Origins and applications of higher composition laws

Alberto Cámara

STNB, January 29th, 2015

1801: Gauss' *Disquisitiones*

Let $D \equiv 0, 1 \pmod 4$ be negative.

Theorem (Reduction algorithm)

Every positive definite primitive binary quadratic form is $\mathrm{SL}_2(\mathbf{Z})$*-equivalent to a unique form* $ax^2 + bxy + cy^2$ *with*

$$|b| \leq a \leq c, \qquad \text{and } b \geq 0 \text{ whenever } b = a \text{ or } a = c.$$

This gives a fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on the space of (integral) binary quadratic forms (cf. fundamental domain for the action of the modular group on the upper half plane).

Corollary

The number of $\mathrm{SL}_2(\mathbf{Z})$*-classes of positive definite primitive binary quadratic forms of discriminant* D *is finite.*

Question: if n and m are two integers represented by binary quadratic forms f and g, is the product nm represented by a binary quadratic form?

This leads naturally to Gauss composition: if the answer is yes and nm is represented by h, then there are two integral bilinear forms α, β such that

$$f(x,y)g(z,w) = h\left(\alpha\left(x,y,z,w\right), \beta\left(x,y,z,w\right)\right);$$

h is said to be *composed of f and g*.

Theorem (Gauss)

Composition induces a group law on the set of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of primitive positive definite binary quadratic forms of discriminant D.

(Note: the notion of group and group action were introduced later on)

Later the same century: Dedekind (?)

Let $\mathcal{O}$ be the (imaginary) quadratic order of discriminant D.

Theorem

There is an isomorphism between the group of classes of primitive positive definite binary quadratic forms and the ideal class group of $\mathcal{O}$.

One can define such an isomorphism by:

$$ax^2 + bxy + cy^2 \longmapsto \left[a, \frac{-b+\sqrt{D}}{2}\right]_{\mathbf{Z}} \subset \mathcal{O}.$$

This proves the finiteness of class numbers of quadratic orders.

Gauss composition can be used to make computations with ideal classes of quadratic orders very explicit (cf. *NUCOMP* algorithm).

2001: Bhargava's Odissey

Where would one go and look for generalizations of Gauss composition?

We have: $G \circlearrowright V$.

$G = \mathrm{SL}_2$, V the space of forms.

First idea: look for pairs (G, V), defined over $\mathbf{Z}$ and parametrizing *interesting* objects.

Notice:

The action of $\mathrm{GL}_2(\mathbf{C})$ on the space of binary quadratic forms over $\mathbf{C}$ *essentially* has one orbit: any two forms with nonzero discriminant can be mapped to one another by a transformation in $\mathrm{GL}_2(\mathbf{C})$.

In other words, over $\mathbf{C}$ there is only one pair (S, I) with S a nondegenerate quadratic ring and I an oriented ideal class of S: $S = I = \mathbf{C} \oplus \mathbf{C}$.

Prehomogeneous vector spaces

Definition

A prehomogeneous vector space is a pair (G, V) where G is an algebraic group and V a rational vector space representation of F such that $G(\mathbf{C}) \circlearrowright V(\mathbf{C})$ has a Zariski-dense orbit.

Composition laws describing orders and ideals in number fields must come from $G(\mathbf{Z}) \circlearrowright V(\mathbf{Z})$, for prehomogeneous spaces defined over $\mathbf{Z}$.

Sato–Kimura, 1977: classification of complex reduced, irreducible prehomogeneous spaces in 36 types.

Wright–Yukie, 1992: over a field K, K-orbits of prehomogeneous spaces *often* correspond to field extensions of K.

