Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x, y) = ax^2 + bxy + cy^2 \ (a, b, c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

$\mathrm{Disc}(Q) = b^2 - 4ac$. ($\mathrm{SL}_2$-invariant)

Theorem 1 (Gauss) *The set of* $\mathrm{SL}_2(\mathbb{Z})$*-equivalence classes of primitive integral binary quadratic forms of discriminant* D *has a natural group structure.* ($\cong \mathrm{NCl}(S)$)

(This is "Gauss composition")

Orbit problems

Gauss composition may be stated as the solution to an orbit problem:

Theorem 2 $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{Sym}^2(\mathbb{Z}^2) \xleftrightarrow{1\text{–}1} (S, I)$, *where S is a quadratic ring, and I is an ideal class.*

In general we may consider any algebraic group G and any rational representation V. The question then arises:

Question 2: For what pairs (G, V) does

$$G(\mathbb{Z}) \setminus V(\mathbb{Z})$$

parametrize rings, modules, maps, etc.?

Where to look for more such representations?

Key observation:

Over $\mathbb{C}$, the action of GL_2 on the space of binary quadratic forms/$\mathbb{C}$ has just one orbit.

Definition. A pair (G, V) such that G has just one (Zariski open) orbit on V is called a *prehomogeneous vector space*.

Sato and Kimura (1977) gave a classification of all PVS's. (There are 36 of them!)

Wright and Yukie (1990) showed that orbits of PVS's over fields k often correspond to field extensions of k.

Goal: Understand $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ for prehomogeneous vector spaces (G, V).

In modern language, the group described in Theorem 1 is the *narrow class group* of the unique quadratic order of discriminant D.

Two hundred years later, Gauss composition remains one of the best methods for understanding class groups of quadratic fields, and is still the best way of computing them.

However, the method only applies to orders in *quadratic* fields.

Question 1: Do there exist analogous composition laws on other spaces of forms, which could be used to shed light on the structure of higher degree fields?

What about binary cubic forms?

I learned of the following theorem from Wee-Teck Gan in 1999:

Theorem 3 (Delone–Faddeev/Gan–Gross–Savin) *The $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms are in canonical bijection with cubic rings.*

To $ax^3 + bx^2y + cxy^2 + dy^3$, one associates the cubic ring having $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ and multiplication table

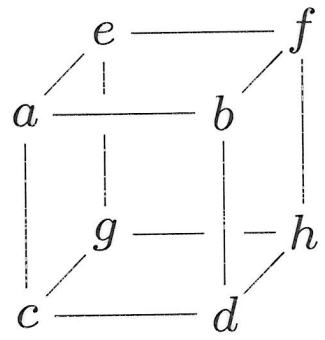
$$\begin{aligned} \omega\theta &= -ad \\ \omega^2 &= -ac + b\omega - a\theta \\ \theta^2 &= -bd + d\omega - c\theta. \end{aligned}$$

Basis-free way to get a binary cubic form from a cubic ring:

Given a cubic ring R, the index form $1 \wedge x \wedge x^2$ is a well-defined cubic form on $R/\mathbb{Z}$.

Gauss's Law Revisited

What would happen if we put numbers on the corners of a cube?



Can slice the cube into pairs of 2×2 matrices in three different ways:

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix}, \quad N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix}, \quad N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}$$

Gauss's Law Revisited (cont'd)

Using these slicings, we can construct three quadratic forms:

$$Q_1(x, y) = -\mathrm{Det}(M_1 x - N_1 y).$$

$$Q_2(x, y) = -\mathrm{Det}(M_2 x - N_2 y).$$

$$Q_3(x, y) = -\mathrm{Det}(M_3 x - N_3 y).$$

The Cube Law. *For any cube A, the sum of Q_1, Q_2, Q_3 is zero.*

(Note the analogy with elliptic curves.)

Theorem 3 *This is Gauss composition!*

Composition of cubes

Theorem 4 (The Cube Law)

$$\mathrm{SL}_2(\mathbb{Z})^3 \backslash (\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2) \overset{1\text{–}1}{\longleftrightarrow} (S, (I_1, I_2, I_3)),$$

where S is a quadratic ring and I_1, I_2, I_3 are ideal classes whose product is the trivial class.

