On the classification of rings of "small" rank

Manjul Bhargava

March 14, 2009

The purpose of these notes is to study *rings of rank n*:

Definition 1 A *ring of rank n* is a commutative, associative ring with identity that is free of rank n as a $\mathbb{Z}$-module.

That is, a ring of rank n is a ring (commutative, associative, with unit) whose underlying additive group is isomorphic to $\mathbb{Z}^n$.

The prototypical examples of rings of rank n are, of course, orders in degree n number fields. The class of all such examples consists precisely of those rings of rank n that are *integral domains*.

However, there are many interesting examples of rings of rank n that are not integral domains. For example, there are degenerate rings such as $\mathbb{Z}[x]/(x^n)$ or $\mathbb{Z}[x_1, \ldots, x_{n-1}]/(x_1, \ldots, x_{n-1})^2$. One may also construct rings of rank n by taking (any rank n subring of) a direct sum of k rings having ranks $n_1, \ldots, n_k$ respectively, where $n_1 + \cdots + n_k = n$. For instance, $\mathbb{Z}^{\oplus n}$ is a nice example of a ring of rank n.

More generally, we may consider rings of rank n over any base ring T: a *ring of rank n over T* is any ring that is locally free of rank n as a T-module.

Concerning terminology, we refer to rings of rank 2, 3, 4, 5, or 6 as *quadratic*, *cubic*, *quartic*, *quintic*, or *sextic* rings respectively.

In these notes, we wish to classify rings of small rank n, where by "small" we mean "at most 5".

We begin with the simplest possible case, namely $n = 1$.*

1 $n = 1$

Theorem 1 *The only ring of rank* 1 *is* $\mathbb{Z}$. (Prove this!)

2 $n = 2$

So $n = 1$ was pretty easy. The case $n = 2$ is actually not that much more difficult:

Any quadratic ring S has a basis of the form $\langle 1, \tau \rangle$. To specify the ring structure on S, we only need to know $\tau \cdot \tau$, i.e.,

$$\tau^2 = b\tau + c \tag{1}$$

for some $b, c \in \mathbb{Z}$. The discriminant D of this quadratic is $b^2 + 4c$. Now the basis $\langle 1, \tau \rangle$ of S is not unique; τ may be negated, or translated by any integer. Via such a transformation, $b \in \mathbb{Z}$ can be transformed into any integer of the same parity. Thus, by translating τ by an appropriate integer, we may assume $b = 0$ or 1. Note that the value of the discriminant $D = b^2 + 4c$ will not change under such a transformation.

Therefore, for any quadratic ring, we can choose a basis $\langle 1, \tau \rangle$ such that either

$$\tau^2 = c \text{ or } \tau^2 = \tau + c, \tag{2}$$

where c is some integer; these quadratics have discriminants

$$4c \text{ or } 4c + 1, \tag{3}$$

respectively.

Conversely, given any discriminant D of the form $4c$ or $4c + 1$, we may construct a quadratic ring $S = S(D)$ with basis $\langle 1, \tau \rangle$ where τ satisfies either the first or second equation in (2) respectively. This integer D is called the *discriminant* $\mathrm{Disc}(S)$ of the quadratic ring S.

We conclude that quadratic rings S (up to isomorphism) are in one-to-one correspondence with the set $\mathbb{D} := \{D \in \mathbb{Z} : D \equiv 0 \text{ or } 1 \pmod 4\}$ via the discriminant map $S \mapsto \mathrm{Disc}(S)$. We summarize this in the following

Theorem 2 *Isomorphism classes of quadratic rings* S *are in canonical bijection with elements of the set* $\mathbb{D} = \{D \in \mathbb{Z} : D \equiv 0 \text{ or } 1 \pmod 4\}$ *of discriminants. Under this bijection, a quadratic ring* S *corresponds to* $\mathrm{Disc}(S) \in \mathbb{D}$*, and an element* $D \in \mathbb{D}$ *corresponds to the quadratic ring* $S(D) := \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$.

*Actually, I guess the "zero ring", in which there is just one element, namely $1 = 0$, is a ring of rank 0, and this clearly is the only ring of rank 0. So perhaps THIS is the simplest possible case!

Thus, we see that quadratic rings are uniquely specified, up to isomorphism, by their "discriminants".

