2 + y$ (Reduktion mit $G'$ )	$G = \{f_1, f_2, f_3 = y^4 - 2y^2 + y\}$
3.		$f_1 = (x - y^2 + 1)f_2 + f_3 + 0$ $f_2 = 0 \cdot f_1 + 0 \cdot f_3 + f_2$ $f_3 = 0 \cdot f_1 + 0 \cdot f_2 + f_3$	$G = \{f_2, f_3\}$
2.	$G' = \{f_2, f_3\}$	$S(f_2, f_3) = y^6 - y^4 + 2xy^2 - xy$ $S(f_2, f_3) = (2y^2 - y)f_2 + (y^2 - 1)f_3 + 0$ (Reduktion mit $G'$ )	

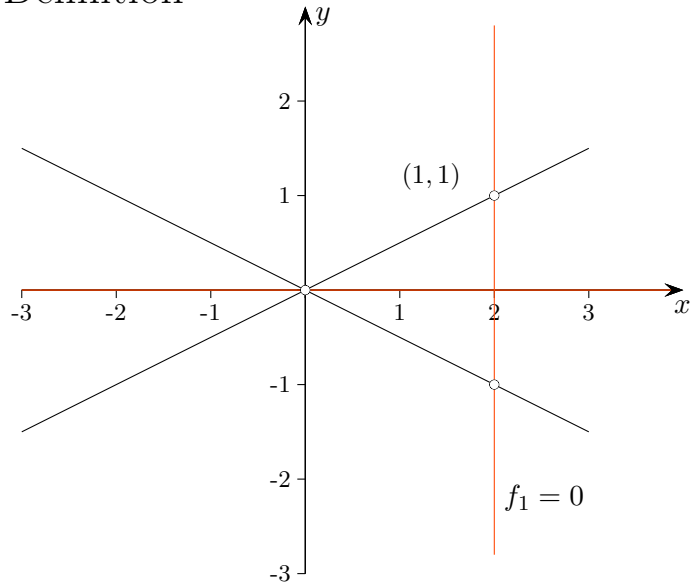
$$G = \{x + y^2 - 1, y^4 - 2y^2 + y\}$$

$$y^4 - 2y^2 + y = y(y - 1)(y^2 + y - 1)$$

Schnittpunkte  $(1, 0), (0, 1), \left(\frac{1}{2}(\sqrt{5} - 1), \frac{1}{2}(\sqrt{5} - 1)\right), \left(-\frac{1}{2}(\sqrt{5} + 1), -\frac{1}{2}(\sqrt{5} + 1)\right)$

↑

## ↑ Gröbner Basis Definition



$$f_1 = xy - 2y$$

$$f_2 = x^2 - 4y^2$$

$$F = \{f_1, f_2\}$$

Gröbner Basis  $G = \{g_1 = xy - 2y, g_2 = x^2 - 4y^2, g_3 = y^3 - y\}$

$$G = \{g_1, g_2, g_3\} \left| \begin{array}{l} S(g_1, g_2) = -2xy + 4y^3 \\ S(g_1, g_3) = xy - 2y^3 \\ S(g_2, g_3) = x^2y - 4y^5 \end{array} \right. \begin{array}{l} S(g_1, g_2) = -2 \cdot g_1 + 0 \cdot g_2 + 4 \cdot g_3 + 0 \text{ (Reduktion mit } G) \\ S(g_1, g_3) = 1 \cdot g_1 + 0 \cdot g_2 - 2 \cdot g_3 + 0 \\ S(g_2, g_3) = (x+2) \cdot g_1 + 0 \cdot g_2 + (-4y^2 - 4) \cdot g_3 + 0 \end{array}$$

Sei  $I$  das von  $F = \{f_1, f_2, \dots, f_m\}$  erzeugte Ideal, das aus allen Linearkombinationen mit Elementen aus  $F$  besteht. Die Koeffizienten sind Polynome mit (hier) den Variablen  $x$  und  $y$ .

Definition

$G = \{g_1, g_2, \dots, g_n\}$  mit Elementen aus  $I$  heißt Gröbner Basis von  $I$ , wenn jedes  $S$ -Polynom  $S(g_i, g_j)$  bei der Reduktion mit  $G$  den Rest  $0$  hat.

Satz

Das ist genau dann der Fall, falls die Monome  $\text{FM}(g_i)$ ,  $g_i \in G$ , das Ideal  $\text{FM}(I)$  erzeugen,  $\text{FM}$  führendes Monom, d.h. für alle  $f \in I$ ,  $f \neq 0$ , gibt es ein  $g_i$  mit  $\text{FM}(g_i)$  teilt  $\text{FM}(f)$ .

Folgerung: Genau die Elemente aus  $I$  ungleich  $0$  haben bei der Reduktion mit  $G$  den Rest  $0$ .

Für  $f = a_1g_1 + \dots + a_n g_n + r$  gilt  $f \in I \iff r \in I$ .  $r = 0 \implies f \in I$ .

Sei umgekehrt  $f \in I$  und  $r \neq 0$ . Dann ist  $r \in I$  und es gibt ein  $g_i$  (Satz) mit  $\text{FM}(g_i)$  teilt  $\text{FM}(r)$ .

Das ist ein Widerspruch zur Reduktion von  $f$  mit  $G$ .

Eine Situation wie

$$G = \{g = x^3 - 2xy, h = x^2y + x - 2y^2\}$$

$$-y \cdot g + x \cdot h = x^2 \in I$$

kann bei Gröbner Basen  $G$  nicht eintreten,  $x^3$ ,  $x^2y$  können nicht  $x^2$  erzeugen (teilen).



## ↑ Gröbner Basis

Der Satz erscheint naheliegend.

Der Divisionsalgorithmus besagt, dass für

$$S(g_i, g_j) = a_1g_1 + \dots + a_n g_n + r, \quad a_i, r \text{ Polynome}$$

entweder  $r = 0$  oder  $r$  eine Linearkombination von Monomen ist, so dass keines von ihnen durch einen der führenden Terme der  $g_i$  teilbar ist. Wegen  $r = S(g_i, g_j) - a_1g_1 - \dots - a_n g_n \in I$  ist  $r = 0$ , wenn die führenden Monome der Elemente aus  $I$  jeweils durch ein führendes Monom eines  $g_i$  geteilt werden, wenn also die Monome  $\text{FM}(g_i)$  das Ideal  $\text{FM}(I)$  erzeugen (es hinreichend viele kleine  $g_i$ 's gibt).

Der Beweis der Umkehrung,

hat jedes  $S$ -Polynom  $S(g_i, g_j)$  bei der Reduktion mit  $G$  den Rest  $0$  hat, so erzeugen die Monome  $\text{FM}(g_i)$  das Ideal  $\text{FM}(I)$ , ist nicht so offensichtlich und soll skizziert werden.

### 1. Fall

Sei  $g \in I$ , d. h. es gibt eine Darstellung

$$g = a_1g_1 + \dots + a_n g_n, \quad a_i \text{ Polynome.}$$

Falls sich hier keine führenden Terme der Summanden  $a_i g_i$  wegheben, ist der führende Term von  $g$  auch auf der rechten Seite zu finden, eventuell als Summe führender Terme.  $\text{FM}(g)$  liegt daher im von den  $\text{FM}(g_i)$  erzeugten Ideal.

### 2. Fall

Für  $g = a_1g_1 + \dots + a_n g_n$  ist es jedoch möglich, wie im Beispiel auf der vorigen Seite, dass die Summe  $S$  einiger führender Terme von  $a_j g_j$  mit gleichem Monom null ist und damit - wie bei  $S(g_i, g_j)$  - herausfällt. O.B.d.A sei  $a_1 + a_2 + a_3 + a_4 = 0$  für eine herausfallende Summe mit gleichen führenden Monomen. Es verwundert daher nicht, dass  $S$  als Linearkombination der  $S(g_i, g_j)$  dargestellt werden kann. Die  $S$ -Polynome wiederum sind Linearkombinationen der  $g_i$  (Rest null nach Voraussetzung).

Betrachte hierzu die Umformungen:

$$\begin{aligned} S &= a_1g_1 + a_2g_2 + a_3g_3 + a_4g_4 && g_i \text{ normiert, d. h. leitender Koeffizient} = 1 \\ &= a_1(g_1 - g_2) + (a_1 + a_2)(g_2 - g_3) + (a_1 + a_2 + a_3)(g_3 - g_4) + \underbrace{(a_1 + a_2 + a_3 + a_4)}_0 g_4 \\ &= a_1S(g_1, g_2) + (a_1 + a_2)S(g_2, g_3) + (a_1 + a_2 + a_3)S(g_3, g_4), && S(g_i, g_j) = g_i - g_j \\ g &= b_1g_{n_1} + \dots + b_k g_{n_k} \end{aligned}$$

Mit dieser Darstellung können wir wie im 1. und 2. Fall argumentieren: Falls sich bei den führenden Termen nichts weghebt, haben wir  $\text{FM}(g)$  als Element des von den  $\text{FM}(g_i)$  erzeugten Ideals dargestellt, andernfalls erhalten wir wieder mit Hilfe der  $S$ -Polynome und deren Reduktion eine neue Darstellung von  $g$  als Linearkombination der  $g_i$  mit kleinerem maximalen Grad der Summanden, und so weiter. Das Verfahren muss schließlich mit einer Summe enden, in der die führenden Terme erhalten bleiben, da eine absteigende Monomordnungs-Folge endlich ist.

Der Satz zeigt die besondere Bedeutung der Elemente aus  $I$  mit kleinen (minimalen) führenden Monomen. In der Literatur wird, von wenigen Ausnahmen abgesehen, die Aussage des Satzes in wenig genetischer Weise als Definition für eine Gröbner Basis genommen. Dieses Vorgehen ist erst dann didaktisch gerechtfertigt, wenn die Relevanz der führenden (minimalen) Monome erkannt wurde.

## ↑ Reduzierte Gröbner Basis

1.  $G = \{f_1, f_2, \dots, f_n\}$
2.  $G' = G$   
Ermittle für jedes Paar  $f_i, f_j \in G'$  ( $i < j$ ) den Rest  $r$  bei der Division von  $S(f_i, f_j)$  durch die Elemente von  $G'$  (Reduktion mit  $G'$ ). Falls  $r \neq 0$ , füge  $r$   $G$  hinzu ( $G = G \cup \{r\}$ ).
3. Falls  $G \neq G'$ , so gehe zu 2. Diese Polynome ergeben die Gröbner Basis.
4. Streiche alle Elemente aus  $G$ , dessen führendes Monom durch ein führendes Monom eines der restlichen Elemente aus  $G$  teilbar ist.  $g \in G$  normieren, minimale Gröbner Basis
5. Eliminiere durch Multiplikation und Subtraktion aus den Elementen von  $G$  Terme, die durch das führende Monom eines anderen Elements aus  $G$  teilbar sind. reduzierte Gröbner Basis

Da eine Gröbner Basis  $G$  genau dann vorliegt,  
falls es für alle  $0 \neq g \in I$  ein  $g_i$  mit  $\text{FM}(g_i)$  teilt  $\text{FM}(g)$  gibt,  
bleibt die Gröbner Basis im 4. Schritt erhalten. Die Normierung ändert daran nichts.

Wenn irgendein Term eines Polynoms  $g \in G$  durch das führende Monom eines anderen Polynoms  $h \in G$  teilbar ist, können wir diesen Term zum Verschwinden bringen, indem wir  $g$  durch  $g$  minus ein Vielfaches von  $h$  ersetzen. Da sich dabei nichts an den führenden Monomen der Elemente von  $G$  ändert, bleibt  $G$  im 5. Schritt eine Gröbner Basis.

Eine minimale Gröbner Basis erhält man mit dem folgenden Algorithmus:

1.  $G = \{f_1, f_2, \dots, f_n\}$
2.  $G' = G$   
Ermittle für jedes Paar  $f_i, f_j \in G'$  ( $i < j$ ) den Rest  $r$  bei Reduktion von  $S(f_i, f_j)$  mit  $G'$ .  
Falls  $r \neq 0$ , dann  $G = G \cup \{r\}$ .
3. Reduziere jedes  $f \in G$  (Ergebnis  $r$ ) mit  $G \setminus \{f\}$ .  
Falls  $r = 0$ , dann  $G = G \setminus \{f\}$ , sonst ersetze in  $G$   $f$  durch  $r$ .
4. Falls  $G \neq G'$ , gehe zu 2.

In der im 3. Schritt schließlich entstehenden Basis hat kein  $f \in G$  mehr einen führenden Term, der durch den führenden Term eines Elements von  $G \setminus \{f\}$  teilbar wäre.

## ↑ Eindeutig bestimmte reduzierte Gröbner Basis, Normalform

Satz

Jedes (endlich erzeugte) Ideal  $I$  hat eine eindeutig bestimmte reduzierte Gröbner Basis (hinsichtlich einer Monomordnung).

Seien  $F = \{f_1, f_2, \dots, f_m\}$  und  $G = \{g_1, g_2, \dots, g_n\}$  reduzierte Gröbner Basen für das Ideal.

Für  $f_i$  existiert ein  $j$  mit  $\text{FM}(g_j)$  teilt  $\text{FM}(f_i)$ , da die Reduktion von  $f_i$  mit  $G$  null ist.

Für dieses  $g_j$  existiert genau ein  $k$  mit  $\text{FM}(f_k)$  teilt  $\text{FM}(g_j)$ , da die Reduktion von  $g_j$  mit  $F$  null ist.

Dann folgt:  $\text{FM}(f_k)$  teilt  $\text{FM}(f_i)$ . Es muss  $k = i$  sein, da  $F$  als reduzierte Gröbner Basis minimal ist, und dann auch  $\text{FM}(f_i) = \text{FM}(g_j)$ . Somit gibt es zu jedem  $f_i \in F$  genau ein  $g_j \in G$  mit  $\text{FM}(f_i) = \text{FM}(g_j)$ .

Die Situation ist symmetrisch. Zu jedem  $g_j \in G$  gibt es genau ein  $f_i \in F$  mit  $\text{FM}(f_i) = \text{FM}(g_j)$ .

Insbesondere haben  $G$  und  $F$  gleichviele Elemente.

Tatsächlich muss sogar  $f_i = g_j$  sein, denn:

$f_i - g_j \in I$  reduziert mit  $F$  ergibt null.  $\text{FM}(f_i - g_j)$  muss daher durch ein führendes Monom eines  $f \in F$  teilbar sein. Nun sind die Basen aber reduziert und die Menge der führenden Monome von  $f \in F$  stimmt mit der Menge der führenden Monome von  $g \in G$  überein. Somit enthält  $f_i - g_j$  kein Monom (die führenden Monome von  $f_i$  und  $g_j$  heben sich weg), das durch das führende Monom irgendeines Elements von  $F$  teilbar wäre. Also ist  $f_i - g_j = 0$ . □

Satz

Der Rest  $r$  bei Reduktion von  $f \in k[x_1, x_2, \dots, x_n]$  mit einer Gröbner Basis  $G$  ist eindeutig.

Mit  $f - r_1 \in \langle G \rangle$  (von  $G$  erzeugtes Ideal) und  $f - r_2 \in \langle G \rangle$  ( $r_i$  Reste) ist auch  $r_1 - r_2 \in \langle G \rangle$ .

Dann muss es ein  $\text{FM}(g_i)$  ( $g_i \in G$ ) geben, dass  $\text{FM}(r_1 - r_2)$  teilt.

Das ist ein Widerspruch zur Reduktion mit  $G$ , somit gilt  $r_1 - r_2 = 0$ .

Der Divisionsrest  $r$  von  $f$  unter  $G$  heißt Normalform von  $f$  bezüglich  $G$ ,  $r = N_G(f)$ .

