ON THE PARAMETRIZATION OF RINGS OF LOW RANK

JIM STANKEWICZ

I'm speaking today about a topic that should be of interest to everyone here: Dissertations. In particular I'd like to go over a couple of points on what I'd call, "The Dissertation we'd all love to write." I refer to the 2001 Princeton thesis "Higher Compostion Laws" by Manjul Bhargava. I'd say we'd all love to have written it, not necessarily because everyone here knows or loves Gauss Composition but rather because of the impact this thesis.

After he graduated in 2001, this thesis was turned into a series of 4 papers in the Annals, each covering a different bit of his thesis that he wrote while on visiting positions at Princeton, Harvard and the Clay Math Institute and in July 2003 he became a full professor at Princeton, most substantially on the work coming from his thesis(though it would be a blatant lie to say that's all that put him in that position).

The aspect of his thesis that we examine today is the parametrization of rings of low rank over $\mathbf{Z}$(i.e. primarily dealing with the work the latter two annals papers). We give the following conventions for ease:

- By a *ring* we will mean an associative, commutative ring with unit.
- By a *ring of low rank* over a ring R we will mean a ring which is a free module over R(we may switch this to locally free later when we move away from Principal ideal Domains, but until and unless we finish with $\mathbf{Z}$ this is good enough) of "low rank" and in the case $R = \mathbf{Z}$ we'll mean up to 5 or so.
- By parametrize, we will mean finding a set of "complete invariants" for a ring of low rank, that is, a set of objects associated to a ring of low rank which are invariant under R-module isomorphism and that if two rings are not isomorphic, they have differing invariants.

1. A few trivial cases

1.1. **Rank zero.** Can anyone think of a free $\mathbf{Z}$-module of rank zero?

1.2. **Rank one.** If a $\mathbf{Z}$-module M is free of rank one, it is isomorphic to $x\mathbf{Z}$ for some $x \in M$. If M is a ring, then $1 \in M$, so there exists some $n \in \mathbf{Z}$ such that $xn = 1$ thus n is a unit in this ring and thus in $\mathbf{Z}$ so $n = \pm 1$. Thus up to isomorphism $M = \mathbf{Z}$.

We call these trivial cases because in fact the rank is a complete invariant here!

2. Nontrivial cases

In general, if we have a ring R of rank n, $R = x_0\mathbf{Z} \oplus \cdots \oplus x_{n-1}\mathbf{Z}$. Since $1 \in R$ there exist $m_0, \ldots, m_{n-1}$ such that $\sum m_i x_i = 1$. Then consider the exact sequence of $\mathbf{Z}$-modules

$$0 \to \mathbf{Z}\sum m_i x_i \to R \to R/(\mathbf{Z}\sum m_i x_i) \to 0$$

Date: April 26, 2010.

By the additivity of rank in exact sequences, the rank of $R/\mathbf{Z}$ is $n-1$ so there exist $x_1, \dots x_{n-1}$ such that $\langle 1, x_1, \dots x_{n-1}\rangle$ is a basis for R over $\mathbf{Z}$.

Moreover, we can determine everything about R as a ring from the pairwise multiplications $x_i x_j = c^0_{i,j} + \sum_{k=1}^{n-1} c^k_{i,j} x_k$.

Therefore we can familiarly write R as $\mathbf{Z}[x_1, \dots, x_{n-1}]/\left(x_i x_j - c^0_{i,j} - \sum_k c^k_{i,j} x_k\right)$. To obtain information about isomorphism classes and thus complete invariants, we have to pare down a little further than these structure constants.

2.1. **Rank 2 and the Discriminant.** The first nontrivial case is rank 2. As above, we have a basis $\langle 1, \tau\rangle$ and the ring will then be completely determined by the constants b, c where $\tau^2 = b\tau + c$. Any $\mathbf{Z}$ isomorphism of $\mathbf{Z}[\tau]$ moves τ to $\pm\tau - r$ where $r \in \mathbf{Z}$. Notice that τ satisfies the polynomial $X^2 - bX - c$ which has discriminant $b^2 + 4c$. We can however shift τ so that this polynomial is "minimal" in some way.