The discriminant is, in fact, a well-defined invariant for any ring R of rank n, as follows. To any ring of rank n we may attach the *trace* function $\mathrm{Tr} : \mathcal{R} \to \mathbb{Z}$, which assigns to an element $\alpha \in \mathcal{R}$ the trace of the endomorphism $\mathcal{R} \xrightarrow{\times\alpha} \mathcal{R}$. The *discriminant* $\mathrm{Disc}(\mathcal{R})$ of such a ring $\mathcal{R}$ is then defined as the determinant $\det(\mathrm{Tr}(\alpha_i\alpha_j)) \in \mathbb{Z}$, where $\{\alpha_i\}$ is any $\mathbb{Z}$-basis of $\mathcal{R}$.

It is a classical fact, due to Stickelberger, that a ring having finite rank as a $\mathbb{Z}$-module must have discriminant congruent to 0 or 1 (mod 4). We have already seen this in the case of rank 2: such a ring must have $\mathbb{Z}$-basis of the form $< 1, \tau >$, where τ satisfies a quadratic $\tau^2 + r\tau + s = 0$ with $r, s \in \mathbb{Z}$. The discriminant of this ring is then computed to be $r^2 - 4s$, which is congruent to 0 or 1 modulo 4.

The discriminant is THE fundamental invariant of rings of rank n. It, in some sense, measures the "size" of the ring. In the case $n = 2$, the discriminant also completely characterizes the ring. For higher n, however, it is NOT a complete invariant; for example, it is easy to come up with nonisomorphic rings of rank 3 having the same discriminant. (Try this!)

Thus the classification of rings of rank > 2 requires additional information.

We end this section with some simple exercises for the case $n = 2$:

Exercise 1 What $D \in \mathbb{D}$ corresponds to the quadratic ring $\mathbb{Z} \oplus \mathbb{Z}$? What about $\mathbb{Z}[x]/(x^2)$?

Exercise 2 Which quadratic rings are integral domains? (That is, for which $D \in \mathbb{D}$ is $S(D)$ an integral domain?)

Exercise 3 Show that every quadratic ring $S(D)$ has automorphism group isomorphic to C_2.

3 $n = 3$

The case $n = 3$, in the case of integral domains, was beautifully handled by Delone and Faddeev [5] in their classical work on cubic irrationalities; their work was recently refined to general cubic rings by Gan, Gross, and Savin [6]. In this section, we discuss this classification.

3.1 Cubic rings and binary cubic forms

Just as quadratic rings are parametrized by elements of $\mathbb{D}$, the theorem of Delone–Faddeev–Gan–Gross–Savin states that cubic rings are parametrized by $\mathrm{GL}_2(\mathbb{Z})$-*equivalence classes of integral binary cubic forms.*

More precisely, an *integral binary cubic form* is a homogeneous polynomial of degree 3 in two variables with integer coefficients, i.e., it is of the form

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

where $a, b, c, d \in \mathbb{Z}$. The group $\mathrm{GL}_2(\mathbb{Z})$ acts on integral binary cubic forms in the so-called "twisted" way; namely, an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on a binary cubic form $f(x, y)$ by

$$(\gamma \cdot f)(x, y) = \frac{1}{\det(\gamma)} \cdot f((x, y) \cdot \gamma).$$

The theorem of Delone–Faddeev–Gan–Gross–Savin then states:

Theorem 3 ([5],[6]) *There is a canonical bijection between isomorphism classes of cubic rings and the set of* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of integral binary cubic forms. Under this bijection, the discriminant of a cubic ring is equal to the discriminant of the corresponding binary cubic form.*

Proof: Given a cubic ring R, let $\langle 1, \omega, \theta \rangle$ be a $\mathbb{Z}$-basis for R. Translating ω, θ by the appropriate elements of $\mathbb{Z}$, we may assume that $\omega \cdot \theta \in \mathbb{Z}$. A basis satisfying the latter condition is called *normal*. If $\langle 1, \omega, \theta \rangle$ is a normal basis, then there exist constants $a, b, c, d, \ell, m, n \in \mathbb{Z}$ such that

$$\begin{array}{rcl} \omega\theta & = & n \\ \omega^2 & = & m + b\omega - a\theta \\ \theta^2 & = & \ell + d\omega - c\theta. \end{array} \tag{4}$$

To the cubic ring R, we associate the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, form a potential cubic ring having multiplication laws (4). The values of ℓ, m, n are subject to the

associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega \cdot \omega\theta$, which when multiplied out using (4), yield a system of equations that possess a unique solution for n, m, ℓ, namely

$$\begin{array}{rcl} n & = & -ad \\ m & = & -ac \\ \ell & = & -bd. \end{array} \tag{5}$$

If follows that any binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, via the recipe (4) and (5), leads to a unique cubic ring $R = R(f)$.