## ↑ Monomordnung

Monome mit z. B. 3 Variablen ( $x^4, xy^2z^3, yz^5$ ) sind Terme  $x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}$  mit einem Exponentenvektor  $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{N}_0^3$ .

$$(x_1, x_2, x_3) = (y, x, z), \text{ (3! Permutationen möglich)} \quad x^4 = y^0x^4z^0 \hat{=} (0, 4, 0), \quad yz^5 = y^1x^0z^5 \hat{=} (1, 0, 5)$$

Eine Monomordnung lässt sich bei festgelegter Reihenfolge der Variablen als Ordnung der Exponentenvektoren auffassen. Es gibt sehr viele Möglichkeiten, diese Menge anzuordnen. Für die Polynomdivision ist es erforderlich, dass die Ordnung bei der Multiplikation erhalten bleibt

$$(\alpha_1, \alpha_2, \alpha_3) < (\beta_1, \beta_2, \beta_3) \implies (\alpha_1 + \gamma_1, \alpha_2 + \gamma_2, \alpha_3 + \gamma_3) < (\beta_1 + \gamma_1, \beta_2 + \gamma_2, \beta_3 + \gamma_3)$$

(der führende Term des Produkts zweier Polynome ist dann das Produkt der führenden Terme der Faktoren) und jede Teilmenge  $\subseteq \mathbb{N}_0^n$  ein kleinstes Element hat, damit die Division nach endlich vielen Schritten abbricht.

lexikographische Ordnung lex, Maple plex( $x, y, z$ ) mit  $x > y > z$

$$(1, 3, 4) < (2, 1, 2), \quad (3, 1, 4) < (3, 2, 1), \quad (3, 3, 1) < (3, 3, 2)$$

Die Werte der ersten gemeinsamen Koordinaten von links, in der sich die beiden Vektoren unterscheiden, bestimmen die Ordnung.

$$\text{für } x > y \text{ in } k[x, y] \quad (x, y) \hat{=} (1, 1) \\ x^3 > x^2y > x^2 > xy^2 > xy > x > y^3 > y^2 > y > 1$$

$$\text{für } y > x \text{ in } k[x, y] \quad (y, x) \hat{=} (1, 1) \\ y^3 > xy^2 > y^2 > x^2y > xy > y > x^3 > x^2 > x > 1.$$

Grad-lexikographische Ordnung deglex, tdeg, lexdeg, Maple grlex( $x, y, z$ ) mit  $x > y > z$

Der Grad (Summe der einzelnen Grade) eines Monoms ist erstes Ordnungskriterium.

Falls beide Monome gleichen Grad haben, wird lexikographisch geordnet,

$$\text{für } x > y > z \text{ in } k[x, y, z] \quad (x, y, z) \hat{=} (1, 1, 1) \\ x^3 > z^3 > x^2 > xy > xz > y^2 > yz > z^2 > x > y > z > 1.$$

Grad-revers-lexikographische Ordnung degrevlex, Maple tdeg( $x, y, z$ ) mit  $x > y > z$

Der Grad (Summe der einzelnen Grade) eines Monoms ist erstes Ordnungskriterium.

Falls beide Monome gleichen Grad haben, wird revers lexikographisch geordnet, d. h.

$(\alpha_1, \alpha_2, \alpha_3) < (\beta_1, \beta_2, \beta_3)$ , falls für die ersten gemeinsamen Koordinaten von rechts, in der sich die beiden Vektoren unterscheiden,  $\alpha_i > \beta_i$  gilt.

$$\text{für } x > y > z \text{ in } k[x, y, z] \quad (x, y, z) \hat{=} (1, 1, 1) \\ x^3 > z^3 > x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1.$$

$$y^2 > xz \iff (0, 2, 0) > (1, 0, 1) \iff 0 < 1$$

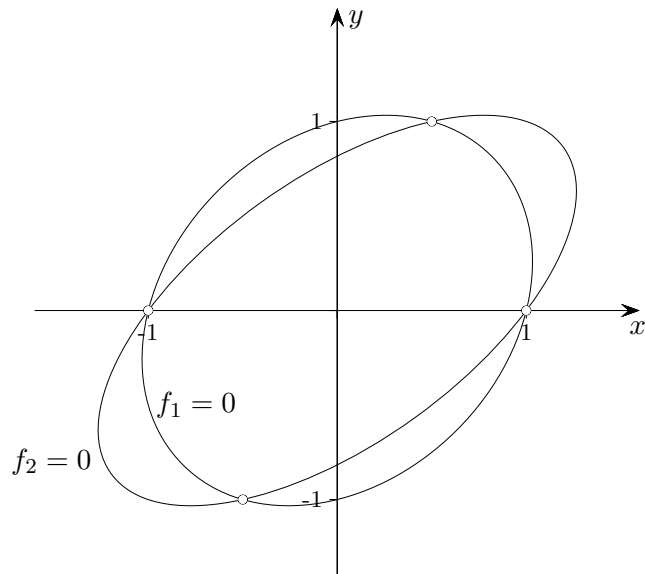
Mit [WolframAlpha](#)

MonomialList[1 + z + y + x + z<sup>2</sup> + yz + xz + y<sup>2</sup> + xy + x<sup>2</sup> + z<sup>3</sup> + x<sup>3</sup>, {x, y, z}, "Lexicographic"]

"DegreeLexicographic"

"DegreeReverseLexicographic"

## ↑ Schnitt von Ellipsen



$$f_1 = 2x^2 - xy + 2y^2 - 2$$

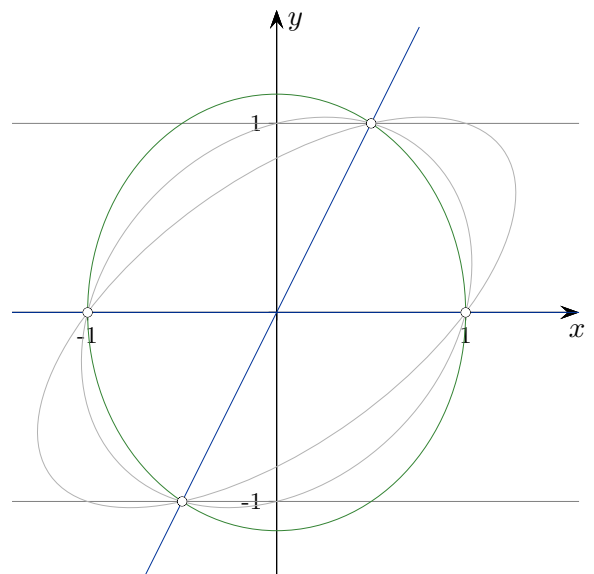
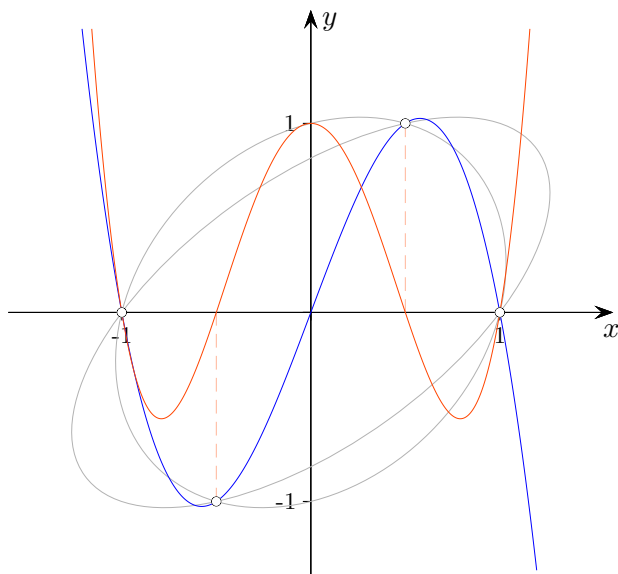
$$f_2 = 2x^2 - 3xy + 3y^2 - 2$$

Gröbner Basis lex  $y > x$

$$G = \{4x^4 - 5x^2 + 1, 8x^3 - 8x + 3y\}$$

$$4x^4 - 5x^2 + 1 = (x - 1)(x + 1)(2x + 1)(2x - 1)$$

Schnittpunkte  $(1, 0)$ ,  $(-1, 0)$ ,  $(1/2, 1)$ ,  $(-1/2, -1)$



Gröbner Basis lex  $x > y$

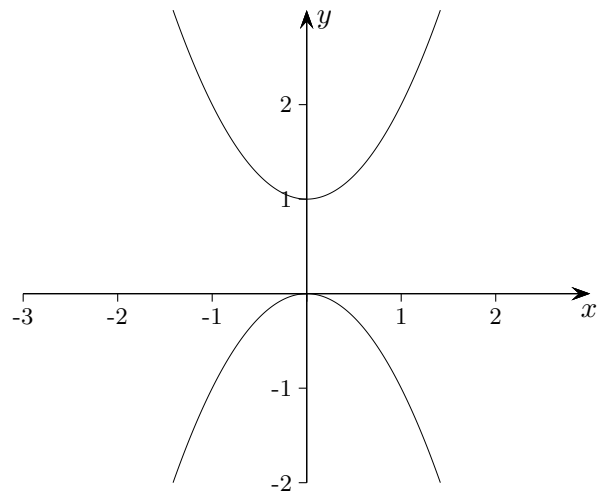
$$G = \{y^3 - y, 2xy - y^2, 4x^2 + 3y^2 - 4\}$$

$$y^3 - y = y(y - 1)(y + 1)$$

Die Graphen veranschaulichen die von der Monomordnung abhängige Berechnung der Schnittpunkte mit Hilfe der Gröbner Basen.

↑ Schnittmenge (Varietät) leer

$$\begin{aligned}x^2 + 1 &= 0 \\ -x^2 &= 0\end{aligned}$$



$$I = \langle x^2 + 1, -x^2 \rangle$$

Die Gröbner Basis für das Ideal  $I$  lautet:  $\{1\}$

Das Gleichungssystem hat genau dann keine Lösung in  $\mathbb{C}$ , wenn das Ideal  $I$  die Eins enthält, also genau dann, wenn die 1 als Linearkombination der erzeugenden Elemente von  $I$  darstellbar ist.

Ob ein Ideal die Eins enthält oder nicht, kann man seiner Gröbner Basis leicht ansehen. Da der führende Term eines jeden Polynoms aus dem Ideal durch den führenden Term eines Elements der Gröbner Basis teilbar sein muss, enthält diese im Falle eines Ideals, das die Eins enthält, ein Polynom, dessen führendes Monom die Eins ist. Da diese bezüglich jeder Monomordnung das kleinste Monom ist, muss somit die Gröbner Basis eine Konstante enthalten. Die zugehörige minimale und erst recht die reduzierte Gröbner Basis besteht in diesem Fall nur aus der Eins.

Wir halten fest:

Ein nichtlineares Gleichungssystem ist genau dann unlösbar selbst in  $\mathbb{C}$ , wenn seine reduzierte Gröbner Basis nur aus der Eins besteht.

Zu zeigen ist jedoch noch

Schwache Form des Hilbertschen Nullstellensatzes, siehe [hier](#)

Genau dann, wenn die  $I$  erzeugenden Polynome  $f_i$  keine gemeinsame Nullstelle in  $\mathbb{C}$  haben, gilt  $1 \in I$  (1 kann als Linearkombination der  $f_i$  dargestellt werden,  $I = \mathbb{Q}[x_1, x_2, \dots, x_n]$ ).

Für Polynome mit einer Variablen ist die Aussage offensichtlich, da gilt  $\text{ggT}(f, g) = 1 \iff f, g$  haben keine gemeinsame Nullstelle in  $\mathbb{C}$ .  $\text{ggT}(f(x), g(x)) = u(x)f(x) + v(x)g(x)$

Starke Form des Hilbertschen Nullstellensatzes

Sei  $I = \langle f_1, \dots, f_k \rangle$  und  $g \in \mathbb{Q}[x_1, x_2, \dots, x_n]$  verschwinde in jedem Punkt von  $V(I) \subset \mathbb{C}^n$ . Dann gibt es eine natürliche Zahl  $\ell$ , so dass  $g^\ell$  in  $I$  liegt.

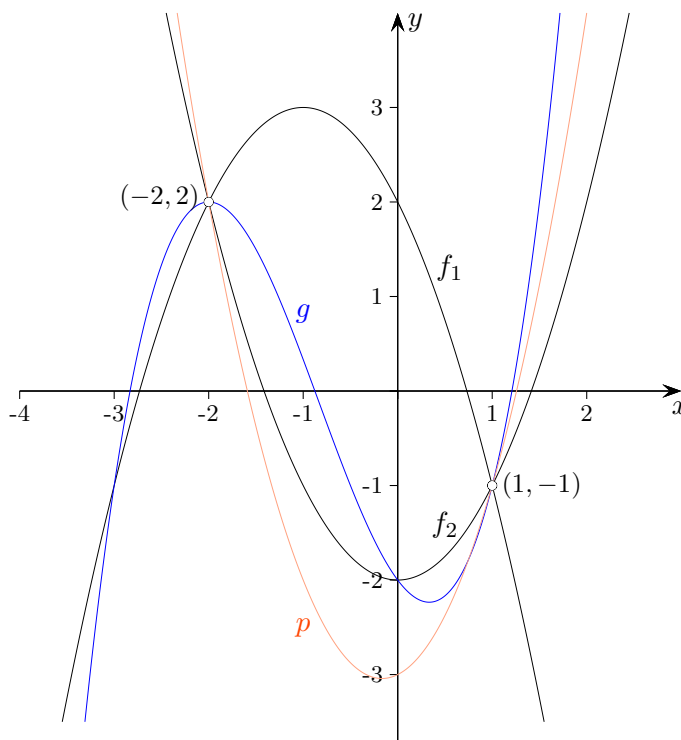
$$I = \langle f_1 = x^3, f_2 = y^3, f_3 = xy(x + y) \rangle$$

$g = x + y$  verschwindet auf  $V(I)$ .

$$g^3 = x^3 + 3x^2y + 3xy^2 + y^3 = f_1 + f_2 + 3f_3$$

$$\implies g^3 \in I$$

## ↑ Starke Form des Hilbertschen Nullstellensatzes



$$I = \langle f_1 = -x^2 - 2x + 2 - y, f_2 = x^2 - 2 - y \rangle$$

Die Gröbner Basis für das Ideal  $I$  lautet:  $\{g_1 = y^2 - y - 2, g_2 = x + y\}$ ,  $V(I) = \{(-2, 2), (1, -1)\}$

$p$  und  $g$  verschwinden auf  $V(I)$ , siehe Grafik.

Nach der starken Form des Hilbertschen Nullstellensatzes liegt jeweils eine Potenz dieser Polynome in  $I$  (hier ist der Exponent 1).

$$p = 3x^2 + x - 6 - 2y = 3g_1 + (3x - 3y + 1)g_2$$

$$g = 2x^3 + 5x^2 - 4x - 6 - 3y = (3 + 2x)g_1 + (5x + 2x^2 - 3y - 2xy)g_2$$

$$\implies p, g \in I$$

trickreiche Beweisidee, betrachte

$$J = \langle -x^2 - 2x + 2 - y, x^2 - 2 - y, 1 - wg \rangle, \text{ die Gröbner Basis ist } \{1\},$$

allgemeiner:

$$J = \langle f_1, f_2, \dots, f_k, 1 - wg \rangle \subset \mathbb{Q}[x_1, x_2, \dots, x_n, w]$$

Es ist zu erkennen, dass keine gemeinsamen Nullstellen vorliegen können, dass also  $V(J) = \emptyset$  ist. Dann kann die schwache Form des Hilbertschen Nullstellensatzes angewandt werden.

$$1 = a_1 f_1 + \dots + a_k f_k + a_0(1 - wg), \quad a_i \in \mathbb{Q}[x_1, x_2, \dots, x_n, w]$$

Für  $w$  wird in diese Linearkombination  $1/g$  eingesetzt (der letzte Summand fällt weg).

