A (biased) history of quadratic forms

Our historical account is not chronological.

One can say that modern number theory started with

Disquisitiones Arithmeticae (1798; published 1801)

↳ written by Carl Friedrich Gauss.

The two most important ideas in the book are:

- the theory of quadratic reciprocity. ($\rightsquigarrow$ class field theory).
- composition of binary quadratic forms ($\rightsquigarrow$ class groups).

Our focus this November will be on the theory of forms. Today we talk about quadratic forms, which is a polynomial

$$f(x) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j \quad , \quad a_{ij} \text{ in some base ring } R.$$

One can ask a lot of stuff about quadratic forms, and though we know a lot about it there are still some unsolved problems that are deceivingly simple.

Here is a sample of the questions one can ask.

(1) Solutions of $f(x)$ over $\mathbb{Z}$?

- Universality: When does $f(x)$ admit all integers ?

(see my previous Pizza Seminar talk 2017-04-07)

15-290 Theorem If an integral positive-definite quadratic form represents

1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290,

then it represents all positive integers. One only needs to check up to 15 if classical.

↳ 15-theorem: claimed by John Conway and William Schneeberger circa 1995; proved elegantly by Manjul Bhargava (2000) via his theory of escalations.

↳ 290-theorem: conjectured by John Conway; proved by Manjul Bhargava and Jonathan Hanke (2005; written up 2016).

The question of nonuniversality is hard and not solved in general. Here are some examples.

- Quadratic reciprocity: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.
- Fermat 2-square: x^2+y^2 admits all integers $n = p_1^{e_1} \cdots p_r^{e_r} > 0$ such that if e_i is odd, then $p_i \equiv 1 \pmod 4$.
- Legendre 3-square: $x^2+y^2+z^2$ admits all positive integers not of form $4^a(8b+7)$.
- Fermat 4-square: $x^2+y^2+z^2+w^2$ admits all positive integers.
- Ramanujan's ternary form: Consider $x^2+y^2+10z^2$.
  - ↳ The even numbers not of this form are $4^a(16b+6)$.
  - ↳ [Conjecture!] The odd numbers not of this form are

$$3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719.$$

(2) The number/density of solutions of $f(x)$ over $\mathbb{Z}$?

This is another hard problem, and typically attacked using the theory of automorphic forms (at least in modern times). Here are two elementary examples.

- Let $r(n,k) = \#\{x \in \mathbb{Z}^k : n = x_1^2 + \cdots + x_k^2\}$. Then the generating function for $k \in 2\mathbb{Z}$,

$$\vartheta(\tau,k) := \sum_{n=0}^{\infty} r(n,k)\, q^n, \quad q = e^{2\pi i \tau}, \quad \tau \in \mathbb{H},$$

is a modular form of weight k with respect to $\Gamma_1(4) = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle$, via an application of the Poisson summation formula. Hence by the dimension formulas and that the space of modular forms of weight k can be decomposed into Eisenstein series and cusp forms:

$$\mathcal{M}_k(\Gamma_1(4)) = \mathcal{E}_k(\Gamma_1(4)) \oplus \mathcal{S}_k(\Gamma_1(4))$$

one can try to "compute" $r(n,k)$ using two facts:

- we have an explicitly defined basis for $\mathcal{E}_k(\Gamma_1(4))$
- $\mathcal{S}_k(\Gamma_1(4)) = \{0\}$ for $k = 2, 4, 6, 8$.

Thus for $k = 2, 4, 6, 8$ one can write explicit formulas for $\vartheta(\tau,k)$. For example

$$r(n,4) = 8 \sum_{\substack{0<d\mid n \\ 4\nmid d}} d \qquad , \qquad r(n,2) = 4 \sum_{\substack{0<m\mid n \\ m \text{ odd}}} (-1)^{\frac{m-1}{2}}.$$

For large k the space of cusp forms is not always zero, so explicit formulas are hard to compute. Nevertheless, we can give asymptotes by:

- Hecke's estimate (qualitative): the Fourier coefficients of Eisenstein series dominate those of cusp forms.