Lastly, one observes by an explicit calculation that changing the $\mathbb{Z}$-basis $\langle \omega, \theta \rangle$ of $R/\mathbb{Z}$ by an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, and then renormalizing the basis in R, transforms the corresponding binary cubic form $f(x,y)$ by that same element of $\mathrm{GL}_2(\mathbb{Z})$. Hence an isomorphism class of cubic rings determines a binary cubic form uniquely up to the action of $\mathrm{GL}_2(\mathbb{Z})$. This is the desired conclusion. $\square$

One finds by an explicit calculation using (4) and (5) that the discriminant of the cubic ring $R(f)$ is precisely the discriminant of the binary cubic form f; explicitly, it is given by

$$\mathrm{Disc}(R(f)) = \mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \tag{6}$$

We end this subsection with some exercises.

Exercise 4 What binary cubic form f corresponds to the cubic ring $\mathbb{Z}^3$? To $\mathbb{Z}[x]/(x^3)$? To $\mathbb{Z}[x,y]/(x^2, xy, y^2)$? To $\mathbb{Z}[\sqrt[3]{n}]$?

Exercise 5 Prove that $R(f)$ is an integral domain (equivalently, an order in a number field) if and only if f is irreducible as a polynomial over $\mathbb{Q}$.

Exercise 6 Suppose that f has nonzero discriminant. Prove that a cubic ring $R(f)$, having nonzero discriminant, has automorphism group isomorphic either S_3, C_3, C_2 or $\mathbf{1}$. Prove that if f is irreducible over $\mathbb{Q}$, then the only possible automorphism groups for $R(f)$ are C_3 or $\mathbf{1}$. How can one distinguish all these possibilities simply by looking at f? (Hint: look also at the next two exercises!)

Exercise 7 Consider the form $\mathrm{Tr}(x^2)$ on the cubic ring $R = R(f)$. Now restrict this form to the sublattice of $\mathbb{Z} + 3R$ consisting of elements of trace 0. What is the interpretation of this quadratic form in terms of the corresponding binary cubic f?

Exercise 8 (Continuation of Exercise 7) Write down some examples of cubic rings inside Galois cubic fields. Do they all have three automorphisms? What are the associated binary cubics? What can you say about the $\mathrm{Tr}(x^2)$ form for a cubic ring having three automorphisms? Can you use this to give an explicit parametrization of such "C_3-cubic rings"?

Exercise 9 Show that the cubic ring given by a binary cubic form lies in the field generated by the coordinates of the points cut out in $\mathbb{P}^1$ by the form. What if the field is quadratic?

Exercise 10 (*) What can you say about the integers represented by a binary cubic form f, making use of the relationship with the corresponding cubic ring $R(f)$?

3.2 Quadratic resolvent rings of a cubic ring

Here is an alternative way to look at the cubic case, using *resolvent rings*. First, recall that the discriminant of a cubic ring is always an integer that is 0 or 1 (mod 4), i.e., it is always an element of $\mathbb{D}$. We may thus define a *quadratic resolvent ring* of a cubic ring as follows.

Definition 2 For a cubic ring R, the *quadratic resolvent ring* of R is the unique quadratic ring S such that $\mathrm{Disc}(R) = \mathrm{Disc}(S)$.

Now suppose R is an order in a cubic field K. Then there is a natural map $f : R \to S$, namely

$$f(x) = \frac{\mathrm{Disc}(x) + \sqrt{\mathrm{Disc}(x)}}{2} := \frac{[(x-x')(x'-x'')(x''-x)]^2 + (x-x')(x'-x'')(x''-x)}{2}, \tag{7}$$

where x, x', x'' denote the conjugates of x in the Galois closure of K.

The map f satisfies two key properties:

(a) f is discriminant-preserving: $\mathrm{Disc}(f(x)) = \mathrm{Disc}(x)$ (Check this!);

(b) $f : R \to S$ descends to a map $\bar{f} : R/\mathbb{Z} \to S/\mathbb{Z}$ (Check this!).

Note that $\bar{f}$ is a cubic map from $R/\mathbb{Z} \cong \mathbb{Z}^2$ (as $\mathbb{Z}$-modules) to $S/\mathbb{Z} \cong \mathbb{Z}$ (as $\mathbb{Z}$-modules); thus $\bar{f}$ is a binary cubic form!

Exercise 11 Show that $\bar{f}$ gives the same binary cubic form as in the Delone-Faddeev correspondence.

Thus we have obtained a concrete ring-theoretic interpretation of the Delone-Faddeev correspondence in terms of resolvent rings.

Remark 1 Note that the *quadratic resolvent field* of a cubic field, and the corresponding map f for these fields, was very important in the classical solution to the cubic equation.