Dadurch können die Summanden Potenzen von  $g$  in ihre Nenner bekommen. Durch Multiplikation mit der höchsten auftretenden Potenz  $g^\ell$  erhalten wir die gewünschte Polynomgleichung der Form

$$g^\ell = b_1 f_1 + \dots + b_k f_k, \quad b_i \in \mathbb{Q}[x_1, x_2, \dots, x_n].$$

## ↑ Elimination mit Gröbner Basen, Satz (nulldim. Ideal)

$$\begin{aligned}x^2 + y + z &= 1 \\x + y^2 + z &= 1 \\x + y + z^2 &= 1\end{aligned}$$

$$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$$

Die Gröbner Basis mit lexikographischer Ordnung für das Ideal  $I$  lautet:

$$\begin{aligned}g_1 &= x + y + z^2 - 1 \\g_2 &= y^2 - y - z^2 + z \\g_3 &= 2yz^2 + z^4 - z^2 \\g_4 &= z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1)\end{aligned}$$

Mit den Nullstellen  $\alpha_{1/2} = -1 \pm \sqrt{2}$  des quadratischen Terms erhalten wir für das Gleichungssystem die 5 Lösungen:  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(0, 0, 1)$ ,  $(\alpha_1, \alpha_1, \alpha_1)$ ,  $(\alpha_2, \alpha_2, \alpha_2)$

Bei einer endlichen Lösungsmenge haben die Elemente der Gröbner Basis stets die Form, dass die Lösungen schrittweise ermittelt werden können.

Wenn die Gröbner Basis diese Form hat, ist die Lösungsmenge endlich.

Mit  $g_4$  gibt es nur endlich viele mögliche Werte für  $z$ . Diese in  $g_2$  oder  $g_3$  eingesetzt, ergeben endlich viele mögliche Werte für  $y$ , usw.

### Satz (Elimination)

Sei  $I$  ein nulldimensionales Ideal (die Schnittmenge  $V(I)$  ist endlich) und  $G$  die reduzierte Gröbner Basis für  $I$  hinsichtlich der lexikographischen Ordnung  $x_n > \dots > x_2 > x_1$ .

Dann kann  $G$  so angeordnet werden  $(g_1, \dots, g_k)$ , dass  $g_1$  nur die (kleinste) Variable  $x_1$  enthält,  $g_2$  nur die Variablen  $x_1$  und  $x_2$  enthält und  $\text{FM}(g_2)$  ist eine Potenz von  $x_2$ ,  $g_3$  nur die Variablen  $x_1, x_2$  und  $x_3$  enthält und  $\text{FM}(g_3)$  ist eine Potenz von  $x_3$ , usw.

Die Dreiecksform eines linearen Gleichungssystems ist hier noch zu erkennen. Der Satz (Elimination) folgt unmittelbar aus dem folgenden Satz. Wir ordnen die  $g_j$ , so dass  $\text{FM}(g_j) = x_j^m$  ist. Wegen der lexikographischen Ordnung sind in  $g_j$  nur die Variablen  $x_1, x_2, \dots, x_j$  enthalten.

### Satz (nulldimensionales Ideal)

Die Aussagen sind äquivalent.

- 1)  $V(I)$  ist endlich.
- 2) Für jedes  $i \in \{1, \dots, n\}$  gibt es ein  $j \in \{1, \dots, k\}$  mit  $\text{FM}(g_j) = x_i^m$  für ein  $m \in \mathbb{N}$ .

siehe obiges Beispiel  $\text{FM}(g_1) = x$ ,  $\text{FM}(g_2) = y^2$ ,  $\text{FM}(g_4) = z^6$

1)  $\implies$  2)

Sei die Schnittmenge endlich, z.B.  $(a_1, a_2)$ ,  $(b_1, b_2)$ ,  $(c_1, c_2)$ .

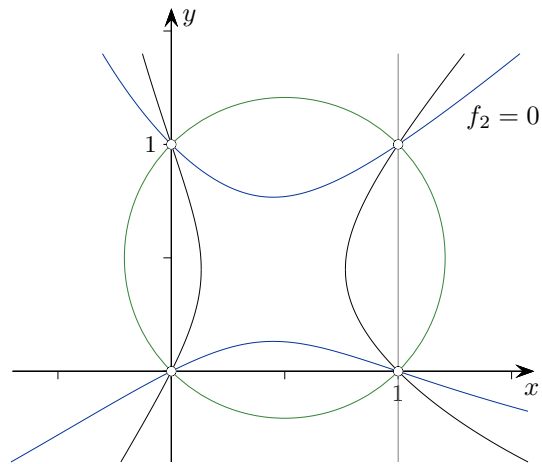
Um die starke Form des Hilbertschen Nullstellensatzes anwenden zu können, benötigen wir ein Polynom  $g(x)$  mit diesen Nullstellen, analog  $g(y)$ . Da es auch mehr Nullstellen sein dürfen, nehmen wir einfacherweise  $g(x) = (x - a_1)(x - b_1)(x - c_1) = x^3 + \dots \in k[x, y]$ . Dann folgt für eine natürliche Zahl  $\ell$   $g^\ell(x) = x^{3\ell} + \dots \in I$ .  $x^{3\ell}$  wird von einem  $\text{FM}(g_j)$  geteilt. Es gibt somit ein  $g_j$  mit einer Potenz von  $x$  als führendes Monom.

2)  $\implies$  1)

Wir hatten uns schon überlegt, dass die Lösungsmenge endlich ist, wenn die Gröbner Basis diese Form hat.



## ↑ Beispiel



Die Abbildung veranschaulicht die Berechnung der Schnittpunkte mit Hilfe der Gröbner Basis.

$$f_1 = x^2y + 2x^2 - xy^2 - 2x - y^2 + y$$

$$f_2 = x^2y + x^2 - xy^2 - x - 2y^2 + 2y$$

Gröbner Basis  $\text{lex } y > x$

$$G = \{g_1 = x^4 + 2x^3 + 3x^2 - 6x, g_2 = x^3 + x^2y + 2x^2 - xy - 3x, g_3 = x^2 + y^2 - x - y\}$$

$$x^4 + 2x^3 + 3x^2 - 6x = x(x-1)(x^2 + 3x + 6)$$

Schnittpunkte  $(0, 0), (1, 0), (0, 1), (1, 1)$

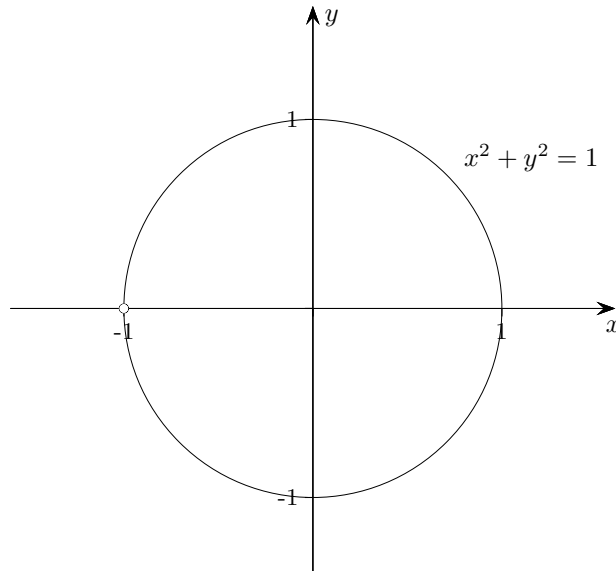
Probe, die Gröbner Basis erzeugt das Ideal  $\langle f_1, f_2 \rangle$ .

$$f_1 = g_2 + (-x-1)g_3$$

$$f_2 = g_2 + (-x-2)g_3$$

## ↑ Implizite Darstellung

Für nichtlineare Gleichungssysteme gibt es vielfältige Anwendungen, z.B. können Parameterdarstellungen in implizite Darstellungen umgeformt werden.



$$x = \frac{1-t^2}{1+t^2}$$

$$y = \frac{2t}{1+t^2}$$

Gröbner Basis lex  $t > x > y$  für

$$I = \langle (1+t^2)x - (1-t^2), (1+t^2)y - 2t \rangle:$$

$$G = \{x^2 + y^2 - 1, ty + x - 1, tx + t - y\}$$

$(-1, 0)$  ist in der Parameterdarstellung nicht enthalten.

$$x = t_1 t_2$$

$$y = t_1 t_2^2$$

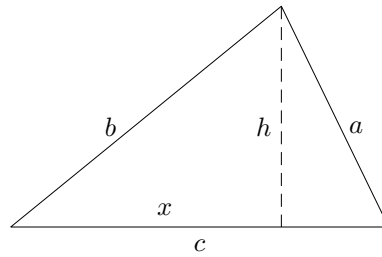
$$z = t_1^2$$

Gröbner Basis lex  $t_1 > t_2 > x > y$  für

$$I = \langle x - t_1 t_2, y - t_1 t_2^2, z - t_1^2 \rangle:$$

$$G = \{x^4 - y^2 z, t_2 y z - x^3, \dots\} \quad \text{ergibt die Fläche } z = x^4 / y^2.$$

## ↑ Formel von Heron



Wie lässt sich der Flächeninhalt  $A$  eines Dreiecks durch die Seitenlängen  $a$ ,  $b$ ,  $c$  ausdrücken?

Nach dem Satz von Pythagoras gilt:  $b^2 = x^2 + h^2$ ,  $a^2 = (c - x)^2 + h^2$ , und weiter  $A = \frac{1}{2}ch$ .

$$f_1 = x^2 + h^2 - b^2$$

$$f_2 = c^2 - 2cx + x^2 + h^2 - a^2$$

$$f_3 = ch - 2A$$

$x, h$  sind zu eliminieren, von Hand wäre das sehr aufwändig.

Gröbner Basis  $\text{lex } x > h > a > b > c > A$

$$G = \{a^4 - 2a^2b^2 - 2a^2c^2 + b^4 - 2b^2c^2 + c^4 + 16A^2, \dots\}$$

$$-16A^2 = a^4 - 2a^2b^2 - 2a^2c^2 + b^4 - 2b^2c^2 + c^4$$

$$= (a + b - c)(a - b + c)(a + b + c)(a - b - c)$$

$$A^2 = \frac{1}{16}(a + b - c)(a - b + c)(a + b + c)(-a + b + c)$$

$$A = \frac{1}{4}\sqrt{(a + b - c)(a - b + c)(a + b + c)(-a + b + c)}$$

alternative Formulierung

$$A = \sqrt{s(s-a)(s-b)(s-c)} \quad \text{mit dem halben Umfang } s = \frac{a+b+c}{2}$$

## ↑ Resultante, Gröbner Basis

$$f = a_2x^2 + a_1x + a_0$$

$$g = b_2x^2 + b_1x + b_0$$

In  $\mathbb{C}$  gilt:

$$\text{Res}(f, g) = 0 \iff f \text{ und } g \text{ haben eine gemeinsame Nullstelle.}$$

$$\text{Res}(f, g) = \begin{vmatrix} a_2 & a_1 & a_0 & \square \\ \square & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & \square \\ \square & b_2 & b_1 & b_0 \end{vmatrix} = a_0^2b_2^2 - a_0a_1b_1b_2 - 2a_0a_2b_0b_2 + a_0a_2b_1^2 + a_1^2b_0b_2 - a_1a_2b_0b_1 + a_2^2b_0^2$$

Gröbner Basis  $\text{lex } x > a_0 > a_1 > a_2 > b_0 > b_1 > b_2$  für

$$I = \langle a_2x^2 + a_1x + a_0, b_2x^2 + b_1x + b_0 \rangle \subset \mathbb{C}[x, a_0, a_1, a_2, b_0, b_1, b_2]:$$

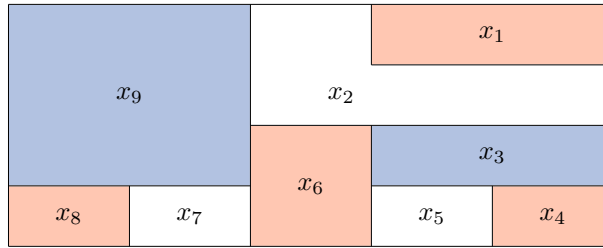
$$G = \{ a_0^2b_2^2 - a_0a_1b_1b_2 - 2a_0a_2b_0b_2 + a_0a_2b_1^2 + a_1^2b_0b_2 - a_1a_2b_0b_1 + a_2^2b_0^2, \dots \}$$

Das Element aus  $G$  ohne  $x$  stimmt mit  $\text{Res}(f, g)$  überein.

Das von diesem Element erzeugte Ideal heißt 1. Eliminationsideal (hier wurde  $x$  eliminiert).

Die Berechnung der Gröbner Basis für  $f$  und  $g$  mit jeweils Grad 4 übersteigt im Allgemeinen die Speicherkapazität.

## ↑ Einfärben von Landkarten



Alle Landkarten können mit vier Farben so gefärbt werden, dass benachbarte Gebiete nicht dieselbe Farbe haben (Vier-Farben-Satz). Um zu entscheiden, ob drei Farben zum Färben einer speziellen Landkarte ausreichen, analysiert man ein System von Polynomen, das die Landkarte repräsentiert. Jede Farbe wird durch eine komplexe kubische Einheitswurzel und jedes Gebiet wird durch eine Variable  $x_i$  so codiert, dass die Variable nur einen der drei Werte annehmen kann, der für eine der drei Farben steht. Somit erhalten wir die Bedingung  $x_i^3 - 1 = 0$  für jedes Gebiet  $i = 1, \dots, 9$ .

Für zwei benachbarte Gebiete, vertreten durch  $x_j$  und  $x_k$ ,

$(j, k) \in \{(1, 2), (2, 3), (2, 6), (2, 9), (3, 4), (3, 5), (3, 6), (4, 5), (5, 6), (6, 7), (6, 9), (7, 8), (7, 9), (8, 9)\}$ , gilt die Bedingung

$$0 = 1 - 1 = x_j^3 - x_k^3 = (x_j - x_k)(x_j^2 + x_j x_k + x_k^2) \quad \text{und wegen } x_j \neq x_k \quad x_j^2 + x_j x_k + x_k^2 = 0.$$

Wir überprüfen, ob das System mit 23 polynomialen Gleichungen gelöst werden kann.

mit Maple

with(Groebner):

```
Basis([x1^3 - 1, x2^3 - 1, x3^3 - 1, x4^3 - 1, x5^3 - 1, x6^3 - 1, x7^3 - 1, x8^3 - 1, x9^3 - 1,
      x1^2 + x1 * x2 + x2^2, x2^2 + x2 * x3 + x3^2, x2^2 + x2 * x6 + x6^2, x2^2 + x2 * x9 + x9^2, x3^2 + x3 * x4 + x4^2,
      x3^2 + x3 * x5 + x5^2, x3^2 + x3 * x6 + x6^2, x4^2 + x4 * x5 + x5^2, x5^2 + x5 * x6 + x6^2, x6^2 + x6 * x7 + x7^2,
      x6^2 + x6 * x9 + x9^2, x7^2 + x7 * x8 + x8^2, x7^2 + x7 * x9 + x9^2, x8^2 + x8 * x9 + x9^2],
      plex(x1, x2, x3, x4, x5, x6, x7, x8, x9));
```

```
[x1^3 - 1, x1^2 + x1 * x2 + x2^2, -x1^2 - x1 * x2 + x2 * x3 + x3^2, x4 + x3 + x2,
      x5 - x2, x6 + x3 + x2, x7 - x2, x8 + x3 + x2, x9 - x3]
```

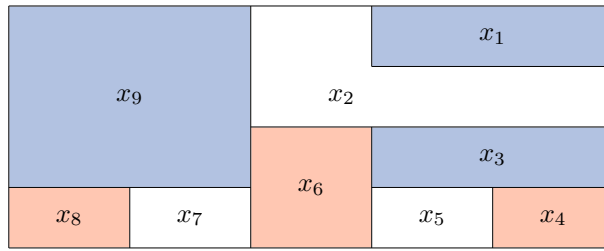
$$\begin{aligned} 0 &= -x_1^2 - x_1 x_2 + x_2 x_3 + x_3^2 \\ &= (x_1 + x_2 + x_3)(x_3 - x_1) \end{aligned}$$

Somit können  $x_1, x_2$  und  $x_3$  verschiedene Farben vertreten ( $x_1 + x_2 + x_3 = 0$ ) oder es gilt  $x_1 = x_3$ .