- Let $X_n = \{x \in \mathbb{Z}^k : n = x_1^2 + \cdots + x_k^2\}$. Then, for $8 \mid k$, the set X_n is equidistributed on the k-sphere of radius $\sqrt{n}$, in the following sense:

  For $F \in C^\infty(S^k)$, $\lim_{n\to\infty} \frac{1}{r(n,k)} \sum_{x \in X_n} F\left(\frac{x}{|x|}\right) = \int_{S^k} F$.

  The argument for this is via a version of Weyl's Equidistribution Criterion, and a generalization of Hecke's estimate.

(3) Searching for solutions of $f(x)$ over number fields?

For this there are two general methods commonly used.

- Hensel's Lemma: Let R be a DVR complete on $\mathrm{Frac}(R) = K$ with respect to its valuation. Suppose $g(x) \in R[x]$ is a monic polynomial such that it admits a root over $R/\mathfrak{m}$ which is simple. Then there is a unique lifting of this root to R.

  ↳ Used to find solutions for the quadratic forms in (1). In particular, x^2 admits all solutions of the form $4^a(8b+1)$ in $\mathbb{Z}_2$.

- Hasse Local-Global Principle (1): Let K be a number field and f a nondegenerate quadratic form which represents 0 in K_v over all primes v of K. Then f represents 0 in K.

- Hasse Local-Global Principle (2): Let f be a classical integral quadratic form in n-variables, which is unique in its genus and $d := \det M_f \neq 0$. Suppose $\alpha \in \mathbb{Z} \setminus \{0\}$ is an integer represented by f over $\mathbb{R}$, and (primitively) represented by f over $\mathbb{Z}_p$ for all p. (In fact, it suffices to do it for $p \mid 2d$ if $n \geq 3$, and $p \mid 2\alpha d$ if $n = 2$.) Then α is (primitively) represented by f over $\mathbb{Z}$.

  ↳ Main tool in proving the 15-290 theorems, together with Hensel's Lemma.

(4) Other stuff one can do?

I will be extremely brief here as each topic is a separate ~~lecture~~ course by itself.

- Generalization to class field theory and Langlands program ($\subset$ FLT, modularity; $\leftarrow$ BSD; $\leftarrow$ Abelian/Shimura varieties...)

- Studying fields via looking at the types of quadratic forms with a nontrivial zero over it, for example Serge Lang's thesis (1952).

  ↳ Topic for next week's Pizza Seminar!

- Applications to other areas of math like knot theory.

  ↳ See Quadratic Forms and Their Applications, 1999, Dublin, for examples.

We now stop with our introduction and focus on one topic for the remainder of this talk, which is ...

Composition Laws and the Bhargava Cube

We will focus on the quadratic case, giving some comments on the higher order cases after that. The starting point for this topic is the following identity:

Brahmagupta's identity: $(x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2) = x_3^2 + Dy_3^2$,

where $x_3 = x_1x_2 + Dy_1y_2$ and $y_3 = x_1y_2 - y_1x_2$.

Gauss generalized this to a composition law on binary quadratic forms

$$(a_1x_1^2 + b_1x_1y_1 + c_1y_1^2)(a_2x_2^2 + b_2x_2y_2 + c_2y_2^2) = a_3x_3^2 + b_3x_3y_3 + c_3y_3^2$$

with x_3, y_3 bilinear functions of x_1, x_2 and y_1, y_2 with integer coefficients.

Goal: Reinterprete this as some group (i.e. modern language), then study Bhargava's further reinterpretation of this.

We now do the classical case of this, which is essentially done by Gauss.

Classically: quadratic extensions

It is well-known that quadratic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\sqrt{D})$ for a squarefree integer D, so the probability that one picks such a D among the positive integers is

$$\prod_p \left(1-\frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Also if D is squarefree then the ring of integers of $K=\mathbb{Q}[\sqrt{D}]$ is

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right].$$

The (ideal) class group is defined to be

$$Cl(K) := \frac{\mathbb{Z}\{\text{fractional ideals}\}}{\mathbb{Z}\{\text{principal ideals}\}}$$

which measures how far K is from being a PID, among other things. What we are interested in is actually the narrow class group, defined to be

$$Cl^+(K) := \frac{\mathbb{Z}\{\text{fractional ideals}\}}{\mathbb{Z}\{\text{totally positive principal ideals}\}}.$$

In this quadratic case it is trivial to see that

- $Cl^+(K) = Cl(K)$ if $D<0$,
- $\#Cl^+(K) = 2\#Cl(K)$ if $D>0$.