4 $n = 4$

We now turn to quartic rings! In analogy with the quadratic resolvents of a cubic ring as in the previous section, we begin by considering *cubic resolvent rings* of a quartic ring.

4.1 Cubic resolvent rings of a quartic ring

Let Q be a *quartic ring*, and assume moreover that Q is an order in an S_4-quartic field K. In parallel with the cubic case discussed in the previous section, we want to find a cubic ring R and a map $\phi : Q \to R$ preserving discriminants.

Such a map ϕ comes up in a natural way in the classical theory of solving the quartic: if x, x', x'', x''' denote the conjugates of x in the Galois closure of K, then we let

$$\phi(x) = xx' + x''x'''. \tag{8}$$

It is known from the classical theory of solving the quartic that ϕ is discriminant-preserving; this amounts to the beautiful identity

$$\begin{aligned}\big([xx' + x''x'''] - [xx'' + x'x''']\big)\big([xx'' + x'x'''] - [xx''' + x'x'']\big)\big([xx''' + x'x''] - [xx' + x''x''']\big)\\ = \quad (x - x''')(x' - x'') \quad \cdot \quad (x - x')(x'' - x''') \quad \cdot \quad (x - x'')(x' - x''').\end{aligned}$$

It is also clear that $\phi(x)$ lies in a cubic ring, being algebraic and having exactly three S_4-conjugates in K.

What does it mean for R to be a *cubic resolvent ring* of Q?

Definition 3 A *cubic resolvent ring* of a quartic ring Q is a cubic ring R such that $\mathrm{Disc}(Q) = \mathrm{Disc}(R)$ and $R \supseteq \{\phi(x) : x \in Q\}$.

Now given Q and a cubic resolvent ring R, we get a natural map

$$\phi : Q \to R$$

preserving discriminants. Again, we see that ϕ descends to a map

$$\bar{\phi} : Q/\mathbb{Z} \to R/\mathbb{Z}, \tag{9}$$

because we see that, for any $c \in \mathbb{Z}$,

$$\phi(x + c) = (x + c)(x' + c) + (x'' + c)(x''' + c) = \phi(x) + d$$

for some $d \in \mathbb{Z}$, namely $d = c\,\mathrm{Tr}(x) + 2c^2$.

4.2 Quartic rings and pairs of ternary quadratic forms

As a map between $\mathbb{Z}$-modules, the map $\bar{\phi}$ in (9) is a quadratic map from $Q/\mathbb{Z} \cong \mathbb{Z}^3$ to $R/\mathbb{Z} \cong \mathbb{Z}^2$, and thus corresponds to a *pair* (A, B) *of integral ternary quadratic forms*, well-defined up to $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$-equivalence.

So given a pair (Q, R) consisting of a quartic ring and a cubic resolvent, we obtain a pair (A, B) of integral ternary quadratic forms. The question now arises: given (A, B), can one recover (Q, R)? (to go back)

The following lemma about ϕ plays an invaluable role in determining the multiplicative structure of Q from (A, B). To state the lemma, we use the notation $\mathrm{Ind}_M(v_1, v_2, \ldots, v_k)$ to denote the (signed) index of the lattice spanned by $v_1, v_2, \ldots, v_k$ in the (oriented) rank k $\mathbb{Z}$-module M; in other words, $\mathrm{Ind}_M(v_1, v_2, \ldots, v_k)$ is the determinant of the tranformation between $v_1, v_2, \ldots, v_k$ and any (positively oriented) $\mathbb{Z}$-basis of M. Then we have:

Lemma 1 *If Q is a quartic ring, and R is a cubic resolvent ring of Q, then for any $x, y \in Q$ we have*

$$\mathrm{Ind}_Q(1, x, y, xy) = \pm \mathrm{Ind}_R(1, \phi(x), \phi(y)). \tag{10}$$

Proof: Since $\mathrm{Disc}(Q) = \mathrm{Disc}(R)$, it suffices to show that the discriminants of the corresponding lattices are equal:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ x & x' & x'' & x''' \\ y & y' & y'' & y''' \\ xy & x'y' & x''y'' & x'''y''' \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ xx' + x''x''' & xx'' + x'x''' & xx''' + x'x'' \\ yy' + y''y''' & yy'' + y'y''' & yy''' + y'y'' \end{vmatrix}.$$

This identity may be verified by direct calculation. □

The sign in expression (10) of course depends on how Q and R are oriented. To fix the orientations on Q and R once and for all, let $\langle 1, \alpha, \beta, \gamma \rangle$ and $\langle 1, \omega, \theta \rangle$ be bases for Q and R respectively such that the map ϕ is given by

$$\phi(r\bar{\alpha} + s\bar{\beta} + t\bar{\gamma}) = B(r, s, t)\bar{\omega} + A(r, s, t)\bar{\theta}, \tag{11}$$

where $\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\omega}, \bar{\theta}$ denote the reductions modulo $\mathbb{Z}$ of $\alpha, \beta, \gamma, \omega, \theta$ respectively. Then we fix the orientations on Q and R so that $\mathrm{Ind}_Q(1, \alpha, \beta, \gamma) = \mathrm{Ind}_R(1, \omega, \theta) = 1$.