Take $b = 2r + \delta$ where δ is 0 or 1. Then

$$(\tau - r)^2 = \tau^2 - 2r\tau + r^2 = (2r+\delta)\tau + c - 2r\tau + r^2 = \delta\tau + (r^2 + c) = \delta(\tau - r) + (\delta r + c + r^2)$$

Note that $b^2 + 4c = 4r^2 + 4r\delta + \delta^2 + 4c = 4(r^2 + r\delta + c) + \delta^2$ so the discriminant of τ is invariant under shifting. Thus to every ring of rank 2 over $\mathbf{Z}$ we associate an integer which is 0 or 1 mod 4. Further to any integer which is zero or one mod 4 (say $D = \delta + 4c$) we can associate to it a ring of rank 2 over $\mathbf{Z}$ (say $\mathbf{Z}[x]/(x^2 - \delta x - c)$) which is unique up to isomorphism. Thus the discriminant is a complete invariant for rings of rank two over $\mathbf{Z}$.

This particular bijection has been known in some form for hundreds of years.

The next breakthrough was in 1964 by Delone and Faddeev who parametrized orders in cubic number fields. This was extended in 2001 to all cubic rings by Wee Teck Gan, Benedict Gross and Gordan Savin (Fourier Coefficients of Modular Forms on G_2).

All else was fleshed out in Bhargava's work.

3. Rank 3

To parametrize rings of higher rank, we consider that the discriminant can be recognized in terms of the trace pairing bilinear form. Consider the trace map $T : R \to \mathbf{Z}$ where we consider multiplication by α as an $n \times n$ integer matrix m_α. Then $T(\alpha) = tr(m_\alpha)$ and $(\alpha, \beta) \to T(\alpha\beta)$ is a bilinear form on R. Then if $\langle x_1, \dots, x_n\rangle$ is a basis for R, the discriminant $\det(T(x_i x_j))$ is an isomorphism invariant because it can be expressed via a matrix which is is unique up to GL_n's action.

Borrowing a convention from Delone and Faddeev we let R be a ring of rank 3 over $\mathbf{Z}$ with basis $\langle 1, \omega, \theta\rangle$. As a first strike, consider that by definition

$$\omega\theta = n + d\omega + e\theta.$$

Thus

$$(\omega - e)(\theta - d) = \omega\theta - d\omega - e\theta + de = n + de,$$

So up to translation by an integer(isomorphism) we can consider $R = \mathbf{Z}[\omega, \theta]$ such that $\omega\theta = n \in \mathbf{Z}$(the example we'd like to make natural is that of a ring of integers like $\mathbf{Z}[\zeta_3]$ or $\mathbf{Z}[\sqrt{n}]$). Then we consider the structure constants

$$\begin{aligned}\omega\theta &= n\\ \omega^2 &= m + b\omega - a\theta\\ \theta^2 &= l + d\omega - c\theta\end{aligned}$$

These are not independent equations however.

Take for example the associative relation $\omega(\theta^2) = (\omega\theta)\theta = n\theta$. Since $\omega(\theta^2) = \omega(l + d\omega - c\theta) = l\omega + dm + db\omega - da\theta - cn = (dm - cn) + (l + db)\omega - da\theta$ we have $n = -da$, $l = -db$ and since $n = -da$, $dm = cn = -cda$ we have $m = -ca$.

There are further relations, but they are tied up as follows: To the ring with a particular basis we associate the quadruple of integers a, b, c, d which give a general homogeneous binary cubic form

$$p(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Of note here is that the discriminant of this cubic form ($\prod_{i<j}(x_i - x_j)^2$ where $(x_i, 1)$ are projective solutions to $p(x, y) = 0$) is the same as the discriminant of R.

To get a well-defined map from a ring, and not just a choice of basis, we mod out by the action of GL_2 on the space of binary cubic forms

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} p(x, y) = \frac{p(Ax + Cy, Bx + Dy)}{AD - BC}.$$

Note This is exactly analogous to the action of $SL_2(\mathbf{Z})$ or $GL_2(\mathbf{Z})$ on binary quadratic forms in the theory of Gauss Composition, where $AD - BC = 1$ always.

For completeness, we include the theorem of gauss composition.