Für  $x_1, x_2$  und  $x_3$  verschieden erhalten wir weiter  $x_2 = x_5 = x_7, x_3 = x_9$  und  $x_8, x_6$  müssen von  $x_2$  und  $x_3$  verschieden sein, also  $x_4$ .

Im 2. Fall erhalten wir  $x_1 = x_3 = x_9, x_4 = x_6 = x_8$  und  $x_2 = x_5 = x_7$ .

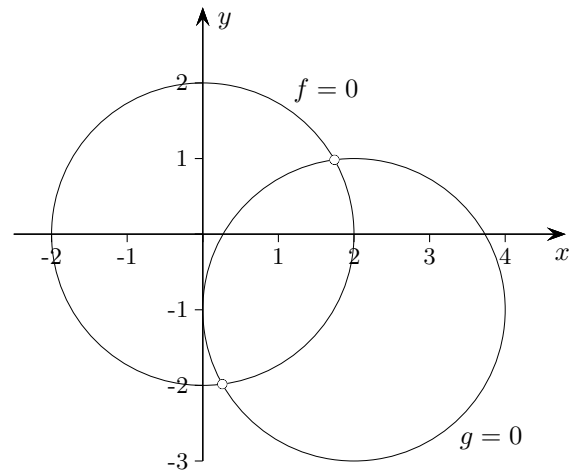
Es gibt daher, von Permutationen der Farben abgesehen, 2 verschiedene Lösungen.



## ↑ Polynom-Transformation

$$f = x^2 + y^2 - 4$$

$$g = (x - 2)^2 + (y + 1)^2 - 4$$



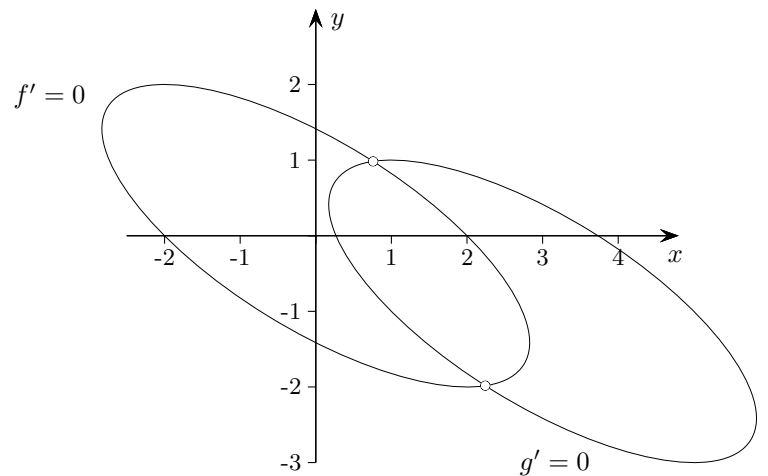
$$f = x^2 + y^2 - 4$$

$$g = (x - 2)^2 + (y + 1)^2 - 4$$

$$x \leftrightarrow x + y \quad \text{Transformation}$$

$$f' = (x + y)^2 + y^2 - 4$$

$$g' = (x + y - 2)^2 + (y + 1)^2 - 4$$



Hier wird ein gemeinsamer Schnittpunkt  $(x_0, y_0)$  von  $f = 0$  und  $g = 0$  auf den gemeinsamen Schnittpunkt  $(x_0 - y_0, y_0)$  von  $f' = 0$  und  $g' = 0$  transformiert.

$$f = x^2yz + 2xy + x$$

$$x \leftrightarrow x + 2z$$

$$y \leftrightarrow y - z$$

$$f' = (x + 2z)^2(y - z)z + 2(x + 2z)(y - z) + x + 2z$$

$$= -4z^4 - (4x - 4y)z^3 - (x^2 - 4xy + 4)z^2 + (x^2y - 2x + 4y + 2)z + 2xy + x$$

Für den Beweis der schwachen Form des Hilbertschen Nullstellensatzes benötigen wir eine in einer Variablen lineare Transformation, so dass wie hier ein Polynom in  $z$  mit dem größten Potenzterm  $-4z^4$  vom Grad des (höchsten) Grades von  $f$  ( $2 + 1 + 1$ ) und Koeffizienten aus  $\mathbb{Q}[x, y]$  vorliegt.

Es wird dann nur um die Existenz von gemeinsamen Schnittpunkten gehen, und nicht um die spezielle Lage.

$$f(x_1, x_2, \dots, x_n) \text{ linear in } x_n \text{ transformiert: } f'(x_1 + \lambda_1 x_n, x_2 + \lambda_2 x_n, \dots, x_{n-1} + \lambda_{n-1} x_n, x_n) = c x_n^{\text{grad } f} + \dots$$

$c$  ist ein Polynom in den  $\lambda_i$ , die so gewählt werden können, dass  $c \neq 0$  ist.

## ↑ Schwache Form des Hilbertschen Nullstellensatzes

Schwache Form des Hilbertschen Nullstellensatzes

Genau dann, wenn die  $I$  erzeugenden Polynome  $f_1, f_2, \dots, f_m$  keine gemeinsame Nullstelle in  $\mathbb{C}$  haben, ist  $1 \in I$  ( $1$  kann als Linearkombination der  $f_i$  dargestellt werden,  $I = \mathbb{Q}[x_1, \dots, x_n]$ ).

Für Polynome mit einer Variablen ist die Aussage offensichtlich, da Polynome in  $\mathbb{C}$  in Linearfaktoren zerfallen.

Der Nullstellensatz wird durch Induktion über die Anzahl  $n$  der Variablen bewiesen.

Für  $n > 1$  betrachten wir ein Erzeugendensystem  $f_1, f_2, \dots, f_m$  von  $I$ . Wir können annehmen, dass  $f_1$  den Term  $x_n^{\text{grad } f_1}$  enthält. Eine lineare Koordinatentransformation ändert schließlich nichts daran, ob  $V(I)$  leer ist oder nicht und auch nichts daran, ob  $I$  die Eins enthält oder nicht.

Unter der Annahme, dass  $V(I) = \emptyset$  ist, basteln wir uns Polynome  $a_i$  aus  $\mathbb{Q}[x_1, \dots, x_{n-1}]$ , die in  $I$  enthalten sind und keine gemeinsame Nullstelle in  $\mathbb{C}^{n-1}$  haben. Nach Induktionsannahme kann die Eins als Linearkombination der  $a_i$  dargestellt werden. Mit den  $a_i$  liegt dann die Eins in  $I$ , und wir sind fertig.

Wir fassen  $f_2, \dots, f_m$  mit einer Linearkombination mit einer neuen Variablen  $u$  zusammen und bilden

$$h = f_2 + u f_3 + \dots + u^{m-2} f_m \in \mathbb{Q}[x_1, \dots, x_n, u], \quad \text{sowie die Resultante}$$

$$\text{Res}(f_1, h, x_n) \in \mathbb{Q}[x_1, \dots, x_{n-1}, u] \quad \text{und schreiben sie als Polynom in } u$$

$$\text{Res}(f_1, h, x_n) = a_k(x_1, \dots, x_{n-1})u^k + \dots + a_0(x_1, \dots, x_{n-1}) \quad \text{mit } a_i \in \mathbb{Q}[x_1, \dots, x_{n-1}].$$

Die Resultante zweier Polynome lässt sich als Linearkombination dieser Polynome darstellen.

Es gibt daher Polynome  $p, q \in \mathbb{Q}[x_1, \dots, x_n, u]$ , so dass gilt

$$\text{Res}(f_1, h, x_n) = p f_1 + q h = p f_1 + q f_2 + q u f_3 + \dots + q u^{m-2} f_m.$$

Vergleichen wir dies mit obiger Darstellung der Resultante als Polynom in  $u$ , sehen wir, dass die Koeffizientenpolynome  $a_i(x_1, \dots, x_{n-1})$  im Ideal  $I = \langle f_1, f_2, \dots, f_m \rangle$  liegen müssen.

Angenommen, die  $a_i$  hätten eine gemeinsame Nullstelle  $(z_1, \dots, z_{n-1})$  in  $\mathbb{C}^{n-1}$ . Dann wäre

$\text{Res}(f_1, h, x_n)(z_1, \dots, z_{n-1}, u) \in \mathbb{Q}[u]$  das Nullpolynom. Somit hätten die beiden Polynome

$$f_1(z_1, \dots, z_{n-1}, x_n) \in \mathbb{Q}[x_n] \quad \text{und}$$

$$h(z_1, \dots, z_{n-1}, x_n, u) \in \mathbb{Q}[x_n, u]$$

einen nichtkonstanten gemeinsamen Faktor. In  $\mathbb{C}$  gäbe es dann eine Nullstelle  $z_n$  von  $f_1(z_1, \dots, z_{n-1}, x_n)$ , für die  $h(z_1, \dots, z_{n-1}, z_n, u)$  das Nullpolynom wäre (der gemeinsame Faktor hängt nicht von  $u$  ab, da  $f_1$  diese Variable nicht enthält).  $f_1(z_1, \dots, z_{n-1}, z_n)$  verschwände und nach Definition von  $h$  auch alle  $f_j(z_1, \dots, z_{n-1}, z_n)$  für  $j = 2, \dots, m$ . Damit läge  $(z_1, \dots, z_{n-1}, z_n)$  in  $V(I)$ , was wir aber als leer vorausgesetzt haben. Damit ist klar, dass die  $a_i$  keine gemeinsame Nullstelle haben können, und der Satz ist bewiesen.

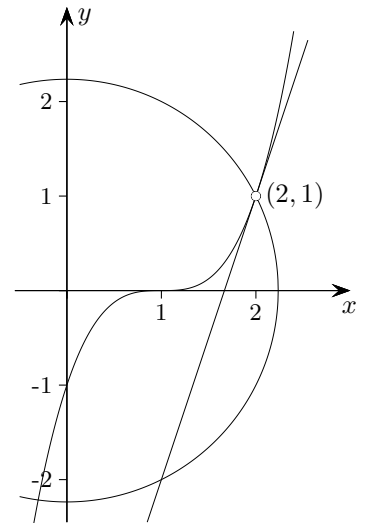
Die folgende Beispielrechnung erhellt die Beweisführung.



## ↑ Nullstellensatz Erläuterungen

$$\begin{aligned} f_1 &= y - 3x + 5 \\ f_2 &= x^2 + y^2 - 5 \\ f_3 &= y - x^3 + 3x^2 - 3x + 1 \end{aligned}$$

$V(I)$  soll mit Hilfe von Resultanten ermittelt werden.



Mit [WolframAlpha](#)

$$\text{GroebnerBasis}[\{y - 3x + 5, x^2 + y^2 - 5, y - x^3 + 3x^2 - 3x + 1\}, \{x, y\}] \\ \{y - 1, x - 2\}$$

Die Polynome  $f_1, f_2, f_3$  erzeugen das Ideal  $I$ .

Spitzen-Idee:  $f_2, f_3$  mit einer Linearkombination mit einer neuen Variablen  $u$  zusammenzufassen

$$h = f_2 + u f_3 \in \mathbb{Q}[x, y, u], \quad \text{die Resultante}$$

$$\text{Res}(f_1, h, y) \in \mathbb{Q}[x, u] \quad \text{zu bilden und sie als Polynom in } u$$

$$\text{Res}(f_1, h, y) = \underbrace{(-x^3 + 3x^2 - 4)}_{a_1} u + \underbrace{10x^2 - 30x + 20}_{a_2} \quad \text{mit Koeffizienten aus } \mathbb{Q}[x] \text{ zu schreiben.}$$

Die Resultante zweier Polynome lässt sich als Linearkombination dieser Polynome darstellen.

Es gibt daher Polynome  $p, q \in \mathbb{Q}[x, y, u]$ , so dass gilt

$$\text{Res}(f_1, h, y) = p f_1 + q h = p f_1 + q f_2 + q u f_3.$$

Vergleichen wir dies mit obiger Darstellung der Resultante als Polynom in  $u$ , z.B.  $a_1 = q f_3$ , sehen wir, dass die Koeffizientenpolynome  $a_1(x)$  und  $a_2(x)$  im Ideal  $I = \langle f_1, f_2, f_3 \rangle$  liegen müssen.

Die Probe mit der Gröbner Basis  $a_1 = (-x^2 + x + 2)(x - 2)$ ,  $a_2 = 10(x - 1)(x - 2)$  zeigt auch  $a_i \in I$ .

Die  $a_i$  haben die gemeinsame Nullstelle  $z_1 = 2$  in  $\mathbb{C}$ . Dann ist

$$\text{Res}(f_1, h, y)(z_1, u) \in \mathbb{Q}[u] \text{ das Nullpolynom}$$

Somit haben die beiden Polynome (in  $\mathbb{C}$  gilt:  $\text{Res}(f, g) = 0 \iff f$  und  $g$  haben eine gemeinsame Nullstelle)

$$f_1(z_1, y) = y - 1 \in \mathbb{Q}[y] \subset \mathbb{Q}[y, u] \text{ und}$$

$$h(z_1, y, u) = (y - 1)(y + u + 1) \in \mathbb{Q}[y, u]$$

einen nichtkonstanten gemeinsamen Faktor, hier  $(y - 1)$ . In  $\mathbb{C}$  gibt es dann die Nullstelle  $z_2 = 1$  von  $f_1(z_1, y)$ , für die  $h(z_1, z_2, u)$  das Nullpolynom ist (der gemeinsame Faktor hängt nicht von  $u$  ab, da  $f_1$  diese Variable nicht enthält).  $f_1(z_1, z_2)$  verschwindet und nach Definition von  $h$  auch alle  $f_j(z_1, z_2)$  für  $j = 2, 3$ .

Damit liegt  $(z_1, z_2) = (2, 1)$  in  $V(I)$ .

Für eine alternative Berechnung mit Resultanten siehe [hier](#).

↑

© Roelfs

## ↑ Lemma von Dickson

Jedes monomiale Ideal  $I \subset k[x_1, \dots, x_n]$  kann von endlich vielen Monomen erzeugt werden.

Der Beweis wird durch vollständige Induktion nach  $n$  geführt.

Im Fall  $n = 1$  wird  $I$  vom Monom mit dem kleinsten Exponenten erzeugt.

Sei heuristisch  $n = 2$ .

Die erzeugenden Monome besitzen die Form  $x^\alpha y^\beta$ ,  $\alpha, \beta \in \mathbb{N}_0$ .

Wir benötigen eine endliche Menge  $L$  an Monomen, so dass jedes Monom aus  $I$  von einem Monom aus  $L$  geteilt wird.

Sei  $J \subset k[x]$  das Ideal (Projektion von  $I$  auf  $k[x]$ ), das von allen  $x^\alpha$  erzeugt wird, für die  $x^\alpha y^\beta \in I$  ist.

