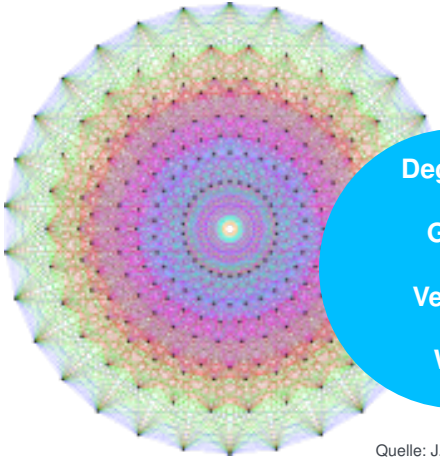
**Universität Stuttgart**
**Institut für diskrete Strukturen & symbolisches Rechnen**



Quelle: J. Stembridge

**Degeratu**
—
**Geck**
—
**Veniani**
—
**Witt**

## G.A.G.A.

Gruppen
Algorithmen
Geometrie
Anwendungen in der Informatik und den Naturwissenschaften

# Dozenten

Anda Degeratu

Meinolf Geck

Davide Veniani

Frederik Witt

# Zielgruppe

Für alle, die

- sich gerne mit abstrakten Strukturen / reiner Mathematik beschäftigen,

  und / oder
- Interesse an algorithmischen Methoden / Entwickeln von Algorithmen und konstruktiven Beweisen / Programmierung (in **Julia**) haben,

  und / oder
- theoretische Grundlagen der Informatik, Physik oder Biologie mit Mathematik verbinden möchten.

# Vorlesungen der Profillinie

- Kernstück der Profillinie sind **G.A.G.A. A & B** (siehe unten). Diese Vorlesungen können unabhängig voneinander belegt werden!
- Ergänzende Vorlesungen: **Algebra** / **Algebra und Zahlentheorie für das Lehramt**, **Geometrie** / **Geometrie für das Lehramt** und **Topologie** sowie ggf. speziellere Vorlesungen wie z.B. **Differentialgeometrie** oder Vorlesungen zur **theoretischen Informatik** oder **Kryptographie** aus dem Fachbereich Informatik.
- Fortgeschrittene Vorlesungen wie z.B. **AKAZie** (Algebraische Kurven und algebraische Zahlentheorie), **Lie-Algebren und Chevalley-Gruppen**
- Fachübergreifende Veranstaltungen wie z.B. **Neural Networks** oder **DAMnIt** (Hauptseminar Diskrete und algebraische Methoden in der Informatik)

# G.A.G.A. A: Kommutative Algebra & 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. $\mathbb{Q}$, $\mathbb{C}$ oder $\mathbb{Z}/p\mathbb{Z}$):

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

Für lineare Gleichungssyteme $i_1 = \ldots = i_n = 1$ berechnet der **Gauß-Algorithmus** ein äquivalentes Gleichungssystem möglichst einfacher Gestalt.

Im nichtlinearen Fall liefert der **Buchberger-Algorithmus**, ein äquivalentes nichtlineares Gleichungssystem, eine sogenannte **Gröbner-Basis**.