Theorem 1 (Gauss Composition)**.** *There is a canonical bijection between $GL_2(\mathbf{Z})$ equivalence classes of binary quadratic forms and pairs (R, I) of quadratic rings R and ideal classes $I \subset Pic(R)$ ($SL_2(\mathbf{Z})$ is somewhat more natural and induces a sort of orientation on the quadratic rings).*

Then if we have an isomorphism $S \to R$, a good basis of S is moved to a good basis of R, say $\langle 1, \alpha, \beta\rangle$ where

$$\begin{pmatrix} 1 & 0 & 0 \\ u & A & B \\ v & C & D \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \theta \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix}$$

where

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_2$$

and u, v depend on A, B, C, D.

We can then express this as the following:

Theorem 2 (Delone-Faddeev-Gan-Gross-Savin)**.** *Isomorphism classes of rings of rank 3 over $\mathbf{Z}$ are in bijection with $GL_2(\mathbf{Z})$ equivalence classes of binary cubic forms over $\mathbf{Z}$.*

Of course none of what I've mentioned so far is Bhargava's work. What Bhargava argues is that hidden in this classification is the discriminant of the ring, which is preserved via this bijection and gives a unique quadratic "resolvent ring". A theorem in this setting would look like the following:

Theorem 3. *Isomorphism classes of pairs of Cubic Rings over* $\mathbf{Z}$ *and their Quadratic Resolvents are in bijection with* $GL_2(\mathbf{Z})$ *equivalence classes of binary cubic forms.*

We make this distinction because it shows the direction we have to take for quartic rings.

3.1. **Rank 4.** What is special about quartic rings is that given a ring of rank 4 over $\mathbf{Z}$, there does not in general exist a unique cubic resolvent. We can however show that there exist cubic resolvents of any quartic ring.

The bridge between the two takes the form of a pair of ternary quadratic forms. Let

$$\begin{aligned} A(x_1,x_2,x_3) &= \sum_{i,j} a_{i,j}x_ix_j \\ B(x_1,x_2,x_3) &= \sum_{i,j} b_{i,j}x_ix_j \end{aligned}$$

These quadratic forms give constants

$$\lambda_{k,\ell}^{i,j} = \begin{vmatrix} a_{i,j} & b_{i,j} \\ a_{k,\ell} & b_{k,\ell} \end{vmatrix}, C_1 = \lambda_{1,1}^{2,3}, C_2 = -\lambda_{2,2}^{1,3}, C_3 = \lambda_{3,3}^{1,2},$$

Which then give structure constants for a quartic ring. Indeed let $\sigma(1,2,3) = (i,j,k)$, then set

$$\begin{aligned} c_{i,i}^{i} &= \mathrm{sgn}(\sigma)\lambda_{i,j}^{i,k} + C_i \\ c_{i,i}^{j} &= \mathrm{sgn}(\sigma)\lambda_{i,k}^{i,i} \\ c_{i,j}^{i} &= \mathrm{sgn}(\sigma)\frac{1}{2}\lambda_{j,j}^{i,k} + \frac{1}{2}C_j \\ c_{i,j}^{k} &= \mathrm{sgn}(\sigma)\lambda_{i,i}^{j,j} \end{aligned}$$

and by a similar associative law construction to degree 3 we must have

$$c_{i,j}^{0} = \sum_{r=1}^{3} \left(c_{j,k}^{r} c_{r,i}^{k} - c_{i,j}^{r} c_{r,k}^{k} \right)$$

: I haven't checked these calculations myself. Somehow the world will have to subsist on Dr. Bhargava's word on this point.

Now given a quadratic form, we can associate a matrix, e.g. to the A given above we can associate the symmetric matrix $(a_{i,j})$. Now given indeterminates x, y we may associate to a pair of integral ternary quadratic forms A, B a matrix $(xa_{i,j} - yb_{i,j})$ and the determinant of this matrix will be an integral binary cubic form. As we know from the above, this cubic form gives a cubic ring and we call any cubic ring which arises in this way from a quartic ring a cubic resolvent.

IOU one example

There are of course many different pairs of quadratic forms which will give the same quartic ring. For instance, we have an analogous action of $GL_3(\mathbf{Z})$ on either quadratic form which gives the same quartic ring. Moreover, excepting the "internal action" of GL_3, if (A,B) are a given pair of quadratic forms giving the quartic ring Q, then $(aA + cB, bA + dB)$ also gives Q if $ad - bc = \pm 1$. Thus our pair only matters up to the action of $GL_3(\mathbf{Z}) \times GL_2(\mathbf{Z})$. Our parametrization result is that this association is a bijection.