Given a binary quadratic form $ax^2+bxy+cy^2$, its discriminant is b^2-4ac. Another thing Gauss essentially did is to give a group structure on $SL_2(\mathbb{Z})$-equivalence classes of nondegenerate binary quadratic forms. In modern language, it is the following statement

Thm: There is a canonical bijection

$$\left\{\begin{array}{l}\text{equivalence classes of nondegenerate}\\ \text{binary integral quadratic forms}\\ \text{of discriminant } D\end{array}\right\} \longleftrightarrow Cl^+\left(\mathcal{O}(\sqrt{D})\right).$$

Explicitly the bijection is given as follow.

($\Rightarrow$) Given $ax^2+bxy+cy^2$, construct

$$I = \left(a, \frac{b-\sqrt{D}}{2}\right)\alpha$$

where α is anything with $\operatorname{sgn}(N(\alpha)) = \operatorname{sgn}(a)$.

($\Leftarrow$) Given $I \subset \mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$, choose an ordered $\mathbb{Z}$-basis α, β for I such that

$$\frac{\beta\sigma(\alpha)-\alpha\sigma(\beta)}{\sqrt{D}} > 0 \quad \text{(orientation condition)}$$

Then construct $f(x,y) = \dfrac{N(\alpha x+\beta y)}{\det\left(\begin{array}{c}\text{change of basis from}\\ 1, \sqrt{D} \text{ to } \alpha,\beta\end{array}\right)}$, which is still an integral form (basically use fact that we can replace I with something of the form $\mathbb{Z}a \oplus \mathbb{Z}\left(b+\frac{D+\sqrt{D}}{2}\right)$ with same class as I in $Cl^+(\mathcal{O}_{\mathbb{Q}[\sqrt{D}]})$.).

Example. For $I=(2, 1+\sqrt{5})$ in $\mathbb{Z}[\sqrt{-5}]$, an (oriented) basis is $2, 1+\sqrt{-5}$.

So $$f(x,y) = \frac{(2x+y+\sqrt{5}y)(2x+y-\sqrt{5}y)}{\det\begin{bmatrix}2 & 1\\ 0 & 1\end{bmatrix}} = 2x^2+2xy+3y^2.$$

We can rewrite the theorem in this page by

$$\left\{\begin{array}{l}\text{equivalence classes of nondegenerate}\\ \text{binary integral quadratic forms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{pairs } (S, I) \text{ with}\\ S \text{ a quadratic extension of}\\ \mathbb{Q}, \text{ and } I \in Cl^+(S)\end{array}\right\}.$$

and furthermore the correspondence preserves discriminants.

Idea of Bhargava Find a "good" generalization of Gauss composition that looks like any big conjecture in number theory, i.e.

$$\left(\begin{array}{c}\text{some algebraic}\\ \text{group}\end{array}\right)\backslash\left(\begin{array}{c}\text{some space}\\ \text{of forms}\end{array}\right) \longleftrightarrow \left(\begin{array}{c}\text{some classes of ideals in}\\ \text{rings}\end{array}\right)$$

"geometric" "algebraic".

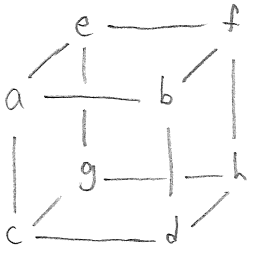
Remark: Actually what we are talking about is a good model for a prehomogeneous vector space. By the classification of Sato and Kimura, together with some general philosophy in this subject, a classification of this sort only exists for number fields $K/\mathbb{Q}$ of degree at most 5, and Bhargava does this.

We now look at the following object, which may seem irrelevant for now.

The Bhargava cube

This is a visual representation of the elements of $\mathcal{C}_2 := \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$.

