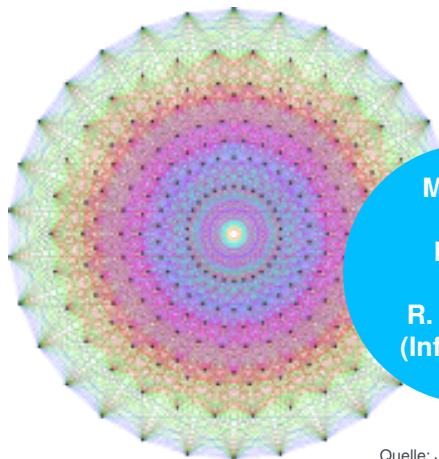




Universität Stuttgart

Institut für diskrete Strukturen & symbolisches Rechnen



M. Geck

—

F. Witt

—

R. Küsters
(Informatik)

Quelle: J. Stembridge

DaMnIt

Diskrete & algebraische
Methoden in der Informatik

Haupt- / Masterseminar
WiSe 24 / 25

- **Voraussetzungen:**
 - gute Algebra-Kenntnisse, insbesondere Körpererweiterungen $\mathbb{Q} \subseteq K$;
 - Interesse an kryptographischen Anwendungen.
- **Themen** werden gemäß Vorkenntnissen individuell angepasst und können ggf. auch mit algorithmischer Komponente (Julia, Sage) versehen werden, z.B.
 - Einführung algebraische Zahlentheorie;
 - ganze algebraische Zahlen, Diskriminante, Kreisteilungsringe;
 - gebrochene Ideale, Dedekindringe, Gitter, kurze Vektoren in Gittern . . .
- **Literatur:**
 - J. Neukirch, „Algebraische Zahlentheorie“, Springer, 1992
 - I.N. Stewart und D.O. Tall, „Algebraic Number Theory“, Chapman and Hall, 1987
- **Anmeldung:** per email an witt@mathematik.uni-stuttgart.de,
Vorbesprechung im September