Theorem 4. *There is a canonical bijection between $GL_3(\mathbf{Z}) \times GL_2(\mathbf{Z})$ equivalence classes of pairs of ternary quadratic forms (A, B) with isomorphism classes of pairs of quartic rings and resolvent cubics (Q, R).*

Now that we know there is a bijection, a natural question arises: how many of these isomorphism classes get attached to the same quartic ring? That is, how many cubic resolvents does a quartic ring have?

Theorem 5. *The number of cubic resolvents of a quartic ring Q is $\sum_{d|ct(Q)} d$ where*

$$ct(Q) = \sup(m)/\{Q' : Q = \mathbf{Z} + mQ'\}$$

If we wish to parametrize just quartic rings, we need to identify pairs of pairs (A, B) which give the same quartic ring but not necessarily the same cubic resolvent. In fact, this is how we push the association a bit further, for instance if every coefficient of A is divisible by n, then $(\frac{1}{n}A, nB)$ will even give the same quartic ring if not the same cubic resolvent.

Theorem 6. *Let $GL_2^{\pm 1}(\mathbf{Q})$ denote the subgroup of $GL_2(\mathbf{Q})$ with determinant ± 1. Then there is a canonical bijection between quartic rings Q and $GL_3(\mathbf{Z}) \times GL_2^{\pm 1}(\mathbf{Q})$ equivalence classes of integral ternary quadratic forms.*

3.2. **Rank 5.** One may note that the parametrization of quartic rings bears some similarity to the solution of of the quartic equation, i.e. it runs through a cubic resolvent. It is well known that there is no solution by radicals to a quintic equation. There is however a notion of a resolvent sextic of a quintic polynomial. Namely if $\alpha_1, \ldots, \alpha_5$ are the roots of a quintic polynomial, the sextic resolvent polynomial is the minimal polynomial for

$$\frac{(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1) - (\alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_5 + \alpha_4\alpha_1 + \alpha_5\alpha_2)}{\prod_{i,j}(\alpha_i - \alpha_j)}.$$

While not so useful for solving an equation by radicals, the sextic resolvent has long been used in the study of quintic equations and finds use here. Indeed most of these correspondences were found in part by first considering the case of orders in number fields.

It is finally here where we bring the genesis of these classifications into focus. Here for instance we have natural coordinate-free maps from one ring R over $\mathbf{Z}$ to another say S, so as modules, we can make a map $R/\mathbf{Z} \to S/\mathbf{Z}$ and the set of maps $Hom(R/\mathbf{Z}, S/\mathbf{Z})$ is in natural bijection with $R/\mathbf{Z}^\vee \otimes S/\mathbf{Z}$ or some approximation thereof.

It turns out that the classical resolvent is not the most natural map from a quintic ring to a sextic ring, but in fact a degree 2 covariant thereof. If R is a quintic ring and S a sextic resolvent, the most natural map is a degree 1 map $R \to \wedge^2 S$.

Thus the bridge we build between R and S comes in the form of elements of $\mathbf{Z}^4 \otimes \wedge^2\mathbf{Z}^5$, or quadruples of quinary alternating 2-forms. Contrast this to the case of cubic rings and quadratic resolvents, where the natural map is degree 3, so we have $Sym^3(\mathbf{Z}^2) \otimes \mathbf{Z} = Sym^3(\mathbf{Z}^2)$, or a binary cubic form. Further consider our last case, where the map to the cubic resolvent is degree 2, so we get $Sym^2(\mathbf{Z}^3) \otimes \mathbf{Z}^2$ or pairs of ternary quadratic forms.

Without saying too much more(i.e. something I don't understand that well) we have the following result:

Theorem 7. *There is a canonical bijection between $GL_5(\mathbf{Z}) \times GL_4(\mathbf{Z})$ orbits of $\wedge^2\mathbf{Z}^5 \otimes \mathbf{Z}^4$ and isomorphism classes of pairs (R, S) of quintic rings with sextic resolvents.*

3.3. **Higher ranks, Moduli spaces, Representation Theory and the genesis of the problem.** Can we get a similar type of parametrization for higher ranks?