V	G	Parametrizes
$D \equiv 0, 1 \pmod 4$	$\mathrm{SL}_1(\mathbf{Z})$	Quadratic rings
$(\mathrm{Sym}^2\mathbf{Z}^2)^*$	$\mathrm{SL}_2(\mathbf{Z})$	Ideal classes in quadratic rings
$\mathrm{Sym}^3\mathbf{Z}^2$	$\mathrm{SL}_2(\mathbf{Z})$	Order three ideal classes in quad. rgs.
$\mathbf{Z}^2 \otimes \mathrm{Sym}^2\mathbf{Z}^2$	$\mathrm{SL}_2(\mathbf{Z})^2$	Ideal classes in quadratic rings
$\mathbf{Z}^2 \otimes \mathbf{Z}^2 \otimes \mathbf{Z}^2$	$\mathrm{SL}_2(\mathbf{Z})^3$	Pairs of ideal classes in quadratic rgs.
$\mathbf{Z}^2 \otimes \wedge^2\mathbf{Z}^4$	$\mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_4(\mathbf{Z})$	Ideal classes in quadratic rings
$\wedge^3\mathbf{Z}^6$	$\mathrm{SL}_6(\mathbf{Z})$	Quadratic rings
$(\mathrm{Sym}^3\mathbf{Z}^2)^*$	$\mathrm{GL}_2(\mathbf{Z})$	Cubic rings
$\mathbf{Z}^2 \otimes \mathrm{Sym}^2\mathbf{Z}^3$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z})$	Order two ideal classes in cubic rings
$\mathbf{Z}^2 \otimes \mathbf{Z}^3 \otimes \mathbf{Z}^3$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z})^2$	Ideal classes in cubic rings
$\mathbf{Z}^2 \otimes \wedge^2\mathbf{Z}^6$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_6(\mathbf{Z})$	Cubic rings
$(\mathbf{Z}^2 \otimes \mathrm{Sym}^2\mathbf{Z}^3)^*$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z})$	Quartic rings
$\mathbf{Z}^4 \otimes \wedge^2\mathbf{Z}^5$	$\mathrm{GL}_4(\mathbf{Z}) \times \mathrm{SL}_5(\mathbf{Z})$	Quintic rings

Composition laws and exceptional Lie groups

Let G be a Lie group, P a maximal parabolic subgroup of G. We write $P = LU$ where L is the Levi factor and U is the unipotent radical at P.

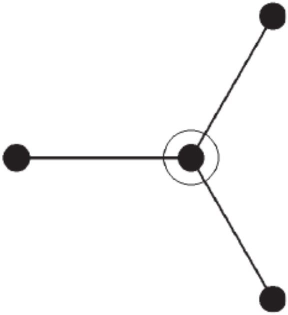
Fact: L acts on $W = U/[U,U]$ by conjugation.
Rubenthaler, Vinberg: pairs (L, W) can be completely classified as prehomogeneous spaces.

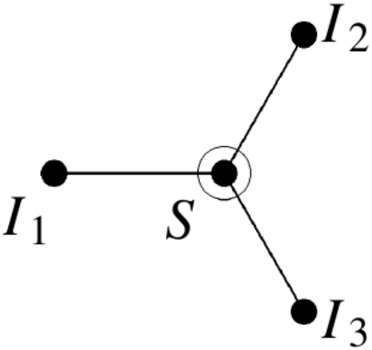
For certain choices of G and P, the group L and space W correspond to the pairs considered in the table.

Example

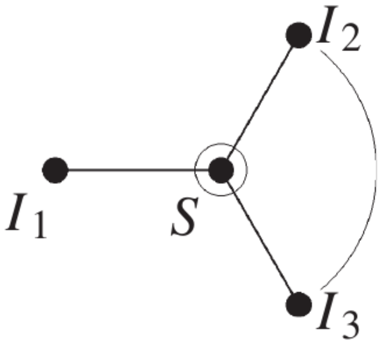
If G is the exceptional Lie group of type D_4 and P corresponds to the central vertex of the associated Dynkin diagram, then $L = \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$ and W is the space of cubes.

$L = \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$
Acts on: (S, I_1, I_2, I_3), S quadratic.
Type: D_4.