Explicitly it is as follow:

$A =$ 

$$\longleftrightarrow \begin{aligned} &a\,v_1\otimes v_1\otimes v_1 + b\,v_1\otimes v_2\otimes v_1\\ &+ c\,v_2\otimes v_1\otimes v_1 + d\,v_2\otimes v_2\otimes v_1\\ &+ e\,v_1\otimes v_1\otimes v_2 + f\,v_1\otimes v_2\otimes v_2\\ &+ g\,v_2\otimes v_1\otimes v_2 + h\,v_2\otimes v_2\otimes v_2 \end{aligned}.$$

Given such a cube, we can slice it in three ways to obtain pairs of matrices, and then let $SL_2(\mathbb{Z})$ acts on those pairs. Explicitly, we have:

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix} \quad M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix}$$

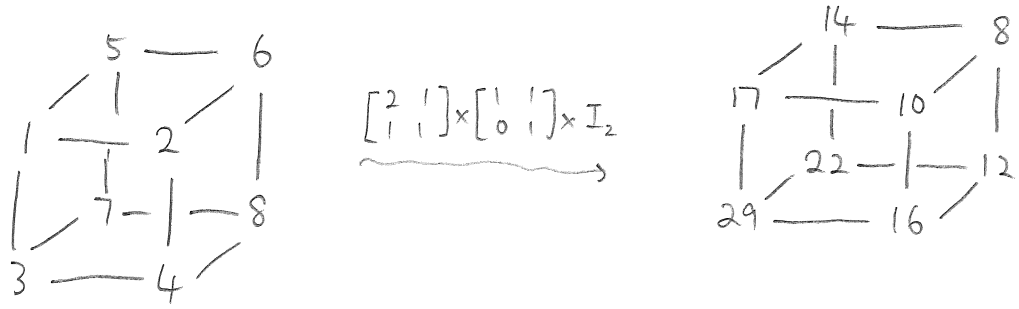
$$N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \quad N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix} \quad N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}$$

and $SL_2(\mathbb{Z})$ acts on (M_i, N_i) by

$$\begin{bmatrix} r & s \\ t & u \end{bmatrix} \cdot (M_i, N_i) = (rM_i + sN_i,\ tM_i + uN_i).$$

By letting $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$, this induces an action on the Bhargava cube, and is a commuting action on the factors.

Example: If we do a computation,



Given a Bhargava cube A as above, we can construct three binary quadratic forms given by

$$Q_i^A(x,y) := -\det(M_i x - N_i y) \qquad (1 \le i \le 3).$$

Notice $\operatorname{disc}(Q_1^A)$ is invariant under $SL_2(\mathbb{Z})$-action, so does Q_2^A and Q_3^A. Also Q_1^A is invariant under $\{1\} \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ as this only acts by row and column operations on M_1 and N_1. A "quick" calculation says $\operatorname{disc}(Q_i^A)$ are all equal, and in fact equals

$$\begin{aligned} \operatorname{disc}(A) := {} & a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ & -2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh). \end{aligned}$$

Thus one has shown that the Γ-action on A preserves its discriminant, since it preserves $\operatorname{disc}(Q_i^A)$ for all $1 \le i \le 3$.

Generalized Gauss Composition

We now seek to reinterpret, and generalize, the theorem in page (7), using the Bhargava cube. To do this we would like a group law just like in the case of elliptic curves, which we call

The Cube Law | The sum $Q_1^A + Q_2^A + Q_3^A$ is Q_{id}, for some choice of identity Q_{id}.

More formally, the Cube Law is the abelian group

$$\text{Free}\left\{\begin{array}{l}\text{primitive binary integral quadratic}\\ \text{forms of discriminant } D\end{array}\right\} \Big/ \; Q_1^A + Q_2^A + Q_3^A = Q_{id}.$$

Easy Consequence: Forms that are $SL_2(\mathbb{Z})$-equivalent are automatically identified.

↳ $(Q_1^A, Q_2^A, Q_3^A) \xrightarrow{(\gamma, id, id)} (Q_1^{A,\prime}, Q_2^A, Q_3^A)$, so $Q_1^A \sim Q_1^{A,\prime} = \gamma \cdot Q_1^A$.