Nach Induktionsvoraussetzung wird  $J$  (hier  $n = 1$ ) von einem Monom  $x^{\alpha_{\min}}$  erzeugt.

Sei für  $x^{\alpha_{\min}} y^\beta \in I$  für  $\beta$  der größte Exponent  $\beta_{\max}$ .  $L$  enthält  $x^{\alpha_{\min}} y^\beta$ .

Betrachte für  $\beta = 0, \dots, \beta_{\max} - 1$  jeweils das Ideal  $J_\beta \subset k[x]$ , das von den Monomen  $x^\alpha$  erzeugt wird, für die  $x^\alpha y^\beta \in I$  gilt. Jedes der  $J_\beta$  wird nach Induktionsannahme von einem Monom erzeugt.

$L$  besteht zusätzlich aus all diesen, mit dem zugehörigen  $y^\beta$  ergänzten Monomen.

Sei heuristisch  $n = 3$ .

Die erzeugenden Monome besitzen die Form  $x^\alpha y^\beta z^\gamma$ ,  $\alpha, \beta, \gamma \in \mathbb{N}_0$ .

Wir benötigen eine endliche Menge  $L$  an Monomen, so dass jedes Monom aus  $I$  von einem Monom aus  $L$  geteilt wird.

Sei  $J \subset k[x, y]$  das Ideal (Projektion von  $I$  auf  $k[x, y]$ ), das von allen  $x^\alpha y^\beta$  erzeugt wird, für die  $x^\alpha y^\beta z^\gamma \in I$  ist.

Nach Induktionsvoraussetzung wird  $J$  (hier  $n = 2$ ) von endlich vielen Monomen  $x^{\alpha_k} y^{\beta_k}$  erzeugt.

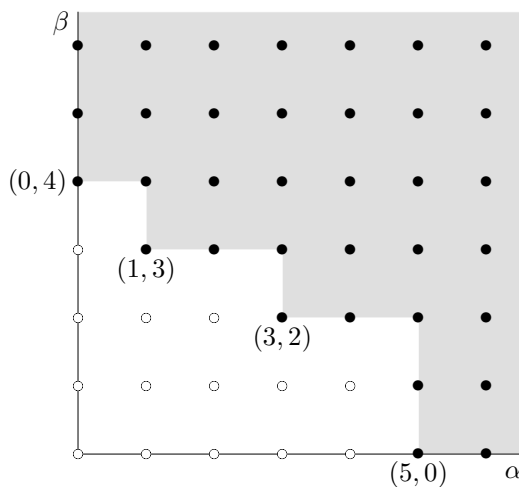
Für ein bestimmtes  $k'$  gibt es dann einen größten Exponenten  $\gamma_{\max}$  mit  $x^{\alpha_{k'}} y^{\beta_{k'}} z^{\gamma_{\max}} \in I$ .

$L$  enthält die  $J$  erzeugenden, mit  $z^{\gamma_{\max}}$  ergänzten Monome  $x^{\alpha_k} y^{\beta_k} z^{\gamma_{\max}}$ .

Betrachte für  $\gamma = 0, \dots, \gamma_{\max} - 1$  jeweils das Ideal  $J_\gamma \subset k[x, y]$ , das von den Monomen  $x^\alpha y^\beta$  erzeugt wird, für die  $x^\alpha y^\beta z^\gamma \in I$  gilt. Jedes der  $J_\gamma$  wird nach Induktionsannahme von endlich vielen Monomen erzeugt.

$L$  besteht zusätzlich aus all diesen, mit dem zugehörigen  $z^\gamma$  ergänzten Monomen.

Der Induktionsschritt von  $n - 1$  nach  $n$  erfordert mehr Indizes, aber keine weitere Idee.



Das Ideal  $I$  wird von den zugehörigen Monomen  $x^\alpha y^\beta$  des grau gefärbten Bereichs erzeugt.

$$\beta_{\max} = 4, y^4 \in L$$

$$J_0 = J_1 = \langle x^5 \rangle, x^5 \in L, x^5 y \in L$$

$$J_2 = \langle x^3 \rangle, x^3 y^2 \in L$$

$$J_3 = \langle x \rangle, xy^3 \in L$$

$$I = \langle y^4, x^5, x^3 y^2, xy^3 \rangle$$

↑

© Roelfs

## ↑ Hilbertscher Basissatz

Für ein beliebiges, im Allgemeinen nicht monomiales Ideal  $I \subset k[x_1, \dots, x_n]$  wählen wir eine Monomordnung und definieren das monomiale Ideal  $\text{FM}(I) = \langle \text{FM}(f) \mid f \in I \setminus \{0\} \rangle$ , das von den führenden Monomen aller Elemente von  $I$  erzeugt wird. Für die null existiert kein führender Term.

Nach dem Lemma von Dickson wird  $\text{FM}(I)$  von endlich vielen Monomen erzeugt, und zwar von der Form  $\text{FM}(f_i)$ ,  $i = 1, \dots, m$ . Wir werden sehen, dass diese Elemente  $f_i$  das Ideal  $I$  erzeugen. Damit folgt

Hilbertscher Basissatz

Jedes Ideal  $I \subset k[x_1, \dots, x_n]$  hat ein endliches Erzeugendensystem.

Um zu zeigen, dass die Elemente  $f_i$  das Ideal  $I$  erzeugen, ist nachzuweisen, dass ein beliebiges Element  $f \in I$  als Linearkombination der  $f_i$  darstellbar ist.

Eine Division von  $f$  durch  $f_1, \dots, f_m$  ergibt  $f = a_1 f_1 + \dots + a_m f_m + r$ ,  $a_i$  und  $r$  Polynome.

Falls  $r$  nicht verschwindet, zeigt der Divisionsalgorithmus, dass das führende Monom  $\text{FM}(r)$  von  $r$  durch keines der führenden Monome  $\text{FM}(f_i)$  teilbar ist. Andererseits ist aber  $r = f - (a_1 f_1 + \dots + a_m f_m) \in I$ , und damit liegt  $\text{FM}(r)$  im Ideal  $\text{FM}(I)$ . Da dieses von den  $\text{FM}(f_i)$  erzeugt wird, muss  $\text{FM}(r)$  Vielfaches eines  $\text{FM}(f_i)$  sein, ein Widerspruch. Also ist  $r = 0$ .

Einfache Folgerung

Sei  $I_1 \subset I_2 \subset I_3 \subset \dots$  eine aufsteigende Kette von Idealen im Polynomring.

Dann stabilisiert sich die Kette irgendwann:  $I_n = I_{n+1} = I_{n+2} = \dots$

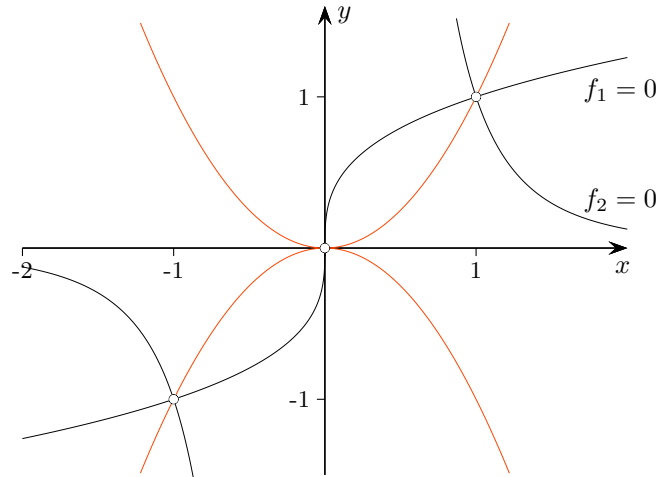
$I := \bigcup_{j \in \mathbb{N}} I_j$  ist auch ein Ideal.

Dieses ist endlich erzeugt:  $I = \langle g_1, \dots, g_m \rangle$

Irgendein  $I_k$  enthält alle  $g_i$ .

## ↑ Vektorraum der Normalformen

Die Normalformen  $N_G(f)$  von  $f \in k[x_1, \dots, x_n]$  (Reste bei Reduktion mit einer Gröbner Basis  $G$ ) sind bei gegebener Monomordnung eindeutig bestimmt und aufgrund der Division nicht teilbar durch die führenden Monome von  $G$ . Normalformen sind daher  $k$ -Linearkombinationen von Monomen aus der Komplementärmenge von  $\text{FM}(G)$ . Sie bilden einen Vektorraum. Schauen wir uns das an einem Beispiel an.



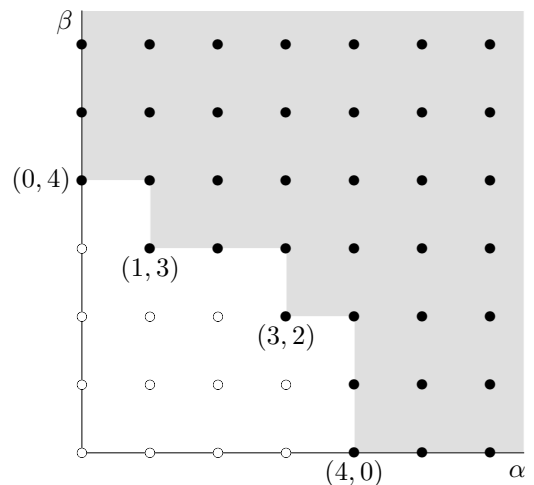
$$I = \langle f_1 = xy^3 - x^2, f_2 = x^3y^2 - y \rangle$$

Gröbner Basis  $\text{deglex } x > y$

$$G = \{f_1 = x(y^3 - x), f_2 = x^3y^2 - y, y(y^3 - x), x^4 - y^2\}$$

$$\langle \text{FM}(I) \rangle = \langle \text{FM}(G) \rangle = \langle xy^3, x^3y^2, y^4, x^4 \rangle, \text{ siehe hier}$$

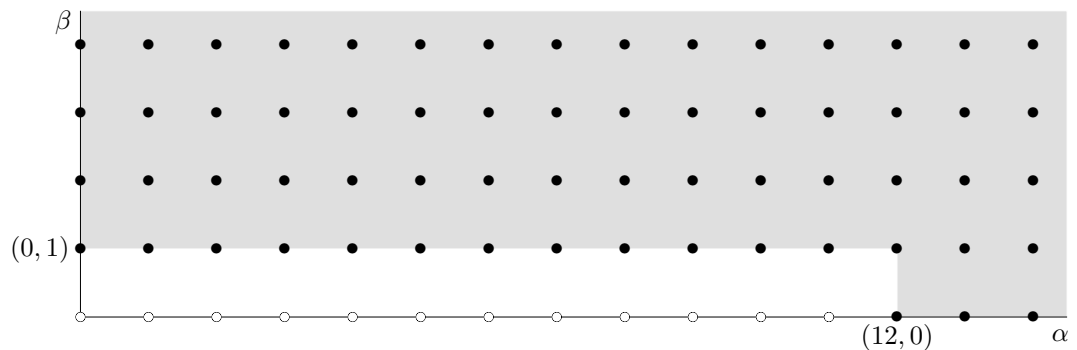
Eine Basis des Vektorraums der Normalformen besteht aus den Monomen  $1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^3$ , die im weißen Bereich liegen.



Wir ändern die Monomordnung.

Gröbner Basis  $\text{lex } y > x$

$$G = \{x^{12} - x^2, y - x^7\} \quad \langle \text{FM}(I) \rangle = \langle y, x^{12} \rangle$$



Nun bilden die Monome  $1, x, x^2, \dots, x^{11}$  eine Basis. Beachte: Die Dimension 12 ist erhalten geblieben.  $V(I)$  enthält 11 verschiedene Punkte.  $V(I) = \{(0,0)\} \cup \{(\zeta, \zeta^7) \mid \zeta^{10} = 1\}$  (Es gibt 10 verschiedene 10-te Einheitswurzeln in  $\mathbb{C}$ .)

## ↑ Multiplikation mod $G$

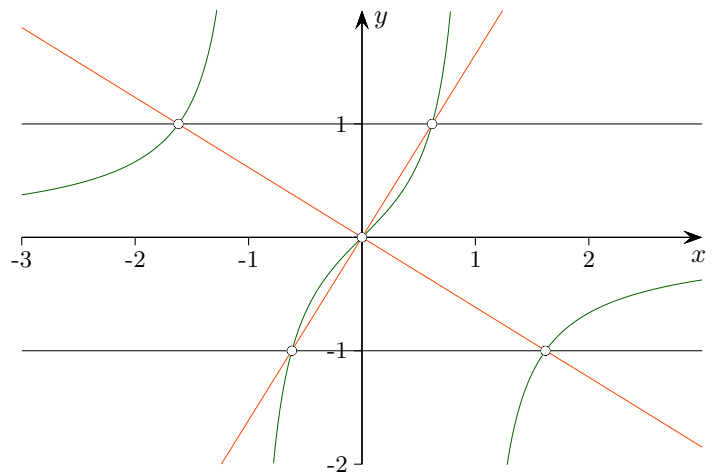
Aus der Eindeutigkeit (siehe [hier](#)) des Restes  $r$  folgt für Nebenklassen unmittelbar:

Sei  $G = \{g_1, \dots, g_m\}$  eine Gröbner Basis für das Ideal  $I \subset R = k[x_1, \dots, x_n]$ .

Dann gilt für  $f, g \in R$ :  $f - g \in I$  ( $f \equiv g, f + I = g + I$ )  $\iff N_G(f) = N_G(g)$

$$\begin{aligned} f &= p + N_G(f) \\ g &= q + N_G(g), \quad p, q \in I, \quad f \equiv N_G(f), \quad g \equiv N_G(g) \\ f - g &= p - q + \underbrace{N_G(f) - N_G(g)}_{N_G(f-g)}, \quad f - g \in I \iff N_G(f-g) = 0 \end{aligned}$$

Mit  $f - g \in I$  nehmen  $f$  und  $g$  auf  $V(I)$  gleiche Werte an.



$$I = \langle x^2y + x - y, xy^2 - x \rangle$$

Gröbner Basis  $\text{lex}(x, y)$

$$G = \{g_1 = x^2 + xy - y^2, g_2 = y^3 - y, g_3 = xy^2 - x\}$$

FM( $G$ ):  $x^2, y^3, xy^2$

Die Monome  $1, x, y, y^2, xy$  sind eine Basis des Vektorraums der Normalformen.  
Das Produkt mod  $G$  von Basiselementen ergibt wieder eine Normalform.

$\circ$	1	$x$	$y$	$y^2$	$xy$
1	1	$x$	$y$	$y^2$	$xy$
$x$	$x$	$y^2 - xy$	$xy$	$x$	$y - x$
$y$	$y$	$xy$	$y^2$	$y$	$x$
$y^2$	$y^2$	$x$	$y$	$y^2$	$xy$
$xy$	$xy$	$y - x$	$x$	$xy$	$y^2 - xy$

Mit [WolframAlpha](#)

$$\text{PolynomialReduce}[x^2y^2, \{x^2 + xy - y^2, y^3 - y, xy^2 - x\}, \{x, y\}]$$

erhalten wir z.B.  $xy \circ xy = x^2y^2 = y^2g_1 + (y - x)g_2 + y^2 - xy$ , somit  $x^2y^2 \equiv y^2 - xy$ .

## ↑ Endlichkeitssatz

Sei  $G = \{g_1, \dots, g_k\}$  eine Gröbner Basis für das Ideal  $I \subset \mathbb{C}[x_1, \dots, x_n]$ .

Der Satz (nulldimensionales Ideal) kann zum Endlichkeitssatz erweitert werden.

Die Aussagen sind äquivalent.