**input** : $G = (g_1, \ldots, g_s)$, $g_i \in k[x_1, \ldots, x_n]$
**output:** $S = \mathrm{STD}(G)$ 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
```

**Abbildung:** Schematische Darstellung des Buchberger-Algorithmus

Kommutative Algebra ist die Grundlage für **algebraische Geometrie**. Dort betrachtet man die gemeinsame Nullstellenmenge endlich vieler Polynome. Z.B. definiert die **Weierstrass-Gleichung**

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, \ldots, a_6 \in K,$$

eine sog. **elliptische Kurve**. Diese spielen sowohl in der Theorie (Fermats letzter Satz), als auch in der Anwendung (**ECC – elliptic curve cryptography**) eine zentrale Rolle.

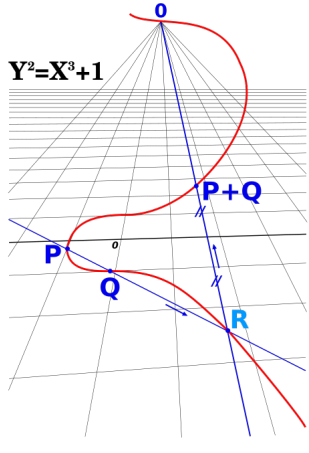
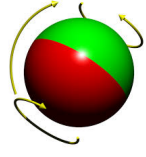



**Abbildung:** Das Gruppengesetz einer **elliptischen Kurve**, hier $y^2 = x^3 + 1$ – Grundlage für die momentan sichersten kryptographischen Verfahren. Siehe Wikipedia „Elliptische Kurve“.

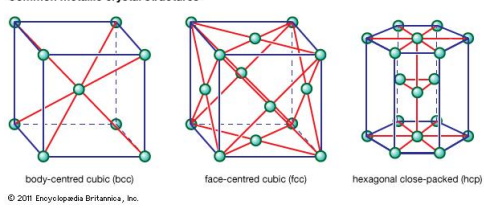
# G.A.G.A. B: Gruppentheorie

## Studium von Symmetrien

- kontinuierlich $\rightsquigarrow$ Lie-Gruppen



- diskret $\rightsquigarrow$ endliche Gruppen



## Klassische Beispiele

- Symmetrie-„Atome“: endliche **einfache** Gruppen. Meilenstein der Mathematik des 20ten Jahrhunderts:

  **Klassifikation dieser Gruppen**

  (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:** $E_8$ (New York Times vom 20. März 2007: The scientific promise of perfect symmetry)

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

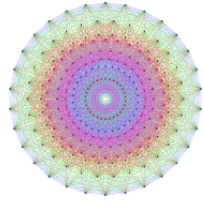


**Abbildung:** Das projezierte Wurzelsystems der E8 in der Coxeter-Ebene

Quelle: J. Stembridge

# Beispiele für fachübergreifende Vorlesungen

- **Geometry of Black Holes:** Wir führen Schwarze Löcher ein und untersuchen ihre Geometrie. Wir beschäftigen uns auch mit Gravitationswellen, wie solche Wellen bei der Kollision zweier Schwarzer Löcher entstehen, wie sie sich im Universum ausbreiten und wie wir sie auf der Erde nachweisen können.

- **Neural Networks:** Wir stellen neurowissenschaftliche Modelle vor, die beschreiben, wie das Gehirn Informationen kodiert und Repräsentationen der Außenwelt erstellt. Wir studieren diese Modelle und versuchen, die mathematischen Ergebnisse aus neurowissenschaftlicher Sicht zu interpretieren.

# Beispiele betreuter Bachelorarbeiten

- Gravitationswellen (Degeratu)
- Zusammenbruch eines Sterns und Entstehung von schwarzen Löchern (Degeratu)
- Gröbner-Basen und Anwendungen (Geck)
- Konstruktion einfacher Lie-Algebren (Geck)
- Mathieu-Gruppen (Veniani)
- Das NTRU-Kryptosystem (Witt)
- Topologische Datenanalyse mit dem Vietoris-Rips-Komplex (Witt)

Siehe auch „betreute Bachelor- und Masterarbeiten“ auf der Startseite des IDSR.

# Beispiele betreuter Masterarbeiten

- Neurale Netzwerke und Quiver-Varietäten (Degeratu)
- Kritische Gehirnhypothese aus einer mathematischen Sicht (Degeratu)
- Die Gesetze der Thermodynamik schwarzer Löcher vom mathematischen Standpunkt (Degeratu)
- Arithmetik elliptischer Kurven über endlichen Körpern (Geck)
- Algorithmen für Chevalleys Theorem (Geck)
- Proteinsequenzen und tropische Geometrie (Witt)
- Neuronale Netze und Gröbnerbasen (Witt)

Siehe auch „betreute Bachelor- und Masterarbeiten“ auf der Startseite des IDSR.