Universität Stuttgart
AG Diskrete Strukturen und Symbolisches Rechnen

input : $G = (g_1, \ldots, g_s)$, $g_i \in k[x_1, \ldots, x_n]$
output: $S = \text{STD}(G)$ Gröbner-Basis von $I = (G)$

```
1  S := G; P := {(f, g) | f, g ∈ S, f ≠ g};
2  while (P ≠ ∅) do
3  |  choose (f, g) ∈ P;
4  |  P := P \ {(f, g)};
5  |  h := NF(spoly(f, g)|S);
6  |  if (h ≠ 0) then
7  |  |  P := P ∪ {(h, f) | f ∈ S};
8  |  |  S := S ∪ {h};
9  |  end
10 end
11 return S
```

Eisermann
—
Geck
—
Witt

G.A.G.A.

Ein algorithmischer Zugang zu diskreten Strukturen in Algebra, Geometrie und Topologie

Die G.A.G.A.-Profillinie

Leitidee der Profillinie:

- Zusammenspiel von Abstraktion (Algebra, Geometrie,Topologie, ...) und Algorithmik zur Lösung konkreter Probleme, zugleich fundamental und anwendungsbezogen.
- Symbolisches Rechnen: Vorrangig exakte/symbolische Lösung mit Hilfe algebraischer Algorithmen für diskrete Strukturen. Komplementär zum wissenschaftlichen Rechnen, welches auf numerischen und approximativen Methoden beruht.
- Breite Basis für Spezialisierungen in theoretischer Mathematik (insbesondere in Algebra, algebraischer Geometrie, Topologie und Gruppentheorie), oder auch in der theoretischen Informatik (z.B. algorithmische Gruppentheorie am Institut für formale Methoden der Informatik).

An wen richtet sich diese Profillinie? Dieser Zyklus eignet sich für Studierende, die

- sich gerne mit abstrakten Strukturen beschäftigen.
- Interesse an algorithmischen Methoden / Entwickeln von Algorithmen und konstruktiven Beweisen / Programmierung haben.

Vorlesungen der Profillinie:

- Kernstück der Profillinie sind die Vorlesungen *G.A.G.A. A & B*, sowie die Vorlesungen *Algebra* und *Topologie*. Alle vier Vorlesungen können unabhängig voneinander belegt werden.
- Die Vorlesung *Geometrie* (ab 2. Fachsemester) bietet einen guten Einstieg in den Bereich Algebra und Geometrie.
- Die abstrakten Natur dieser Profillinie kann sehr gut mit Vorlesungen der Profilinien Darstellungstheorie und Geometrie/Topologie sowie mit theoretisch orientierten Ergänzungsmodulen, z.B. aus der Computerlinguistik, theoretischen Informatik oder Philosophie kombiniert werden.

Schematische Übersicht:

Spezialisierung (M.Sc.)

- Algebra (Geck)
- Topologie Spieltheorie (Eisermann)
- Geometrie (Witt)
- Weitere Gebiete reiner Mathematik (IAZ/IGT)

Vertiefung (B.Sc.)

- GAGA A
- GAGA B

Grundlagen (B.Sc.)

- Algebra, Geometrie, Topologie

G.A.G.A. A: Kommutative Algebra und algebraische Geometrie

Grundlegendes Problem ist das Lösen polynomialer Gleichungssysteme in den Variablen $x_1, \ldots, x_n$ definiert durch $f_i \in k[x_1, \ldots, x_n]$ and $b_i \in k$, $i = 1, \ldots, r$, für einen Körper k (z.B. $\mathbb{Q}$ oder $\mathbb{C}$):

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= \sum_{i_1,\ldots,i_n} a^{(1)}_{i_1,\ldots,i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} = b_1 \\ \vdots \qquad &= \qquad \vdots \\ f_r(x_1, \ldots, x_n) &= \sum_{i_1,\ldots,i_n} a^{(r)}_{i_1,\ldots,i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} = b_r, \end{aligned}$$

Für lineare Gleichungssyteme $i_1 = \ldots = i_n$ berechnet der *Gauß-Algorithmus* ein äquivalentes Gleichungssystem möglichst einfacher Gestalt. Im nichtlinearen Fall liefert der *Buchberger-Algorithmus*, der auf der Titelseite abgebildet ist, ein äquivalentes nichtlineares Gleichungssystem, eine sogenannte *Standard-* oder *Gröbner-Basis*.

Theoretische Anwendung. In der algebraischen Geometrie betrachtet man die gemeinsame Nullstellenmenge endlich vieler Polynome:

Abbildung: Die Nullstellenmenge im $\mathbb{R}^3$ von $f(x, y, z) = x^2 + y^2 - (1 - z)z^2 = 0$, die *Ding-Dong-Fläche*, siehe H. Hauser, *Gallery of Singular Algebraic Surfaces*.

Eine Singularität ist ein nicht glatter Punkt, im obigen Beispiel die Spitze. Eine Auflösung der Singularität ist eine Familie von glatten Nullstellenmengen, die in die Singuläre Nullstellenmenge degeneriert.