- 1)  $V(I)$  ist endlich.
- 2) Für jedes  $i \in 1, \dots, n$  gibt es ein  $j \in \{1, \dots, k\}$  mit  $\text{FM}(g_j) = x_i^m$  für ein  $m \in \mathbb{N}$ .
- 3) Der Vektorraum der Normalformen ist endlich-dimensional.

(Dieser Vektorraum ist isomorph zu  $\mathbb{C}[x_1, \dots, x_n]/I$ .)

1)  $\iff$  2)

nachgewiesen

2)  $\implies$  3)

Das Komplement der Menge  $\text{FM}(G)$  ist endlich, somit ist der Vektorraum endlich-dimensional.

3)  $\implies$  1)

Um zu zeigen, dass  $V(I)$  endlich ist, reicht der Nachweis, dass es für jedes  $i$  nur endlich viele Komponenten  $x_i$  der Punkte aus  $V(I)$  gibt.

Für ein festes  $i$  sind die Elemente  $1, N(x_i), N(x_i^2), N(x_i^3), \dots, N(x_i^s)$  für ein  $s$  linear abhängig.

Die Null ist damit als nichttriviale Linearkombination darstellbar:  $c_0 + c_1 N(x_i) + c_2 N(x_i^2) + \dots + c_s N(x_i^s) = 0$   
 $\iff N(c_0 + c_1 x_i + c_2 x_i^2 + \dots + c_s x_i^s) = 0$ , d.h.  $c_0 + c_1 x_i + c_2 x_i^2 + \dots + c_s x_i^s \in I$ .

Für  $V(I)$  gilt:  $c_0 + c_1 x_i + c_2 x_i^2 + \dots + c_s x_i^s = 0$  und diese Gleichung hat nur endl. viele Lösungen. □

Genauer formuliert:

- 2) Für jedes  $i \in 1, \dots, n$  gibt es ein  $j \in \{1, \dots, k\}$  mit  $\text{FM}(g_j) = x_i^{m_i}$ ,  $m_i \in \mathbb{N}$ .

Dann folgt:  $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n} \in \langle \text{FM}(I) \rangle$

Für die Exponenten  $\alpha_i$  der Monome  $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$  des Komplements von  $\langle \text{FM}(I) \rangle$  gilt für jedes  $i$ :

$0 \leq \alpha_i \leq m_i - 1$ . Die Anzahl dieser Monome - und damit auch die Dimension des Vektorraums der Normalformen - beträgt damit höchstens  $m_1 m_2 \dots m_n$ .

Es soll noch gezeigt werden, dass die Anzahl der Punkte von  $V(I)$  höchstens der Dimension des Vektorraums der Normalformen ist.

Beweisidee:

Zu jedem Punkt  $p_i \in V(I)$ ,  $i = 1, \dots, m$ , wird ein Polynom  $f_i \in k[x_1, \dots, x_n]$  mit  $f_i(p_i) = 1$  und  $f_i(p_j) = 0$  für  $j \neq i$  konstruiert und nachgewiesen, dass die Normalformen  $N(f_i)$  linear unabhängig sind.

Angenommen, die Punkte  $p_1$  und  $p_2$  haben die unterschiedlichen  $t$ -ten Koordinaten  $a$  und  $b$ .

Für  $g_2 = (x_t - b)/(a - b)$  gilt  $g_2(p_1) = 1$  und  $g_2(p_2) = 0$ . In gleicher Weise sei für die Punkte  $p_1$  und  $p_3$  das Polynom  $g_3$  mit  $g_3(p_1) = 1$  und  $g_3(p_3) = 0$  gebildet, usw.

$f_1 = g_2 \cdot g_3 \cdot \dots \cdot g_m$  hat die gewünschte Eigenschaft  $f_1(p_1) = 1$  und  $f_1(p_j) = 0$  für  $j \neq 1$ .

Mit der gleichen Vorgehensweise erhalten wir für jeden Punkt  $p_i$  ein Polynom  $f_i$  mit der angegebenen Eigenschaft.

Zur linearen Unabhängigkeit:

$$c_1 N(f_1) + c_2 N(f_2) + \dots + c_m N(f_m) = 0 \iff N(c_1 f_1 + c_2 f_2 + \dots + c_m f_m) = 0,$$

d.h.  $c_1 f_1 + c_2 f_2 + \dots + c_m f_m$  ist Element von  $I$  und verschwindet daher auf  $V(I)$ .

$p_1$  eingesetzt, ergibt  $0 = c_1$ ,  $p_2$  eingesetzt, ergibt  $0 = c_2$ , usw.

↑

↑  $|V(I)| = \text{Dimension des Vektorraums der Normalformen}$

Betrachten wir das Beispiel auf Seite 4.

$$I = \langle xy - 1, y^2 - 1 \rangle$$

Gröbner Basis  $\text{lex}(x, y)$

$$G = \{y^2 - 1, x - y\}$$

FM( $G$ ):  $x, y^2$

Die Monome  $1, y$ , bilden eine Basis des Vektorraums der Normalformen.  
Die Dimension 2 stimmt hier mit der Anzahl der Schnittpunkte überein.

Beispiel auf Seite 5

$$I = \langle x^2 + y - 1, x + y^2 - 1 \rangle$$

Gröbner Basis  $\text{lex}(x, y)$

$$G = \{x + y^2 - 1, y^4 - 2y^2 + y\}$$

FM( $G$ ):  $x, y^4$

Die Monome  $1, y, y^2, y^3$  bilden eine Basis des Vektorraums der Normalformen.  
Die Dimension 4 stimmt hier mit der Anzahl der Schnittpunkte überein.

Abschließend soll noch eine hinreichende Bedingung gefunden werden, so dass die Anzahl der Punkte von  $V(I)$  genau der Dimension des Vektorraums der Normalformen ist.

Es genügt herauszufinden, unter welcher Voraussetzung die  $N(f_i)$  den Vektorraum der Normalformen aufspannen, die lineare Unabhängigkeit wurde schon nachgewiesen.

Sei  $g$  ein Element dieses Vektorraums und  $a_i = g(p_i)$ . Betrachte  $h = g - (a_1 f_1 + a_2 f_2 + \dots + a_m f_m)$ . Offensichtlich ist  $h(p_i) = 0$  für alle  $i$ .  $h$  verschwindet also auf  $V(I)$ . Nach der starken Form des Hilbertschen Nullstellensatzes folgt  $h^\ell \in I$  für ein  $\ell$ . Wenn jetzt  $h \in I$  wäre, folgte  $N(h) = 0$  und dann weiter  $N(g) = a_1 N(f_1) + a_2 N(f_2) + \dots + a_m N(f_m)$  und die Behauptung wäre bewiesen.

Die Voraussetzung:  $h^\ell \in I$  impliziert  $h \in I$  (anschaulich  $I$  enthält die Wurzeln der Elemente aus  $I$ ) wird in der Idealtheorie mit dem Begriff *Radikal* erfasst.

## ↑ Syzygie

Betrachten wir die Gleichung  $h_1g_1 + \dots + h_ng_n = 0$ ,  $g_i, h_i \in \mathbb{Q}[x, y, z]$ ,  $g_i$  seien gegeben.  
 Gesucht sind für die  $g_i$  alle Linearkombinationen der null mit Koeffizienten aus  $\mathbb{Q}[x, y, z]$ .

Eine Lösung  $h = (h_1, \dots, h_n)$  wird als  $n$ -Tupel geschrieben und heißt Syzygie der  $g_i$ .  
 Die Summe zweier Lösungen, sowie ein Vielfaches (mit einem Polynom) einer Lösung ist wieder eine Lösung.  
 Die Lösungsmenge ist algebraisch ein Modul, Schreibweise  $\text{Syz}(g_1, \dots, g_n)$ . Das ist eine Verallgemeinerung eines Vektorraums. Statt eines Körpers liegt bei einem Modul nur ein Ring (hier Polynomring) vor.

Beispiel

Die Polynome seien aus  $\mathbb{Q}[x, y, z, w]$ .

$\text{Syz}(x^2 - yw, xy - wz, y^2 - xz) = ?$

$(y, -x, w)$  und  $(-z, y, -x)$  sind hier beides Syzygien, denn es ist:

$$\begin{aligned} y(x^2 - yw) - x(xy - wz) + w(y^2 - xz) &= 0 &= x^2y - y^2w - x^2y + xzw + y^2w - xzw \\ -z(x^2 - yw) + y(xy - wz) - x(y^2 - xz) &= 0 &= -x^2z + yzw + xy^2 - yzw - xy^2 + x^2z \end{aligned}$$

An dieser Stelle können wir noch nicht einsehen, dass diese beiden Syzygien den Lösungsmodul erzeugen.

Es ist einfach, Syzygien für eine Gröbner Basis  $g_i$  zu bestimmen.

Zu  $i \neq j$  wird das  $S$ -Polynom  $S(g_i, g_j)$  als Linearkombination der  $g_i$  dargestellt, z.B. ergeben die Koeffizienten von  $S(g_1, g_2) - (h_1g_1 + \dots + h_ng_n) = 0$  eine Syzygie.

$\{g_1 = x^2 - yw, g_2 = xy - wz, g_3 = y^2 - xz\}$  ist eine Gröbner Basis für die Monomordnung  $\text{degrevlex}$ ,  
Maple `tdeg(x, y, z, w)`.

$$\begin{aligned} S(g_1, g_2) &= yg_1 - xg_2 = -wy^2 + xwz = -wg_3 \\ yg_1 - xg_2 + wg_3 &= 0, \quad \text{Syzygie } (y, -x, w) \end{aligned}$$

$$\begin{aligned} S(g_1, g_3) &= y^2g_1 - x^2g_3 = x^3z - y^3w = xzg_1 - ywg_3 \\ y^2g_1 - x^2g_3 - (xzg_1 - ywg_3) &= 0, \quad \text{Syzygie } (y^2 - xz, 0, -x^2 + yw) \end{aligned}$$

$$\begin{aligned} S(g_2, g_3) &= yg_2 - xg_3 = x^2z - yzw = zg_1 \\ yg_2 - xg_3 - zg_1 &= 0, \quad \text{Syzygie } (-z, y, -x) \end{aligned}$$

beachte:  $(y^2 - xz, 0, -x^2 + yw) = y(y, -x, w) + x(-z, y, -x)$



## ↑ Syzygie

Besonders einfach wird die Gleichung  $h_1c_1g_1 + \dots + h_nc_ng_n = 0$ , gegeben  $g_i \in \mathbb{Q}[x, y]$  und  $c_i \in \mathbb{Q}$ , falls die  $g_i$  Monome sind, z. B.

$$h_1c_1x + h_2c_2x^2y + h_3c_3xy^2 = 0.$$

Syzygien  $h = (h_1, h_2, h_3)$ , sie entsprechen den  $S'$ -Polynomen  $S(c_i g_i, c_{i+1} g_{i+1})$ , sind für das Beispiel:

$$\begin{array}{llll} (c_2xy, -c_1, 0), & S'_{1,2} = (xy, -d_{1,2}, 0), & d_{1,2} = c_1/c_2, & S'_{1,2} = (h_1, -d_{1,2}h_2, 0) \\ (c_3y^2, 0, -c_1), & S'_{1,3} = (y^2, 0, -d_{1,3}), & d_{1,3} = c_1/c_3, & S'_{1,3} = (h_1, 0, -d_{1,3}h_3) \\ (0, c_3y, -c_2x), & S'_{2,3} = (0, y, -d_{2,3}x), & d_{2,3} = c_2/c_3, & S'_{2,3} = (0, h_2, -d_{2,3}h_3) \end{array}$$

Ein Syzygien-Modul wird von den  $S'_{i,j}$ ,  $1 < i < j < n$ , erzeugt, z. B.  $h = e_1S'_{1,2} + e_2S'_{1,3} + e_3S'_{2,3}$ ,  $e_i \in \mathbb{Q}$ .

Dazu stellen wir uns die linke Seite von  $h_1c_1g_1 + \dots + h_nc_ng_n = 0$  ausmultipliziert vor und nehmen uns einen Term mit dem Monom  $X$  vor. Da  $h$  als Syzygie angenommen wird, ist die Summe aller Terme mit diesem Monom null. O.B.d.A sei

$$\begin{aligned} h &= (f_1h_1, f_2h_2, f_3h_3) && | \text{ d.h. } f_1h_1c_1g_1 + f_2h_2c_2g_2 + f_3h_3c_3g_3 = \underbrace{(f_1c_1 + f_2c_2 + f_3c_3)}_0 X = 0 \\ &= f_1 \underbrace{(h_1, -d_{1,2}h_2, 0)}_{S'_{1,2}} && | (f_1h_1, f_2h_2, f_3h_3) = (f_1h_1, -f_1d_{1,2}h_2, 0) \\ &\quad + (f_1d_{1,2} + f_2) \underbrace{(0, h_2, -d_{2,3}h_3)}_{S'_{2,3}} && | \quad + (0, f_1d_{1,2}h_2 + f_2h_2, \underbrace{-(f_1d_{1,2} + f_2)d_{2,3}}_{-\frac{f_1c_1 + f_2c_2}{c_3}} h_3) \end{aligned}$$

alternativ

$$h_1c_1x + h_2c_2x^2y + h_3c_3xy^2 = 0.$$

Syzygien  $h = (h_1, h_2, h_3)$ , sie entsprechen den  $S$ -Polynomen  $S(c_i g_i, c_{i+1} g_{i+1})$ , sind für das Beispiel:

$$\begin{array}{llll} (c_2xy, -c_1, 0), & S_{1,2} = (c_2xy, -c_1, 0), & S_{1,2} = (c_2h_1, -c_1h_2, 0) \\ (c_3y^2, 0, -c_1), & S_{1,3} = (c_3y^2, 0, -c_1), & S_{1,3} = (c_3h_1, 0, -c_1h_3) \\ (0, c_3y, -c_2x), & S_{2,3} = (0, c_3y, -c_2x), & S_{2,3} = (0, c_3h_2, -c_2h_3) \end{array}$$

Ein Syzygien-Modul wird von den  $S_{i,j}$ ,  $1 < i < j < n$ , erzeugt, z. B.  $h = e_1S_{1,2} + e_2S_{1,3} + e_3S_{2,3}$ ,  $e_i \in \mathbb{Q}$ .

$$\begin{aligned} h &= (f_1h_1, f_2h_2, f_3h_3) \\ &= \frac{1}{c_2} f_1 \underbrace{(c_2h_1, -c_1h_2, 0)}_{S_{1,2}} && | (f_1h_1, f_2h_2, f_3h_3) = \frac{1}{c_2} (f_1c_2h_1, -f_1c_1h_2, 0) \\ &\quad + \frac{1}{c_2c_3} (f_1c_1 + f_2c_2) \underbrace{(0, c_3h_2, -c_2h_3)}_{S_{2,3}} && | \quad + (0, \frac{1}{c_2} (f_1c_1h_2 + f_2c_2h_2), \underbrace{-\frac{1}{c_3} (f_1c_1 + f_2c_2) h_3}_{f_3}) \end{aligned}$$

↑

## ↑ Syzygie

Die Ermittlung von Syzygien für Polynome  $f_1, f_2, \dots, f_n$ , die keine Gröbner Basis bilden, erfolgt mit deren Gröbner Basis  $g_1, g_2, \dots, g_m$  und ihren  $s_1, s_2, \dots, s_\ell$  Syzygien. Desweiteren wird eine  $n \times m$ -Matrix  $T$  benötigt, mit der die  $f_i$  auf die  $g_j$  transformiert werden. Bei der Buchberger-Algorithmus-Ausführung wird ersichtlich, wie sich die  $g_j$  als Linearkombinationen der  $f_i$  darstellen lassen.