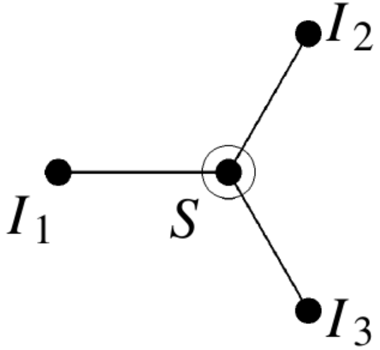


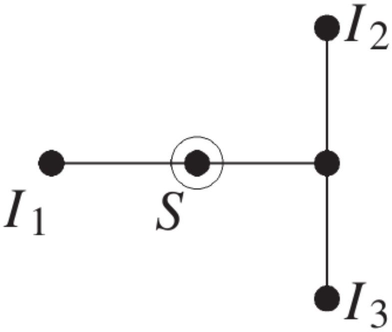


Identify $I_2 = I_3$.
$L = \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$
Acts on: (S, I_1, I_2), S quadratic.
Type: B_3

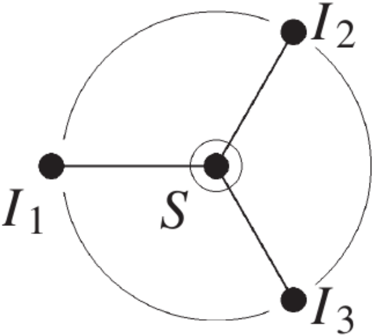


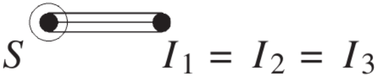
Now instead we fuse I_2 and I_3 by direct sum.
$G = \mathrm{SL}_2 \times \mathrm{SL}_4$
$V = \mathbf{Z}^2 \otimes \wedge^2 \mathbf{Z}^4$
Type: D_5.



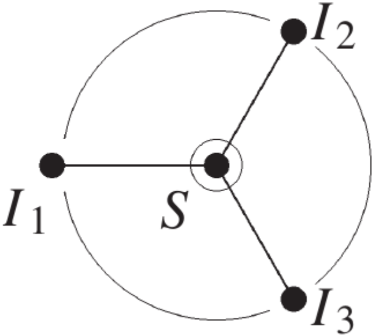


Now identify $I_1 = I_2 = I_3$, so that $I_1^3 \sim S$.
$G = \mathrm{SL}_2$
$V = \mathrm{Sym}^3 \mathbf{Z}^2$
Type: G_2.

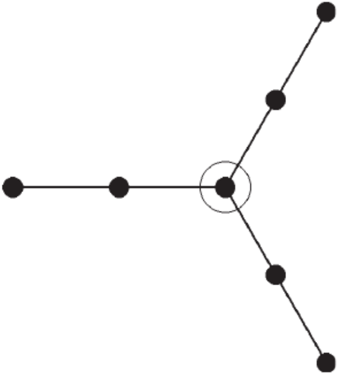




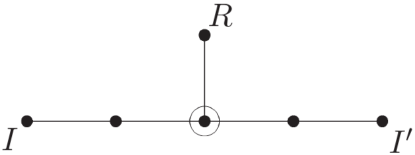
Fuse all three ideals by direct sum.
$G = \mathrm{SL}_6$
$V = \wedge^3 \mathbf{Z}^6$
Type: E_6.



What about the cubic case? Why is there no relevant composition law for 3x3x3 cubes of integers? Because it would take a Dynkin diagram of the form:

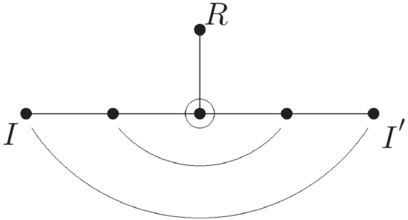


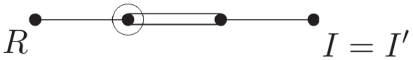
Instead, let's cut one of the legs short and consider 2x3x3 cubes of integers:



R a cubic ring, I, I' a couple of (balanced ideals).
$\Gamma = \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3$.
$V = \mathbf{Z}^2 \otimes \mathbf{Z}^3 \otimes \mathbf{Z}^3$.
Type: E_6.

Now identify $I = I'$, which implies in particular $I^2 \sim R$.





R a cubic ring, I, I' a couple of (balanced ideals).
$\Gamma = \mathrm{GL}_2 \times \mathrm{GL}_3$.
$V = \mathbf{Z}^2 \otimes \mathrm{Sym}^2\mathbf{Z}^3$.
Type: F_4.