Let us write $[Q]$ to mean the $SL_2(\mathbb{Z})$-equivalence class of Q.

Thm 1: Let $D \equiv 0, 1 \pmod 4$, and let Q_{id} be any primitive binary (integral) quadratic form of discriminant D such that there is a cube A_0 with

$$Q_i^{A_0} = Q_{id} \quad \text{for all } 1 \le i \le 3.$$

Then there is a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence class of primitive binary quadratic forms of discriminant D such that:

(a) $[Q_{id}]$ is the additive identity,

(b) $[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{id}]$ for any cube A.

Conversely, given $[Q_1] + [Q_2] + [Q_3] = [Q_{id}]$, there is a cube A of discriminant D, unique up to equivalence, such that $Q_i^A = Q_i$, $1 \le i \le 3$.

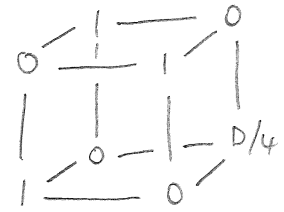
How is it related to Gauss composition?

Let us choose Q_{id} to be the following.

$D \equiv 0 \pmod 4$

$$Q_{id} = x^2 - \frac{D}{4} y^2$$

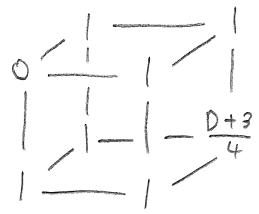
$A =$



$D \equiv 1 \pmod 4$

$$Q_{id} = x^2 - xy + \frac{1-D}{4} y^2$$

$A =$

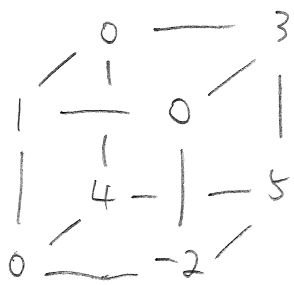


(Stickelberger's criterion forces $D \equiv 0, 1 \pmod 4$).

We demonstrate an example of composition here in case $D \equiv 1 \pmod 4$

Example: Consider the cube below with associated Q_1, Q_2, Q_3.

$A:$



$$Q_1 = -\det\left(\begin{bmatrix} 1 & 0 \\ 0 & -2 \end{bmatrix} x + \begin{bmatrix} 0 & 3 \\ 4 & 5 \end{bmatrix} y\right) = 2x^2 - 5xy + 12y^2$$

$$Q_2 = -\det\left(\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} x + \begin{bmatrix} 0 & 3 \\ -2 & 5 \end{bmatrix} y\right) = -4x^2 - 5xy - 6y^2$$

$$Q_3 = -\det\left(\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} x + \begin{bmatrix} 0 & 4 \\ -2 & 5 \end{bmatrix} y\right) = -3x^2 - 5xy - 8y^2.$$

Here $\operatorname{disc}(A) = -71 \equiv 1 \pmod 4$. Notice that

$$[Q_1] + [Q_2] = [-3X^2 + 5XY - 8Y^2], \quad \begin{aligned} X &= -2x_1x_2 + 4y_1x_2 + y_1y_2 \\ Y &= x_1x_2 + 3y_1y_2 \end{aligned}$$

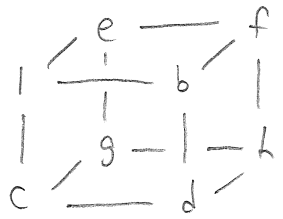
$$[Q_3] + [-3x^2 + 5xy - 8y^2] = [X^2 - XY + 18Y^2], \quad \begin{aligned} X &= 3x_1x_2 - 8y_1y_2 - 2x_1y_2 + 3x_2y_1 \\ Y &= x_1y_2 + x_2y_1 \end{aligned}$$

Therefore $[Q_1] + [Q_2] + [Q_3] = [Q_{id}]$, as expected.