$$[g_1, g_2, \dots, g_m] = [f_1, f_2, \dots, f_n] \underbrace{\begin{bmatrix} t_{11} & \dots & t_{1m} \\ \dots & & \\ t_{n1} & & t_{nm} \end{bmatrix}}_T$$

Für eine Syzygie  $s_k$  der  $g_j$  gilt dann:

$$0 = [g_1, g_2, \dots, g_m] \begin{bmatrix} s_{1k} \\ \dots \\ s_{mk} \end{bmatrix} = [f_1, f_2, \dots, f_n] \underbrace{\begin{bmatrix} t_{11} & \dots & t_{1m} \\ \dots & & \\ t_{n1} & & t_{nm} \end{bmatrix} \begin{bmatrix} s_{1k} \\ \dots \\ s_{mk} \end{bmatrix}}_{\text{ergibt eine Syzygie für die } f_i}$$

Wir ermitteln für das Beispiel (siehe Seite 6) eine Syzygie.

$$\begin{aligned} f_1 &= xy - 2y \\ f_2 &= x^2 - 4y^2 \end{aligned} \quad \text{Gröbner Basis } \{g_1 = xy - 2y, g_2 = x^2 - 4y^2, g_3 = y^3 - y\}$$

Syzygien für die  $g_j$

$$\begin{aligned} S(g_1, g_2) &= xg_1 - yg_2 = -2xy + 4y^4 = -2g_1 + 4g_3 \implies (x+2)g_1 - yg_2 - 4g_3 = 0, \quad s_1 = (x+2, -y, -4) \\ S(g_2, g_3) &= y^3g_2 - x^2g_3 = x^2y - 4y^5 = (x+2)g_1 + (-4y^2 - 4)g_3 \implies s_2 = (x+2, -y^3, -4y^2 + x^2 - 4) \end{aligned}$$

Tabelle  $T$

$$\begin{bmatrix} 1 & 0 & \frac{1}{4}(x+2) \\ 0 & 1 & -\frac{1}{4}y \end{bmatrix} \quad S(f_1, f_2) = xf_1 - yf_2 = 4y^3 - 2xy = -2f_1 + 4g_3 \implies g_3 = \frac{1}{4}(x+2)f_1 - \frac{1}{4}yf_2$$

Syzygien für die  $f_j$

$$\begin{bmatrix} 1 & 0 & \frac{1}{4}(x+2) \\ 0 & 1 & -\frac{1}{4}y \end{bmatrix} \begin{bmatrix} x+2 \\ -y \\ -4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & \frac{1}{4}(x+2) \\ 0 & 1 & -\frac{1}{4}y \end{bmatrix} \begin{bmatrix} x+2 \\ -y^3 \\ -4y^2 + x^2 - 4 \end{bmatrix} = \begin{bmatrix} \frac{1}{4}x^3 - xy^2 + \frac{1}{2}x^2 - 2y^2 \\ -\frac{1}{4}x^2y + y \end{bmatrix} = \begin{bmatrix} \frac{1}{4}(x+2)(x^2 - 4y^2) \\ -\frac{1}{4}y(x+2)(x-2) \end{bmatrix} = \begin{bmatrix} s_{11} \\ s_{12} \end{bmatrix}$$

Mit  $f_1 = y(x-2)$  ist die Probe  $s_{11}f_1 + s_{12}f_2 = 0$  im Kopf möglich.

Nebenbei: Das Ergebnis für zwei Polynome  $f_1$  und  $f_2$  ist stets auch ohne Rechnung offensichtlich. Hier kann der Faktor  $(x+2)$  entfallen.

## ↑ Syzygie

Weitere Syzygien ergeben sich möglicherweise durch:

$$[g_1, g_2, \dots, g_m] = [f_1, f_2, \dots, f_n] \underbrace{\begin{bmatrix} t_{11} & \dots & t_{1m} \\ \dots & & \\ t_{n1} & & t_{nm} \end{bmatrix}}_T$$

$$[f_1, f_2, \dots, f_n] = [g_1, g_2, \dots, g_m] \underbrace{\begin{bmatrix} u_{11} & \dots & u_{1n} \\ \dots & & \\ u_{m1} & & u_{mn} \end{bmatrix}}_U$$

$U$  entsteht durch Reduktion der  $f_i$ .

$$\implies [f_1, f_2, \dots, f_n] = [f_1, f_2, \dots, f_n] TU$$

$$\implies [f_1, f_2, \dots, f_n] (E_n - TU) = 0, \quad n \times n\text{-Einheitsmatrix } E_n$$

Die (transponierten) Spalten der Matrix  $(E_n - TU)$  sind Elemente von  $\text{Syz}(f_1, \dots, f_n)$ .

Im einfachen Beispiel auf der vorigen Seite (die  $f_i$  gehören zur Gröbner Basis) ist  $TU$  die  $2 \times 2$ -Einheitsmatrix und somit  $(E_2 - TU)$  die Nullmatrix, so dass sich nichts Neues ergibt.

## ↑ Syzygie

Ermitteln wir Syzygien für

$$\begin{aligned} f_1 &= x^2 - y \\ f_2 &= xy \\ f_3 &= y^2 - x \end{aligned} \quad \text{Gröbner Basis } \{g_1 = x, g_2 = y\}, \quad (y, -x) \in \text{Syz}(g_1, g_2)$$

$$[g_1, g_2] = [f_1, f_2, f_3] \underbrace{\begin{bmatrix} -y & -1 \\ x & y \\ -1 & -x \end{bmatrix}}_T, \quad T \begin{bmatrix} y \\ -x \end{bmatrix} = \begin{bmatrix} -y^2 + x \\ 0 \\ x^2 - y \end{bmatrix}$$

$$[f_1, f_2, f_3] = [g_1, g_2] \underbrace{\begin{bmatrix} x & y & -1 \\ -1 & 0 & y \end{bmatrix}}_U$$

$$\implies [f_1, f_2, f_3] = [f_1, f_2, f_3] TU$$

$$\implies [f_1, f_2, f_3](E_3 - TU) = 0, \quad 3 \times 3\text{-Einheitsmatrix } E_3$$

Die (transponierten) Spalten der Matrix  $(E_3 - TU)$  sind weitere Elemente von  $\text{Syz}(f_1, f_2, f_3)$ .

$$TU = \begin{bmatrix} 1 - xy & -y^2 & 0 \\ x^2 - y & xy & y^2 - x \\ 0 & -y & 1 - xy \end{bmatrix}, \quad E_3 - TU = \begin{bmatrix} xy & y^2 & 0 \\ -x^2 + y & -xy + 1 & -y^2 + x \\ 0 & y & xy \end{bmatrix}$$

Die 3. Spalte ist linear abhängig von den ersten beiden,

$$(0, -y^2 + x, xy) = -y(xy, -x^2 + y, 0) + x(y^2, -xy + 1, y).$$

Insgesamt erhalten wir die Syzygien  $(xy, -x^2 + y, 0)$ ,  $(y^2, -xy + 1, y)$ ,  $(-y^2 + x, 0, x^2 - y)$ .

Es kann gezeigt werden, dass bei diesem Vorgehen ein Erzeugendensystem des Syzygien-Moduls gefunden wird.

## ↑ Polynomdivision (Reduktion) mit dem Gauss-Algorithmus

$$\frac{x^4 + x^3 + 3x^2 + 2x + 7}{x^2 + x + 1} = ?$$

Wie bei der Reduktion von  $S$ -Polynomen interessiert nur der Rest  $r$ .

$$x^4 + x^3 + 3x^2 + 2x + 7 = q \cdot (x^2 + x + 1) + r$$

Die Koeffizienten werden in eine Matrix eingefügt, geordnet nach Potenzen.

$$\begin{array}{ccccc|c} x^4 & x^3 & x^2 & x & 1 & \\ \hline 0 & 0 & 1 & 1 & 1 & x^2 + x + 1 \\ 1 & 1 & 3 & 2 & 7 & x^4 + x^3 + 3x^2 + 2x + 7 \end{array}$$

Beim Gauss-Algorithmus wird ein Vielfaches einer Zeile zu einer anderen addiert.

Der Rest  $r$  bleibt unverändert, wenn wir Zeilen für  $x \cdot (x^2 + x + 1)$  und  $x^2 \cdot (x^2 + x + 1)$  zur Matrix hinzufügen, damit eine Dreiecksform berechnet werden kann.

Der Dividend bildet die letzte Zeile.

$$\begin{array}{ccccc|c} x^4 & x^3 & x^2 & x & 1 & \\ \hline 1 & 1 & 1 & 0 & 0 & x^4 + x^3 + x^2 \\ 0 & 1 & 1 & 1 & 0 & x^3 + x^2 + x \\ 0 & 0 & 1 & 1 & 1 & x^2 + x + 1 \\ 1 & 1 & 3 & 2 & 7 & x^4 + x^3 + 3x^2 + 2x + 7 \end{array}$$

Der Gauss-Algorithmus liefert:

$$\begin{array}{ccccc} x^4 & x^3 & x^2 & x & 1 \\ \hline 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 5 \end{array}$$

Die händische Probe ergibt:  $x^4 + x^3 + 3x^2 + 2x + 7 = (x^2 + 2)(x^2 + x + 1) + 5$

## ↑ Reduktion mit dem Gauss-Algorithmus

$f = x^2 - y^2 + x + y$  soll mit  $g = xy + 1$  und  $h = y^2 - x$  reduziert werden.

$x^2$	$xy^2$	$xy$	$x$	$y^2$	$y$	$1$		lexikographische Ordnung $x > y$
-1	1	0	0	0	0	0		$xh = xy^2 - x^2$
0	1	0	0	0	1	0		$yg = xy^2 + y$
0	0	0	-1	1	0	0		$h = y^2 - x$
0	0	1	0	0	0	1		$g = xy + 1$
1	0	0	1	-1	1	0		$f = x^2 - y^2 + x + y$

Der Gauss-Algorithmus liefert den Rest **0**:

$x^2$	$xy^2$	$xy$	$x$	$y^2$	$y$	$1$
-1	1	0	0	0	0	0
0	1	0	0	0	1	0
0	0	1	0	0	0	1
0	0	0	-1	1	0	0
0	0	0	0	0	0	0

$$f = x^2 - y^2 + x + y = yg - (x + 1)h = y(xy + 1) - (x + 1)(y^2 - x) + \mathbf{0}$$

Hierauf aufbauend entwickelte Faugère ab 2000 effiziente Algorithmen zur Berechnung einer Gröbner Basis.

## ↑ Gröbner Basis, einleitende Bemerkungen

Wir suchen für die Polynome  $f_1$  und  $f_2$  die gemeinsamen Nullstellen, lösen also das Gleichungssystem

$$f_1(x) = 0 \quad x^3 - x^2 - 2x = 0$$

$$f_2(x) = 0 \quad x^2 - 3x + 2 = 0$$

$$f_3 = f_1 - x f_2 = 2x^2 - 4x$$

$$f_4 = f_3 - 2f_2 = x - 2$$

Durch Multiplikation und Subtraktion fällt jeweils der größte Potenzterm weg.

Eine Nullstelle von  $f_1$  und  $f_2$  ist auch Nullstelle von  $f_4$ , somit ist sie 2.

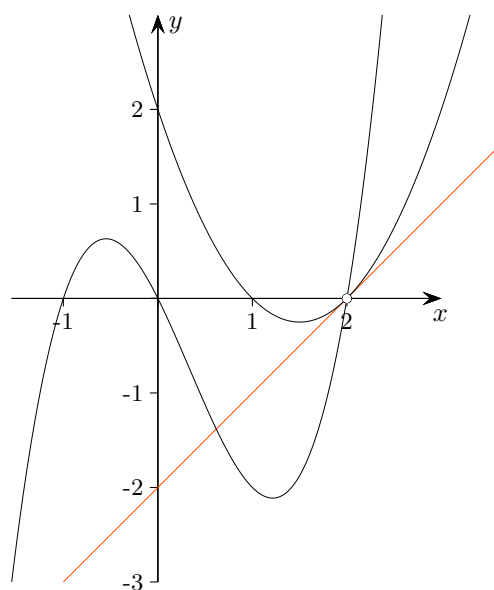
Wenn eine Nullstelle vorliegt, dann ist sie 2.

Die Umkehrung gilt hier auch wegen  $f_1 = (x - 2)(x^2 + x)$  und  $f_2 = (x - 2)(x - 1)$ .

Algebraische Sichtweise:

Im Ideal  $I = \langle f_1, f_2 \rangle = \{k_1 f_1 + k_2 f_2 \mid k_1(x), k_2(x) \text{ Polynome}\}$  dürfen wir addieren, subtrahieren und mit Polynomen multiplizieren, ohne dass sich die Menge  $I$  ändert.

Für das Beispiel gilt  $I = \langle f_1, f_2 \rangle = \langle x - 2 \rangle$ , d.h.  $I$  wird von  $x - 2$  erzeugt.



Betrachten wir nun Polynome mit 3 Variablen, also Funktionen  $f(x, y, z)$  vom  $\mathbb{R}^3$  nach  $\mathbb{R}$ , und das Ideal

$$I = \langle x + y + 3z - 4, x^2 - x, y^2 - y, z^2 - z \rangle.$$

Das Erzeugendensystem  $G = \langle x + y - 1, x^2 - x, y^2 - y, z - 1 \rangle$  von  $I$  ist die reduzierte Gröbner Basis.

Die Elemente von  $I$  lassen sich offensichtlich wegen  $x + y + 3z - 4 = (x + y - 1) + 3(z - 1)$  als Linearkombination, die Koeffizienten sind Polynome, dieser Basiselemente darstellen.

Zu  $G$  gehören dieselben Nullstellen  $\{(1, 0, 1), (0, 1, 1)\}$  wie zu  $I$ , beginne mit  $z - 1 = 0$ .

Zur Ermittlung einer Gröbnerbasis ist ein Divisionsalgorithmus zu entwickeln und zuvor ist eine Ordnung der Potenzterme festzulegen. Für eine lexikographische Ordnung mit  $x > y > z$  gilt z.B.

$$x^2 > xy > xz > y^3 > y^2 > z > 1.$$

## ↑ Gröbner Basis, einleitende Bemerkungen

Der Gröbner-Basis-Algorithmus beruht im Wesentlichen auf der Bildung der sogenannten  $S$ -Polynome. Die Polynome  $f_1 = xy - 2y$ ,  $f_2 = 2y^2 - x^2$  werden so multipliziert und subtrahiert, dass die führenden Potenzterme herausfallen:

$$f_3 = yf_1 - \frac{1}{2}xf_2 = \frac{1}{2}x^3 - 2y^2$$

Sei  $I = \langle xy - 2y, 2y^2 - x^2 \rangle$ .

Reduzierte Gröbner Basis für die lexikographische Ordnung mit  $y > x$ :

$$G = \{x^3 - 2x^2, xy - 2y, 2y^2 - x^2\},$$

lexikographische Ordnung mit  $x > y$ :

$$G = \{y^3 - 2y, xy - 2y, x^2 - 2y^2\}.$$

Falls  $G$  nur endlich viele Lösungen hat, enthält es ein Polynom mit einer von der lexikographische Ordnung abhängigen, kleinsten Variablen.

Zu  $G$  und  $I$  gehören dieselben Nullstellen  $\{(0, 0), (2, \pm\sqrt{2})\}$ , beachte  $x^3 - 2x^2 = x^2(x - 2) = 0$ .

Die Basen sind *reduziert*, da kein Element einer Basis Linearkombination der übrigen ist.

Die führenden (minimalen) Monome für  $y > x$  in  $G = \{x^3 - 2x^2, xy - 2y, 2y^2 - x^2\}$  garantieren, dass jedes Element aus  $I$  durch ein Basiselement teilbar ist.