Furthermore, where did this business of modding out by various GL_n's and SL_n's come from?

The genesis of this is in the Gan-Gross-Savin paper (the one about G_2). Each of the parametrizations I've mentioned (and others I haven't mentioned) come from reductive representations of exceptional Lie Groups.

Take for example the cubic case. Here the exceptional Lie group is G_2. What G-G-S did was to decompose a maximal parabolic subgroup of G_2 into its unipotent radical and the corresponding Levi factor $L\dot{U}$. Here the Levi factor is GL_2 and it acts naturally by conjugation on the abelianization of U, which in this case is $Sym^3(*^2)$.

Quartic rings come from a certain parabolic subgroup of F_4, and quintic rings come from a certain parabolic subgroup of E_8.

There are indeed many other such parametrizations for even more exotic things, like quaternion and octonion rings which come from representations of exceptional lie groups, but as far as a similar parametrization for commutative rings of higher rank over $\mathbf{Z}$? As Bhargava said, "We've run out of exceptional Lie Groups."

This doesn't mean that there's no hope of parameterizing rings of higher rank, just that there's more than one type of parametrization.

For example, one parameterizing object which comes up frequently in algebraic geometry is that of a moduli space. In this case the object that parametrizes the objects (usually geometric objects) that we'd like to keep track of is itself a scheme. These are very useful as we can apply all the machinery of algebraic geometry to them but they are also somewhat limited because you need to eliminate automorphisms from the objects you parametrize.

One tack taken here is the one by Bjorn Poonen, who uses the concept of the structure constants to rigidify the problem. Instead of considering a ring just as a ring, he considers the concept of a "based algebra" where permutations of the generators $\alpha_1, \ldots, \alpha_{n-1}$ are not considered isomorphisms. From there the moduli space of based algebras of rank n lives in affine space of dimension $n\binom{n}{2}$ (given by the $c_{i,j}^k$'s) with relations

$$c_{i,j}^0 = \sum_{r=1}^{n-1} (c_{j,k}^r c_{r,i}^k - c_{i,j}^r c_{r,k}^k)$$

where $k \in \{1, \ldots, n-1\} - \{i, j\}$.

The nice thing about defining things this way is that we can naturally extend this construction to any ring (or even any scheme!). Poonen has already used this to great effect in getting better bounds on the dimension of another important moduli space, the Hilbert scheme.

Others have also done some work on making rings of rank n a moduli space, including Pierre Deligne and Bhargava's student Melanie Matchett Wood (who was the project leader in Arizona).

4. Applications

Given the relative simplicity of the problem and the completeness of the answer, it should not be surprising that the applications are vast. Bhargava's original intent was to get good asymptotics for the number of number fields of degree n and discriminant $\leq X$ as $X \to \infty$. That this number is finite is classical and just figuring this out would have been a great success.

This part of his study has already been realized:

- There is only one Number Field of degree 1
- There are asymptotically $\frac{X}{\zeta(2)}$ quadratic number fields of discriminant $\leq X$
- Davenport and Heilbronn computed in 1970 that asymptotically there are $\frac{X}{3\zeta(3)}$ number fields of discriminant $\leq X$
- The number of S_4 quartic fields with discriminant $\leq X$ is asymptotically $\frac{5\zeta(2)^2\zeta(3)}{24\zeta(5)}X = \frac{5}{24}\prod_p(1+p^{-2}-p^{-3}-p^{-4})X$(and asymptotically only about 90 % of all quartic fields are S_4 quartic, the rest are D_4.
- The number of S_5 quintic fields with discriminant $\leq X$ is asymptotically $\frac{13}{120}\prod_p(1+p^{-2}-p^{-4}-p^{-5})X$

Likewise, we can do real analogues of Gauss composition to pair rings with class group elements to get asymptotics for certain types of class groups.

From the connection to Lie Groups comes work on modular forms on exceptional groups. G-G-S have already figured out how to make Fourier coefficients work on G_2 and some people at UCSD are currently trying to use Bhargava's work to find Fourier coefficients for F_4 modular forms.