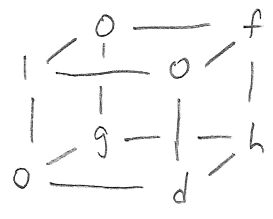
In fact, we show our choice of Q_{id} is Gauss composition via Dirichlet's Formulation ⟹

Let A be a projective cube, i.e. all Q_i^A are primitive. Then, under the Γ-action, as the greatest common divisor of the vertices is 1,

$$A \overset{\Gamma}{\sim}$$



$$\overset{\Gamma}{\sim}$$



.

The quadratic forms associated to the last cube is

$$Q_1 = -dx^2 + hxy + fg\,y^2$$

$$Q_2 = -gx^2 + hxy + df\,y^2$$

$$Q_3 = -fx^2 + hxy + dg\,y^2 .$$

Note that, under Q_{id} as above

- if $D \equiv 0 \pmod 4$,

$$[ax^2+bxy+cy^2] + [cx^2+bxy+ay^2] = X^2 - \frac{D}{4}y^2, \quad X = \frac{b}{2}x_1x_2 + \frac{b}{2}y_1y_2 + ax_1y_2 + cx_2y_1, \quad Y = x_1x_2 - y_1y_2$$

- if $D \equiv 1 \pmod 4$,

$$[ax^2+bxy+cy^2] + [cx^2+bxy+ay^2] \xrightarrow{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}} = [ax^2+bxy+cy^2] + [ax^2-bxy+cy^2] = X^2 - XY + \frac{1-D}{4}Y^2,$$

$$X = ax_1x_2 - cy_1y_2 + \frac{1-b}{2}x_1y_2 + \frac{1+b}{2}x_2y_1, \quad Y = x_1y_2 + x_2y_1 .$$

In both cases one gets

$$[-dx^2+hxy+fgy^2] + [-gx^2+hxy+dfy^2] = [dgx^2+hxy-fy^2]$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad \|$$

$$[Q_1] + [Q_2] \qquad\qquad -[Q_3] ,$$

which is Dirichlet's interpretation of Gauss composition.

Upshot: Thm 1 generalizes Gauss composition!!

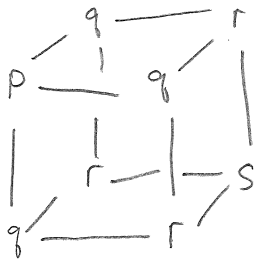
Before sketching the proof of theorem 1, let us give some more composition laws that it implies. Refer to Bhargava's papers for the full list.

- Composition of $2\times2\times2$ cubes: Let $D\equiv 0,1 \pmod 4$. Then there exists a unique group law on the set of Γ-equivalence classes of projective cubes of discriminant D such that
  - $[A_{ijk}]$ is the additive identity,
  - For $i=1,2,3$, the maps $[A] \longmapsto [\mathcal{O}_i^A]$ yield group homomorphisms to $Cl((Sym^2\mathbb{Z}^2)^*; D)$, defined as the set of $SL_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D with the group structure defined by the Cube Law.

This group is denoted $Cl(\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2; D)$

- Composition of binary cubic forms:

An integral binary cubic form $C=px^3+3qx^2y+3rxy^2+y^3$ can be associated the following cube:



If $Sym^3\mathbb{Z}^2$ is the space of such cubic forms, we have defined an inclusion $\iota: Sym^3\mathbb{Z}^2 \hookrightarrow \mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2$. Such a cubic form is projective if the associated cube is projective. Observe that the three forms associated to it is the Hessian

$$H(x,y) = Q_i^{(C)} = -\frac{1}{36}\begin{vmatrix} C_{xx} & C_{xy} \\ C_{yx} & C_{yy}\end{vmatrix} = (q^2-pr)x^2+(ps-qr)xy+(r^2-qs)y^2.$$

Hence one sees that C is projective iff $\gcd(q^2-pr,\ ps-qr,\ r^2-qs)=1$.

Also a trivial computation tells us that the preimage of the identity cubes in Gauss composition corresponds to the cubic forms

$$D\equiv 0 \pmod 4 \qquad\qquad D\equiv 1 \pmod 4$$

$$C_{id} = 3x^2y + \frac{D}{4}y^3, \qquad C_{id} = 3x^2y + 3xy^2 + \frac{D+3}{4}y^3.$$

Hence Theorem 1 implies: There is a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence classes of projective binary cubic forms C of discriminant D such that:

- $[C_{id}]$ is the additive identity,
- $[C] \mapsto [\iota(C)]$ is a group homomorphism to $Cl(\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2; D)$.