V	G	Type
$D \equiv 0, 1 \pmod 4$	$\mathrm{SL}_1(\mathbf{Z})$	A_1
$(\mathrm{Sym}^2 \mathbf{Z}^2)^*$	$\mathrm{SL}_2(\mathbf{Z})$	B_2
$\mathrm{Sym}^3 \mathbf{Z}^2$	$\mathrm{SL}_2(\mathbf{Z})$	G_2
$\mathbf{Z}^2 \otimes \mathrm{Sym}^2 \mathbf{Z}^2$	$\mathrm{SL}_2(\mathbf{Z})^2$	B_3
$\mathbf{Z}^2 \otimes \mathbf{Z}^2 \otimes \mathbf{Z}^2$	$\mathrm{SL}_2(\mathbf{Z})^3$	D_4
$\mathbf{Z}^2 \otimes \wedge^2 \mathbf{Z}^4$	$\mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_4(\mathbf{Z})$	D_5
$\wedge^3 \mathbf{Z}^6$	$\mathrm{SL}_6(\mathbf{Z})$	E_6
$(\mathrm{Sym}^3 \mathbf{Z}^2)^*$	$\mathrm{GL}_2(\mathbf{Z})$	G_2
$\mathbf{Z}^2 \otimes \mathrm{Sym}^2 \mathbf{Z}^3$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z})$	F_4
$\mathbf{Z}^2 \otimes \mathbf{Z}^3 \otimes \mathbf{Z}^3$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z})^2$	E_6
$\mathbf{Z}^2 \otimes \wedge^2 \mathbf{Z}^6$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_6(\mathbf{Z})$	E_7
$(\mathbf{Z}^2 \otimes \mathrm{Sym}^2 \mathbf{Z}^3)^*$	$\mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z})$	F_4
$\mathbf{Z}^4 \otimes \wedge^2 \mathbf{Z}^5$	$\mathrm{GL}_4(\mathbf{Z}) \times \mathrm{SL}_5(\mathbf{Z})$	E_8

Density of discriminants

Let R be a ring admitting a **Z**-basis $\{\alpha_1, \dots, \alpha_n\}$.

Definition

$\mathrm{Disc}(R) = \det\left(\mathrm{Tr}(\alpha_i \alpha_j)\right)_{1 \le i,j \le n}$.

For a number field K, $\mathrm{Disc}(K) = \mathrm{Disc}(\mathcal{O}_K)$.

Theorem (Minkowski)

For number fields, up to isomorphism, $\#\{K;\ \mathrm{Disc}(K) = D\} < \infty$.

We set $N_n(x) = \#\{K;\ \mathrm{Gal}(K^g|\mathbf{Q}) = \mathfrak{S}_n,\ \mathrm{Disc}(K) \le x\}$.

Conjecture

The limit

$$c_n = \lim_{x \to +\infty} \frac{N_n(x)}{x}$$

exists and is positive for all $n \ge 2$.

Example

$c_1 = 0,\ c_2 = 6/\pi^2 = 1/\zeta(2).$

For c_2: we need to count integers up to x which are 0 or 1 $\pmod 4$ and squarefree.

Davenport–Heilbronn, 1971: $c_3 = 1/3\zeta(3)$
(via **Delone–Faddeev, 1964**).

Bhargava, 2005 and **2010**: values of c_4 and c_5.

$n = 3$. Davenport–Heilbronn

Cubic orders are parametrized by $\mathrm{GL}_2(\mathbf{Z})\backslash(\mathrm{Sym}^3\mathbf{Z}^2)^*$, that is: $\mathrm{GL}_2(\mathbf{Z})$-equivalence classes of binary cubic forms.
They form a lattice in the 4-dimensional $\mathbf{R}$-vector space

$$V = (\mathrm{Sym}^3\mathbf{R}^2)^* = \left\{ax^3 + bx^2y + cxy^2 + dy^3;\ a, b, c, d \in \mathbf{R}\right\}.$$

Davenport–Heilbronn: explicitly construct a fundamental domain $\mathcal{F}$ for $\mathrm{GL}_2(\mathbf{Z}) \circlearrowright V$.