Gauss composition:

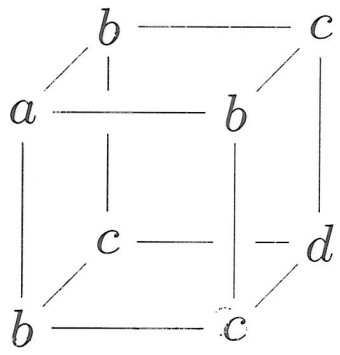
$$(S, I) \circ (S, I') = (S, II').$$

Cube composition:

$$(S, (I_1, I_2, I_3)) \circ (S, (I_1', I_2', I_3')) = (S, (I_1 I_1', I_2 I_2', I_3 I_3')).$$

Composition of binary cubic forms

Impose symmetry:



$$\longleftrightarrow \quad ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

is a triply-symmetric cube.

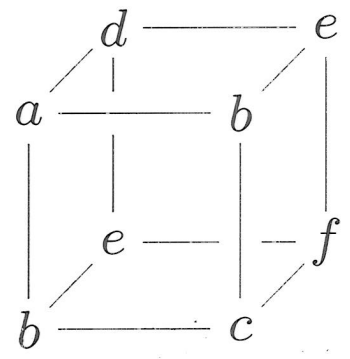
$$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \xrightarrow{\text{sym.}} \mathrm{Sym}^3\mathbb{Z}^2.$$

cube binary cubic form

Theorem 6 $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{Sym}^3(\mathbb{Z}^2) \xleftrightarrow{1\text{–}1} (S, I)$, *where S is a quadratic ring, and I is an ideal class of order* 3. or 1.

Composition of pairs of binary quadratic forms

Impose double symmetry:



$\longleftrightarrow \quad (ax^2+2bxy+cy^2, dx^2+2exy+fy^2)$

is a doubly-symmetric cube.

$$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \xrightarrow{\text{sym.}} \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2.$$

cube pair of b.q.f.'s

Theorem 7 $\mathrm{SL}_2(\mathbb{Z})^2 \backslash \mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^2) \xleftrightarrow{1\text{–}1} (S, I)$, *where S is a quadratic ring, and I is an ideal class.*

The discussions above illustrate that once we have a law of composition on the space of cubes, then various other of its "invariant and covariant spaces" also inherit a law of composition; Gauss composition is indeed just one of these.

Operations

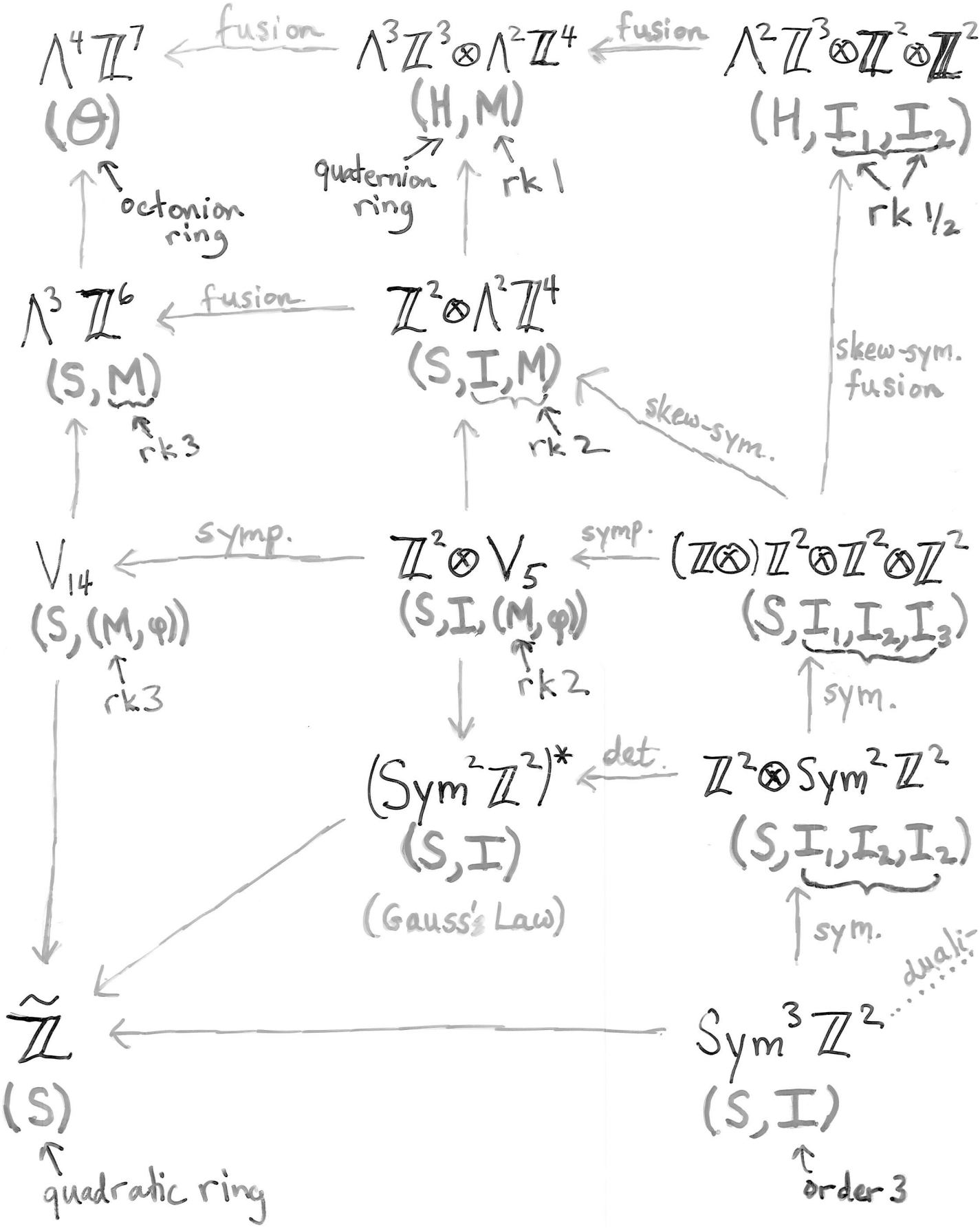
1. symmetrization ("=")