This group is denoted $Cl(\mathrm{Sym}^3\mathbb{Z}^2; D)$.

Proof sketch of Thm 1

Let S be the quadratic ring of discriminant $D\equiv 0,1 \pmod 4$, and $K = S\otimes_{\mathbb{Z}}\mathbb{Q}$ the quadratic field of S. Say (I_1, I_2, I_3) a triple of oriented ideals is balanced if $I_1 I_2 I_3 \subset S$ and $N(I_1)N(I_2)N(I_3)=1$. Two balanced triples are equivalent if $I_j = K_j I_j'$ for some $K_j \in K$, $1\le j\le 3$. The main result to prove theorem 1 is the following, which is a more elaborate version of the result in page (7).

Thm: There is a discriminant-preserving bijection

$$\left\{\begin{array}{c}\text{nondegenerate } \Gamma\text{-orbits}\\ \text{on the space } \mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2\\ \text{of integer cubes}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{isomorphism classes of pairs } (S, \overbrace{(I_1, I_2, I_3)}^{I}),\\ S = \text{nondegenerate quadratic ring}\\ I = \text{equivalence class of balanced ideals}\end{array}\right\}.$$

We do not describe the correspondence here, but we note that it descends to an isomorphism

$$Cl(\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2 : D) \;\cong\; Cl^+(S(D)) \times Cl^+(S(D))$$

after noting that equivalence classes of projective balanced ideals are isomorphic to $Cl^+(S(D)) \times Cl^+(S(D))$ by the projection $(I_1, I_2, I_3) \mapsto (I_1, I_2)$. Then to prove theorem 1 one simply computes the norms associated to I_1, I_2, I_3.

Interesting observation: The number of orbits of projective cubes of a fixed discriminant is a square number.

Higher order cases: A comment

Theorems analogous to Thm 1 exists for cubic, quartic, and quintic extensions, but of course the cube with Γ-action does not suffice. For instance, in the cubic case we need a $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z}) =: \Gamma'$ action on $\mathbb{Z}^2\otimes\mathbb{Z}^3\otimes\mathbb{Z}^3$, and over there the bijection looks like:

$$\left\{ \begin{array}{l} \text{nondegenerate } \Gamma'\text{-orbits} \\ \text{on } \mathbb{Z}^2\otimes\mathbb{Z}^3\otimes\mathbb{Z}^3 \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{isomorphism classes of pairs } (R, (I, I')): \\ R = \text{nondegenerate cubic ring} \\ (I, I') = \text{equivalence class of balanced ideals} \end{array} \right\}$$

See more details in, say, Bhargava's ICM (2006) talk.

By using methods of Davenport (analytic) and above, one can try to compute the density of fields of low order having a fixed absolute discriminant. In the cases of degrees 1 and 2 it is trivial. For degrees 3, 4, 5, ...

Thm: The number of ① fields having absolute value of discriminant X is asymptotic to ② as $X \to \infty$ ...

①	②
cubic	$\frac{1}{3\,\zeta(3)}$
quartic	$\frac{5\,\zeta(2)^2\,\zeta(3)}{24\,\zeta(5)}$

There is also a formula for quintics. Since I am not familiar with the ideas for this theorem (perhaps a future Pizza Seminar talk) I will stop here.

References

(1) Manjul Bhargava, "Higher Composition Laws".

(2) Manjul Bhargava, "ICM Talk 2006".

(3) Manjul Bhargava, "On the Conway-Schneeberger Fifteen Theorem".

(4) Manjul Bhargava and Jonathan Hanke, "Universal Quadratic Forms and the 290 Theorem".

(5) Henri Cohen, "A Course in Computational Number Theory".

(6) Fred Diamond and Jerry Shurman, "A First Course in Modular Forms".

---

(7) Me, Pizza Seminar Notes 2017-04-07.