The number of cubic orders having discriminant at most x is the number of integer points in the region

$$\mathcal{F}_x = \mathcal{F} \cap \{v \in V;\ |\mathrm{Disc}(v)| \le x\}$$

Toy example

For counting SL_2-classes of positive definite primitive binary quadratic forms of discriminant at most x, we would take
$V = \left\{ax^2 + bxy + cy^2;\ a, b, c \in \mathbf{R}\right\}$, $\Gamma = \mathrm{SL}_2(\mathbf{Z})$,

$$\mathcal{F} = \{|b| < a < c\} \cup \{0 < b < a = c\} \cup \{0 < b = a < c\}$$

$$\mathcal{F}_x = \mathcal{F} \cap \left\{|b^2 - 4ac| \leq x\right\}$$

The number of integral points in a region $\mathcal{R}$ in Euclidean space can be approximated correctly by its volume provided:

1. $\mathcal{R}$ is compact.
2. $\mathcal{R}$ is *round-looking* (smooth boundaries and no serious *spikes* or *tentacles*).

Fact: $\mathrm{vol}(\mathcal{F}_x) = \pi^2/18$.

Problem: $\mathcal{F}_x$ has a tentacle going to infinity, arising from non-compactness of $\mathrm{SL}_2(\mathbf{Z})\backslash\mathrm{SL}_2(\mathbf{R})$.

Davenport–Heilbronn: most points in the tentacle correspond to reducible binary cubic forms (ie: a binary quadratic form times a linear form). The number of integral points in the tentacle corresponding to irreducible forms is $O(x)$.
Similarly, the contrary happens in the *smooth* part of $\mathcal{F}_x$.

Theorem

$$\#\{\ \textit{cubic orders } R;\ \mathrm{Disc}(R) \leq x\} \sim \frac{\pi^2}{18}x, \quad (x \to \infty).$$

Are we done?

NO: passing from cubic orders to maximal cubic orders requires a rather delicate sieve.

Theorem

$$\#\{K;\ [K:\mathbf{Q}] = 3, \mathrm{Disc}(K) \leq x\} \sim \frac{1}{3\zeta(3)}x, \quad (x \to \infty).$$

$n = 4$. Bhargava

Same ideas with much more difficult computations and subtler obstacles. We have V, G, $\mathcal{F}$, $\mathcal{F}_x$ as above, but now:

$$V = (\mathbf{R}^2 \otimes \mathrm{Sym}^3 \mathbf{R}^2)^*, \quad G = \mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z}).$$

Now $\dim_{\mathbf{R}} V = 12$. Bhargava constructs $\mathcal{F}$ and computes:

$$\mathrm{vol}(\mathcal{F}_x) = \frac{5}{24}\zeta(2)^2\zeta(3)x.$$

Problem: $\mathcal{F}_x$ has three big *cusps*.

1st cusp: reducible points corresponding to $Q = S_1 \oplus S_2$, S_i quadratic.
2nd cusp: $Q = R \oplus L$, R cubic and L linear.
3rd cusp: irreducible points corresponding to D_4-quartic fields.

Theorem

Let $\Xi(x)$ be the set of isomorphism classes of pairs (Q, R), where Q is an $\mathfrak{S}_4$-quartic order of discriminant at most x and R is a cubic resolvent of Q. Then:

$$\#\Xi(x) \sim \frac{5}{24}\zeta(2)^2\zeta(3)x, \quad (x \to \infty)$$

We need to drop the R in order to count only isomorphism classes of Q.

Theorem

Let $\Theta(x)$ be the set of isomorphism classes of $\mathfrak{S}_4$-quartic orders with discriminant at most x.

$$\#\Theta(x) \sim \frac{5}{24}\frac{\zeta(2)^2\zeta(3)}{\zeta(5)}x, \quad (x \to \infty).$$

Going from orders to maximal orders requires again a sieve (**hard!**).