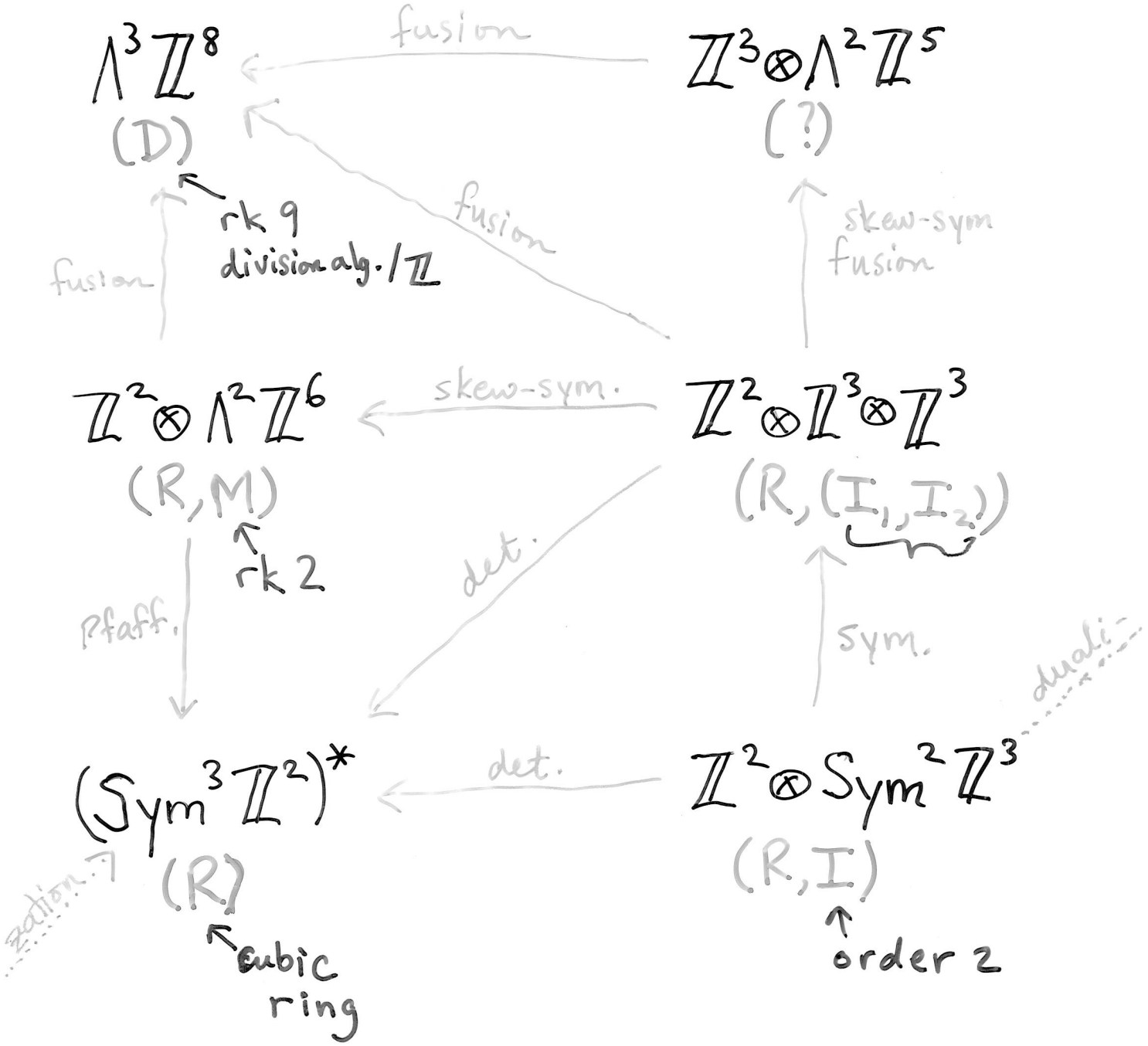
2. skew-symmetrization ("$\oplus$")