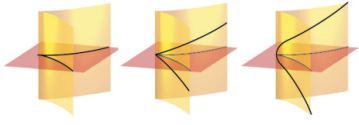


Abbildung: Die Auflösung der singulären Kurve $x^2 = y^3$ Quelle: H. Hauser

Mithilfe von Standardbasen beweist man das berühmte

Theorem (Hironaka, Fields-Medaille 1970).

Jede Nullstellenmenge einer singulären Nullstellenmenge über einen Körper der Charakteristik 0 (z.B. $\mathbb{R}$ oder $\mathbb{C}$) besitzt eine Auflösung.

Siehe H. Hauser, *The Hironaka Theorem on resolution of singularities*, Bulletin of the AMS, vol. 40, no. 3, 323–403.

Praktische Anwendung. Viele Probleme in der diskreten Mathemtik lassen sich auf die Lösung polynomialer Gleichungssysteme zurückführen. Standardbasis-Techniken können z.B. zur Berechnung von Sudokus eingesetzt werden (siehe auch E. Arnold, S. Lucas, *Gröbner Basis Representations of Sudoku*, The College Mathematics Journal 41(2):101–112):

				5			8	
				6	2			5
6			4			7		
		7				9	6	
		5	2		6	1		
	3	6				4		
		3			7			4
1			5	8				
	6			1				

Das gegebene Sudoku...

3	4	1	7	5	9	2	8	6
8	7	9	1	6	2	3	4	5
6	5	2	4	3	8	7	9	1
2	1	7	3	4	5	9	6	8
4	8	5	2	9	6	1	3	7
9	3	6	8	7	1	4	5	2
5	9	3	6	2	7	8	1	4
1	2	4	5	8	3	6	7	9
7	6	8	9	1	4	5	2	3

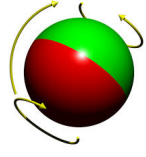
... und die mit Hilfe von Standard-Basen gefundene Lösung.

Andere Aufgaben erfordern das Lösen einer *n-dimensionalen algebraischen Interpolationsaufgabe*: Zu einer gegebenen Menge $\{p_1, \ldots, p_s\}$ im $\mathbb{Q}^n$ bestimme man die Polynome f in $\mathbb{Q}[x_1, \ldots, x_n]$ mit $f(p_i) = a_i$ für vorgebene Werte $a_i \in \mathbb{Q}$, $i = 1, \ldots, s$. Die Differenz zweier Lösungen ist ein Polynom g mit $g(p_i) = 0$, so dass auch hier Standard-Basis-Techniken erfolgreich angewendet werden können. Eine konkrete Industrieanwendung bei der Erdölförderung wird im Artikel von C. Baciu und M. Kreuzer, *Algebraisches Öl*, MDMV 19/2011, 142–147, beschrieben.

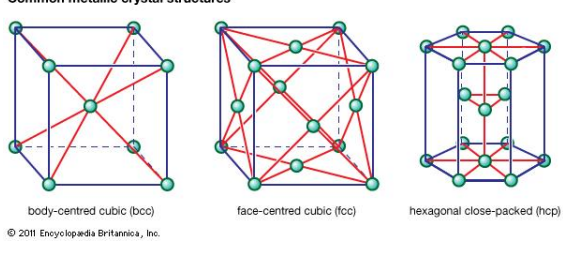
G.A.G.A. B: Gruppentheorie

Gruppentheorie = Studium von Symmetrien

- kontinuierlich $\rightsquigarrow$ Lie-Gruppen



- diskret $\rightsquigarrow$ endliche Gruppen



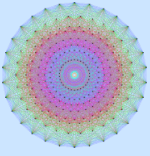
- Symmetrie-„Atome“: endliche **einfache** Gruppen.
- Ein Meilenstein der Mathematik des 20ten Jahrhunderts: **Klassifikation**.
  (angekündigt 1981 • komplett bewiesen 2004 • 12000 Seiten Beweis)
- Beispiele aus dem Grundstudium:
  Alternierende Gruppen $\mathfrak{A}_n$ mit $n \geq 5$, oder lineare Gruppen wie $\mathrm{PSL}_n(K)$.

Neue Beispiele entstehen als Gruppen von Automorphismen „interessanter“ mathematischer Strukturen:

- Vektorräume mit Skalarprodukten
- Lie-Algebren
- Graphen
- Geometrien
- ...

Berühmtes Beispiel: E_8

- Lie-Algebra der Dimension 248 (Cartan–Killing $\sim$ 1890).
- Zugehörige Gruppe G über einem beliebigen Körper K (Chevalley 1955).
  Beispiel: $\quad |K| = 2 \quad \Rightarrow \quad |G| \approx 3,38 \times 10^{74}$.
- Wurzelsystem E_8 mit 240 Vektoren im $\mathbb{R}^8$



- Artikel über E_8 in der New York Times vom 20. März 2007:
  The scientific promise of perfect symmetry