Diese Eigenschaft ist für eine Gröbner Basis als endliche Teilmenge von  $I$  charakterisierend.

Auf  $x^3$  kann wegen  $x^3 - 2x^2 = 2y(xy - 2y) + (2 - x)(2y^2 - x^2)$  nicht verzichtet werden.

Für  $f \in \mathbb{C}[x, y, z]$  ist die Form  $f = g + r$ ,  $g$  ist Linearkombination der Basiselemente und  $r$  durch diese nicht teilbar, eindeutig.

Zu gegebener Ordnung ist die reduzierte Gröbner Basis eines Ideals eindeutig.



# ↑ Gröbner Basis, Integer Programming

Die Idee von Conti and Traverso 1991 soll an einem einfachen Beispiel dargestellt werden. Gesucht sind die Nullstellen in  $\mathbb{N}$  des Gleichungssystems.

$$\begin{array}{l|l} a + b + c = 4 & x \\ a + 2b = 5 & y \\ b + 2c = 4 & z \end{array}$$

Das Gleichungssystem wird äquivalent einzeilig umgeformt, für jede Zeile wird eine Variable benötigt.

$$\begin{aligned} x^{a+b+c} y^{a+2b} z^{b+2c} &= x^4 y^5 z^4 \\ &= (xy)^a (xy^2 z)^b (xz^2)^c = s^a t^b u^c & | \quad xy = s, xy^2 z = t, xz^2 = u \\ s^a t^b u^c &= x^4 y^5 z^4 \end{aligned}$$

Das Problem besteht nun darin, für die letzte Zeile  $a$ ,  $b$  und  $c$  zu ermitteln. Hierbei sind die Abkürzungen  $s$ ,  $t$  und  $u$  zu berücksichtigen. In 2 Schritten gelangt man zum Ziel.

## 1. Schritt

$$\begin{aligned} &\text{GroebnerBasis}[\{xy - s, xy^2 z - t, xz^2 - u\}, \{x, y, z, s, t, u\}] \\ &\text{hier } G = \{z^3 s^2 - tu, yu - z^2 s, yzs - t, xt - zs^2, xz^2 - u, xy - s\} \end{aligned}$$

## 2. Schritt

$$\begin{aligned} &\text{PolynomialReduce}[x^4 y^5 z^4, \{z^3 s^2 - tu, yu - z^2 s, yzs - t, xt - zs^2, xz^2 - u, xy - s\}, \{x, y, z, s, t, u\}] \\ &\text{hier } st^2 u \text{ Das ergibt die Lösung } a = 1, b = 2, c = 1. \end{aligned}$$

Das Vorgehen ist plausibel.

$$\text{Betrachte die Reduktion } x^4 y^5 z^4 = \underbrace{(\dots)(z^3 s^2 - tu) + (\dots)(yu - z^2 s) + \dots}_{= 0 \text{ für die Abkürzungen, siehe 1. Schritt}} + st^2 u$$

$$\text{Beim System} \quad \begin{array}{l|l} 2a + b - 3c + d = 4 & x \\ -3a + 2b - 2c - d = -3 & y \end{array}$$

ist wegen der entstehenden negativen Exponenten in einem Laurent-Polynomring  $\mathbb{R}[x^{\pm 1}, y^{\pm 1}]$  zu rechnen.

$$\begin{aligned} x^{2a+b-3c+d} y^{-3a+2b-2c-d} &= x^4 y^{-3} \\ &= (x^2 y^{-3})^a (xy^2)^b (x^{-3} y^{-2})^c (xy^{-1})^d = s^a t^b u^c v^d & | \quad x^2 y^{-3} = s, xy^2 = t, \\ s^a t^b u^c v^d &= x^4 y^{-3} & | \quad x^{-3} y^{-2} = u, xy^{-1} = v \end{aligned}$$

Wir benötigen  $\mathbb{R}[x^{\pm 1}, y^{\pm 1}] = \mathbb{R}[x, y, w]/(xyw - 1)$ .

Für diesen Isomorphismus wird eine neue Variable  $w$  eingeführt.

Mit  $xyw - 1 = 0$  folgen  $w = x^{-1} y^{-1}$ ,  $xw = y^{-1}$  und  $yw = x^{-1}$ .

Aus  $x^2 y^{-3}$ ,  $xy^2$ ,  $x^{-3} y^{-2}$ ,  $xy^{-1}$  wird  $x^5 w^3$ ,  $xy^2$ ,  $yw^3$ ,  $x^2 w$ . Beachte:  $x^{-3} y^{-2} = (yw)^3 y^{-2} = yw^3$

GroebnerBasis[ $\{x^5 w^3 - s, xy^2 - t, yw^3 - u, x^2 w - v, xyw - 1\}$ ,  $\{x, y, w, s, t, u, v\}$ ] ergibt

$$G = \{g_1 = t^5 u^3 v^4 - 1, g_2 = s - t^3 u^2 v^5, g_3 = w - tuv, g_4 = y - t^2 uv, g_5 = x - t^2 w v^2\}$$

PolynomialReduce[ $x^7 w^3$ ,  $\{g_3, g_5\}$ ,  $\{x, y, w, s, t, u, v\}$ ] ergibt  $t^{17} u^{10} v^{17}$ ,  $(a, b, c, d) = (0, 17, 10, 17)$ .

## ↑ Gröbner Basis, Integer Programming

$$t^{17}u^{10}v^{17} \xrightarrow{g_1} t^{12}u^7v^{13} \xrightarrow{g_1} t^7u^4v^9 \xrightarrow{g_1} t^2uv^5, \quad (0, 12, 7, 13), (0, 7, 4, 9), (0, 2, 1, 5)$$

$$t^{17}u^{10}v^{17} \xrightarrow{g_2} st^{14}u^8v^{12} \xrightarrow{g_2} s^2t^{11}u^6v^7 \xrightarrow{g_2} s^3t^8u^4v^2, \quad (1, 14, 8, 12), (2, 11, 6, 7), (3, 8, 4, 2)$$

Die Lösungsvielfalt des Gleichungssystem 
$$\begin{aligned} 2a + b - 3c + d &= 4 \\ -3a + 2b - 2c - d &= -3 \end{aligned}$$

lässt sich damit darstellen

(Differenz des inhomogenen Systems ergibt eine Lösung des homogenen Systems):

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 5 \end{pmatrix} + \lambda \begin{pmatrix} 0 \\ 5 \\ 3 \\ 4 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 7 \\ 4 \\ 3 \end{pmatrix} + \nu \begin{pmatrix} 2 \\ 9 \\ 5 \\ 2 \end{pmatrix} + \xi \begin{pmatrix} 3 \\ 11 \\ 6 \\ 1 \end{pmatrix}$$

Mit der Software REDUCE und

```
load_package groebner;
torder({x, y, w, s, t, u, v}, lex);
gb:=groebner {x**5*w**3 - s, x*y**2 - t, y*w**3 - u, x**2*w - v, x*y*w - 1};
preduce (x**7*w**3, gb);
erhalten wir t^2 * u * v^5 und damit (0, 2, 1, 5).
```

Dasselbe Ergebnis liefert [Macaulay2](#) (online-Version).

```
i1: QQ[x, y, w, s, t, u, v, MonomialOrder=>Lex]
i2: I=ideal(x^5 * w^3 - s, x * y^2 - t, y * w^3 - u, x^2 * w - v, x * y * w - 1)
i3: x^7 * w^3 % gb I
o3: t^2uv^5
```

Mit `i4: gens gb I` wird die Gröbner Basis (gb) ermittelt (gens von generators).

Mit [Macaulay2](#) kann ohne Umwege im Quotientenring gerechnet werden.

```
i1: R=QQ[s, t, u, v, MonomialOrder=>Lex, Global=>>false]
i2: R2=R[x, y, z, w]/(x * y * z * w - 1)
i3: I=ideal (x^2 * y^-3 - s, x * y^2 - t, x^-3 * y^-2 - u, x * y^-1 - v)
i4: x^4 * y^-3 % gb I
```

Wir erhalten wieder  $t^2uv^5$  und damit (0, 2, 1, 5).

## ↑ Optimierungsproblem in $\mathbb{N}$

Für das folgende, erstaunlicherweise algebraisch lösbares Problem muss lediglich die Monomordnung angepasst werden.

$$m = 3a + 4b + 2c \quad \longrightarrow \quad \text{Maximum}$$

$$\begin{aligned} 3a + 2b + c &\leq 60 \\ a + 2b + 3c &\leq 80 \\ 2a + b + c &\leq 42 \end{aligned} \quad a, b, c \geq 0$$

Umformulierung

$$n = -3a - 4b - 2c + 0 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 \quad \longrightarrow \quad \text{Minimum}$$

$$\begin{array}{l|l} 3a + 2b + c + e_1 = 60 & x \\ a + 2b + 3c + e_2 = 80 & y \\ 2a + b + c + e_3 = 42 & z \end{array} \quad a, b, c, e_1, e_2, e_3 \geq 0$$

$$\begin{aligned} x^{3a+2b+c+e_1} y^{a+2b+3c+e_2} z^{2a+b+c+e_3} &= x^{60} y^{80} z^{42} \\ &= (x^3 y z^2)^a (x^2 y^2 z)^b (x y^3 z)^c x^{e_1} y^{e_2} z^{e_3} = u_1^a u_2^b u_3^c u_4^{e_1} u_5^{e_2} u_6^{e_3} \\ &\quad | x^3 y z^2 = u_1, x^2 y^2 z = u_2, x y^3 z = u_3, \\ &\quad | x = u_4, y = u_5, z = u_6 \end{aligned}$$

Mit **Macaulay2** ohne Berücksichtigung der Minimum-Bedingung:

```
i1: R = QQ[x, y, z, u1, u2, u3, u4, u5, u6]
i2: I = ideal(u1 - x^3 * y * z^3, u2 - x^2 * y^2 * z, u3 - x * y^3 * z, u4 - x, u5 - y, u6 - z)
i3: x^60 * y^80 * z^42 % gb I
o3: u1^3 u2^19 u3^13 u6
```

Für  $(a, b, c) = (3, 19, 13)$  ist  $m = 111$ .

Mit Berücksichtigung der Minimum-Bedingung:

```
i1: R = QQ[u1, u2, u3, u4, u5, u6,
Weights => -3, -4, -2, 0, 0, 0, MonomialOrder =>Lex, Global =>false]
i2: R2 = R[x, y, z]
i3: I = ideal(u1 - x^3 * y * z^3, u2 - x^2 * y^2 * z, u3 - x * y^3 * z, u4 - x, u5 - y, u6 - z)
i4: x^60 * y^80 * z^42 % gb I
o3: u2^25 u3^10 u6^7
```

Für  $(a, b, c) = (0, 25, 10)$  ist das Maximum  $m = 120$ .

Bei der gewichteten Monomordnung werden die Exponenten zuerst mit den Gewichten multipliziert.

## ↑ Kompatible Monomordnung

Umformulierung

$$n = -3a - 4b - 2c + 0 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 \quad \longrightarrow \quad \text{Minimum}$$

$$\begin{array}{l|l} 3a + 2b + c + e_1 = 60 & x \\ a + 2b + 3c + e_2 = 80 & y \\ 2a + b + c + e_3 = 42 & z \end{array} \quad a, b, c, e_1, e_2, e_3 \geq 0$$

$$\begin{aligned} u_1^a u_2^b u_3^c u_4^{e_1} u_5^{e_2} u_6^{e_3} &= x^{60} y^{80} z^{42} \\ | x^3 y z^2 &= u_1, \quad x^2 y^2 z = u_2, \quad x y^3 z = u_3, \\ | x = u_4, \quad y = u_5, \quad z = u_6 \end{aligned}$$

Diese Beziehungen können auch mit einer Abbildung  $\varphi$  (Homomorphismus) formuliert werden.

$$\begin{aligned} \varphi: \mathbb{Q}[u_1, u_2, \dots, u_6] &\longrightarrow \mathbb{Q}[x, y, z] \\ u_1 &\longrightarrow x^3 y z^2 \\ u_2 &\longrightarrow x^2 y^2 z \\ &\dots \\ u_6 &\longrightarrow z \end{aligned}$$

$\ell = (\ell_1, \ell_2, \dots, \ell_6)$  ist genau dann eine Lösung des LGSs, falls  $\varphi(u_1^{\ell_1} u_2^{\ell_2} \dots u_6^{\ell_6}) = x^{60} y^{80} z^{42}$  ist.

Nahezu plausibel:

Um das Minimum von  $n(\ell)$  zu ermitteln, benötigen wir auf  $\mathbb{Q}[u_1, u_2, \dots, u_6]$  eine (zur Zielfunktion kompatible) Monomordnung  $\prec$ ,

für die gilt:

$$\varphi(u_1^{\ell_1^*} u_2^{\ell_2^*} \dots u_6^{\ell_6^*}) = \varphi(u_1^{\ell_1^{**}} u_2^{\ell_2^{**}} \dots u_6^{\ell_6^{**}}) \text{ und } n(\ell^*) < n(\ell^{**}) \text{ impliziert } u_1^{\ell_1^*} u_2^{\ell_2^*} \dots u_6^{\ell_6^*} \prec u_1^{\ell_1^{**}} u_2^{\ell_2^{**}} \dots u_6^{\ell_6^{**}}.$$

## ↑ Optimierungsproblem in $\mathbb{Z}$

$$n = 3a + 4b + 5c + 8d \quad \longrightarrow \quad \text{Minimum}$$

$$\begin{array}{l|l} 3a - 2b + c + 2d = 160 & x \\ a + 2b - 3c - 5d = 84 & y \\ 2a - b + c = 127 & z \end{array} \quad a, b, c, d \geq 0$$

$$\begin{aligned} x^{3a-2b+c+2d} y^{a+2b-3c-5d} z^{2a-b+c} &= x^{160} y^{84} z^{127} \\ &= (x^3 y z^2)^a (x^{-2} y^2 z^{-1})^b (x y^{-3} z)^c (x^2 y^{-5})^d = u_1^a u_2^b u_3^c u_4^d \\ &\quad | x^3 y z^2 = u_1, x^{-2} y^2 z^{-1} = u_2, x y^{-3} z = u_3, x^2 y^{-5} = u_4 \end{aligned}$$

Macaulay2

```
i1: R = QQ[u1, u2, u3, u4,
      Weights => 3, 4, 5, 8, MonomialOrder => Lex, Global => false]
i2: R2 = R[x, y, z, w]/(x * y * z * w - 1)
i3: I = ideal(x^3 y z^2 - u1, x^-2 y^2 z^-1 - u2, x y^-3 z - u3, x^2 y^-5 - u4)
i4: x^160 * y^84 * z^127 %o gb I
o3: u1^72 u2^39 u3^22
```

Für  $(a, b, c, d) = (72, 39, 22, 0)$  ist das Minimum  $n = 482$ .

Dasselbe Ergebnis erhält man hier mit (nur i1 wird verändert):

```
i1: QQ[u1, u2, u3, u4 ]
i2: R2 = R[x, y, z, w]/(x * y * z * w - 1)
i3: I = ideal(x^3 y z^2 - u1, x^-2 y^2 z^-1 - u2, x y^-3 z - u3, x^2 y^-5 - u4)
i4: x^160 * y^84 * z^127 %o gb I
o4: u1^72 u2^39 u3^22
```

Jedoch ist jetzt für  $(a, b, c, d) = (72, 39, 22, 0)$  nicht erwiesen, dass  $n = 482$  minimal ist.  $(a, b, c, d) = (100, 115, 42, 24)$  löst auch das Gleichungssystem, hingegen ist  $n = 1162$ .

Startseite