Theorem

$$c_4 = \frac{5}{24} \prod_p (1 + p^{-2} - p^{-3} - p^{-4}).$$

Corollary

When ordered by size of discriminant, quartic fields are:

- 90.644%: *of $\mathfrak{S}_4$-type.*
- *The rest: of D_4-type.*
- 0%: *other Galois groups.*

(By Hilbert irreducibility, if we order degree n polynomials by size of coefficients, 100% *are of S_4-type).*

$n = 5$. Bhargava

$$V = \mathbf{R}^4 \otimes \wedge^2 \mathbf{R}^5, \quad G = \mathrm{GL}_4(\mathbf{Z}) \times \mathrm{SL}_5(\mathbf{Z}).$$

Now $\dim_{\mathbf{R}}(V) = 40$.
Bhargava constructs $\mathcal{F}$ and computes the volume of $\mathcal{F}_x$.

Problem: $\mathcal{F}_x$ is highly non-compact.

- There are 160 cusps. They contain points that can be discarded (reducible, other Galois types).
- 100% of integral points corresponding to orders in $\mathfrak{S}_5$-quintic fields are away from the cusps.

Theorem

$$c_5 = \frac{13}{120} \prod_p \left(1 + p^{-2} - p^{-4} - p^{-5}\right).$$

Getting started

Carl Friedrich Gauss.
Disquisicions aritmètiques.
Institut d'Estudis Catalans, Barcelona, 1996.
Traducció i pròleg de Griselda Pascual Xufré.

Manjul Bhargava.
Higher composition laws and applications.
In *International Congress of Mathematicians. Vol. II*, pages 271–294. Eur. Math. Soc., Zürich, 2006.

Manjul Bhargava.
Gauss composition and generalizations.
In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 1–8. Springer, Berlin, 2002.

The corpus of Bhargava's thesis

Manjul Bhargava.
Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations.
Ann. of Math. (2), 159(1):217–250, 2004.

Manjul Bhargava.
Higher composition laws. II. On cubic analogues of Gauss composition.
Ann. of Math. (2), 159(2):865–886, 2004.

Manjul Bhargava.
Higher composition laws. III. The parametrization of quartic rings.
Ann. of Math. (2), 159(3):1329–1360, 2004.

Manjul Bhargava.
Higher composition laws. IV. The parametrization of quintic rings.
Ann. of Math. (2), 167(1):53–94, 2008.

Curiosities

In the ICM 2006 survey, Bhargava announces an upcoming paper, of which I have not found a trace:

Manjul Bhargava.
Higher composition laws. V. The parametrization of quaternionic and octonionic rings and modules.

On parametrizing orders:

Manjul Bhargava.
On the classification of rings of "small" rank.
Notes for Arizona Winter School. Available at http://swc.math.arizona.edu/aws/2009/09BhargavaNotes.pdf, 2009.

On prehomogeneous vector spaces

M. Sato and T. Kimura.
A classification of irreducible prehomogeneous vector spaces and their relative invariants.
Nagoya Math. J., 65:1–155, 1977.

Mikio Sato and Takuro Shintani.
On zeta functions associated with prehomogeneous vector spaces.
Ann. of Math. (2), 100:131–170, 1974.

David J. Wright and Akihiko Yukie.
Prehomogeneous vector spaces and field extensions.
Invent. Math., 110(2):283–314, 1992.

On cubic fields

B. N. Delone and D. K. Faddeev.
The theory of irrationalities of the third degree.
Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

H. Davenport and H. Heilbronn.
On the density of discriminants of cubic fields.
Bull. London Math. Soc., 1:345–348, 1969.

H. Davenport and H. Heilbronn.
On the density of discriminants of cubic fields. II.
Proc. Roy. Soc. London Ser. A, 322(1551):405–420, 1971.

Quartic and quintic densities

Manjul Bhargava.
The density of discriminants of quartic rings and fields.
Ann. of Math. (2), 162(2):1031–1063, 2005.

Manjul Bhargava.
The density of discriminants of quintic rings and fields.
Ann. of Math. (2), 172(3):1559–1591, 2010.

Computing in quadratic and cubic fields via composition laws

Daniel Shanks.
On Gauss and composition. I, II.
In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 163–178, 179–204. Kluwer Acad. Publ., Dordrecht, 1989.

K. Belabas.
A fast algorithm to compute cubic fields.
Math. Comp., 66(219):1213–1237, 1997.

Thanks