3. symplectization ("$\oplus$" + symp. struct.)

4. hermitianization (galois conjugate)

5. dualization (dual under class field theory)


$\Lambda^4\mathbb{I}^7$
(Θ)
fusion
$\Lambda^3\mathbb{I}^3\otimes\Lambda^2\mathbb{I}^4$
(H, M)
fusion
$\Lambda^2\mathbb{I}^3\otimes\mathbb{I}^2\otimes\mathbb{I}^2$
(H, I_1, I_2)
octonion ring
quaternion ring
rk 1
rk 1/2
$\Lambda^3\mathbb{I}^6$
(S, M)
fusion
$\mathbb{I}^2\otimes\Lambda^2\mathbb{I}^4$
(S, I, M)
skew-sym.
skew-sym. fusion
rk 3
rk 2
V_{14}
(S, (M, φ))
symp.
$\mathbb{I}^2\otimes V_5$
(S, I, (M, φ))
symp.
$(\mathbb{I}\otimes)\mathbb{I}^2\otimes\mathbb{I}^2\otimes\mathbb{I}^2$
(S, I_1, I_2, I_3)
rk 3
rk 2
sym.
$(\mathrm{Sym}^2\mathbb{I}^2)^*$
(S, I)
(Gauss's Law)
det.
$\mathbb{I}^2\otimes\mathrm{Sym}^2\mathbb{I}^2$
(S, I_1, I_2, I_2)
sym.
dualize
$\widetilde{\mathbb{I}}$
(S)
quadratic ring
$\mathrm{Sym}^3\mathbb{I}^2$
(S, I)
order 3


$\Lambda^3\mathbb{Z}^8$
(D)
rk 9
division alg./$\mathbb{Z}$
fusion
$\mathbb{Z}^3\otimes\Lambda^2\mathbb{Z}^5$
(?)
skew-sym
fusion
fusion
fusion
$\mathbb{Z}^2\otimes\Lambda^2\mathbb{Z}^6$
(R, M)
rk 2
skew-sym.
$\mathbb{Z}^2\otimes\mathbb{Z}^3\otimes\mathbb{Z}^3$
$(R, (I_1, I_2))$
Pfaff.
det.
sym.
$(\mathrm{Sym}^3\mathbb{Z}^2)^*$
(R)
cubic
ring
det.
$\mathbb{Z}^2\otimes\mathrm{Sym}^2\mathbb{Z}^3$
(R, I)
order 2
duali-
zation

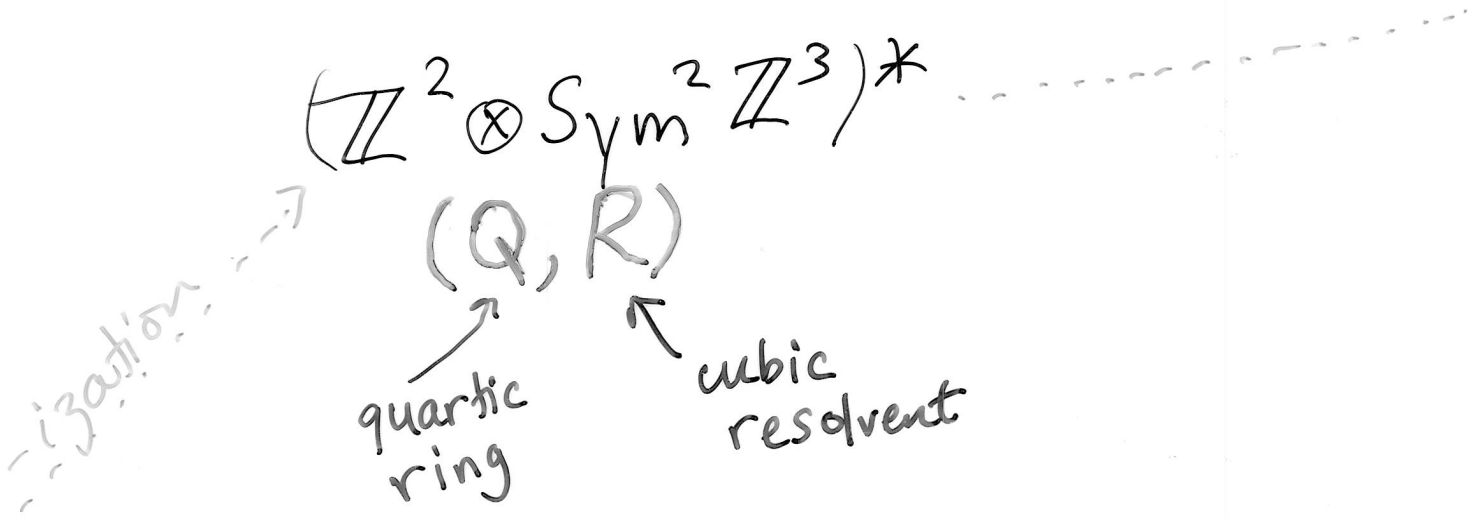
(E_8)

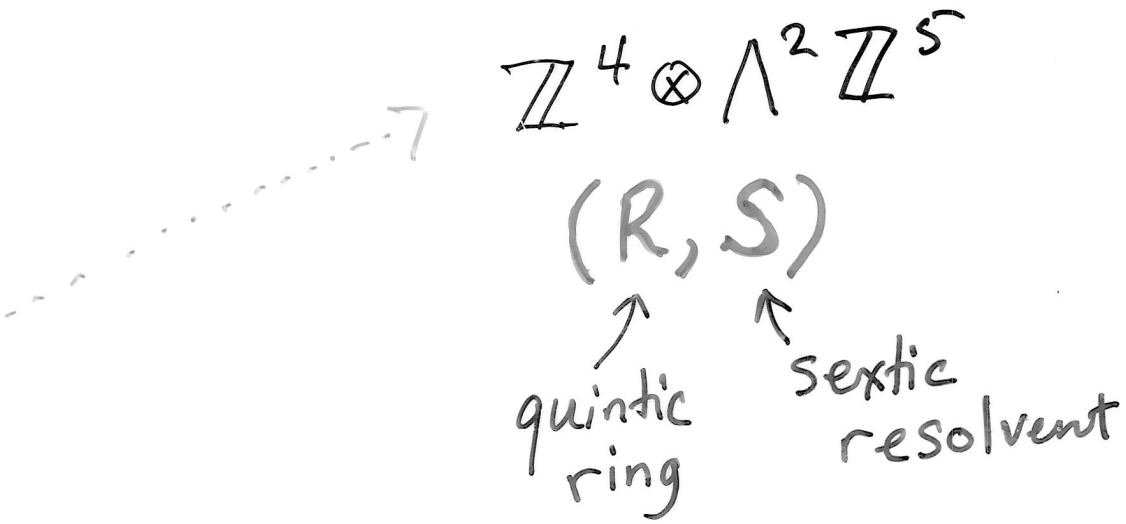
(E_7)

(E_6)

(G_2)

(F_4)


$(\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3)^*$
(Q, R)
quartic ring
cubic resolvent


$\mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$
(R, S)
quintic ring
sextic resolvent

Applications.

1. Computational Applications

Work of Shanks, Belabas, Morra, others...

2. Theory of prehomogeneous vector spaces

Work of Sato, Shintani, Datskovsky, Wright, Yukie, Taniguchi, others...
+Thorne

3. Exceptional groups and modular forms

Work of Gross, Gan-Gross-Savin, Lucianovic, Weissman, Volpato, others...

4. Noncommutative algebras

Work of Elkies, Gross, Lucianovic, Krutelevich, others...

5. Density theorems