For a fixed (A, B), we can use the lemma to understand the ring structure on Q. First, let Q have $\mathbb{Z}$-basis $\langle 1 = \alpha_0, \alpha_1, \alpha_2, \alpha_3 \rangle$, where we have

$$\alpha_i \alpha_j = \sum_{k=0}^{3} c_{ij}^k \alpha_k \tag{12}$$

for some set of integral constants $c_{ij}^k \in \mathbb{Z}$.

We may make one additional assumption about the basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ without any harm. By translating $\alpha_1, \alpha_2, \alpha_3$ by appropriate constants in $\mathbb{Z}$, we may arrange for the coefficients of α_1 and α_2 in $\alpha_1\alpha_2$, together with the coefficient of α_1 in $\alpha_1\alpha_3$, to each equal zero. We call a basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ satisfying the latter conditions a *normal basis* for Q. Similarly, a basis $\langle 1, \omega, \theta \rangle$ of R is called normal if the coefficients of ω and θ in $\omega\theta$ are both equal to zero.

In terms of the constants c_{ij}^k in (12), the condition that the basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ is normal is equivalent to

$$c_{12}^1 = c_{12}^2 = c_{13}^1 = 0. \tag{13}$$

Similarly, that the basis $\langle 1, \omega, \theta \rangle$ of R is normal is equivalent to the multiplication table of R taking the form (4). We choose to normalize bases because bases of $Q/\mathbb{Z}$ (resp. $R/\mathbb{Z}$) then lift uniquely to normal bases of Q (resp. R).

Let $x = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3$, $y = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3$ be general elements of Q, where $r_i, s_i \in \mathbb{Z}$. Then using (12), we find that

$$xy = c + t_1\alpha_1 + t_2\alpha_2 + t_3\alpha_3,$$

where $c \in \mathbb{Z}$ and

$$t_k = \sum_{1 \le i,j \le 3} c_{ij}^k \, r_i s_j \tag{14}$$

for $k = 1, 2, 3$. It follows that

$$\mathrm{Ind}_Q(1, x, y, xy) = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & r_1 & r_2 & r_3 \\ 0 & s_1 & s_2 & s_3 \\ 0 & t_1 & t_2 & t_3 \end{vmatrix}. \tag{15}$$

The right side of (15) is a polynomial of degree 4 in the variables r_1, r_2, r_3, s_1, s_2, s_3, which we denote by $p(r_1, r_2, r_3, s_1, s_2, s_3)$.

Similarly,

$$\mathrm{Ind}_R(1, \phi_{4,3}(x), \phi_{4,3}(y)) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & B(r_1, r_2, r_3) & A(r_1, r_2, r_3) \\ 0 & B(s_1, s_2, s_3) & A(s_1, s_2, s_3) \end{vmatrix}. \tag{16}$$

The right side of (16) is also a polynomial of degree 4 in the variables r_1, r_2, r_3, s_1, s_2, s_3, which we denote by $q(r_1, r_2, r_3, s_1, s_2, s_3)$. (Note that the multiplicative structure of R was not needed for computing the polynomial q.)

By Lemma 1, we conclude that for all integers $r_1, r_2, r_3, s_1, s_2, s_3$,

$$p(r_1, r_2, r_3, s_1, s_2, s_3) = q(r_1, r_2, r_3, s_1, s_2, s_3).$$

As they take equal values at all integer arguments, the polynomials p and q must in fact be identical. Equating coefficients of like terms yields a system of linear equations in the 15 variables c_{ij}^k ($k \geq 1$) in terms of the coefficients of the quadratic forms A and B, and this system is easily seen to have a unique solution. Writing out the pair (A, B) of ternary quadratic forms as

$$\begin{aligned} A(x_1, x_2, x_3) &= \sum_{1 \leq i \leq j \leq 3} a_{ij}\, x_i x_j \\ B(x_1, x_2, x_3) &= \sum_{1 \leq i \leq j \leq 3} b_{ij}\, x_i x_j, \end{aligned} \tag{17}$$

and letting $a_{ji} = a_{ij}$ and $b_{ji} = b_{ij}$, define the constants $\lambda_{k\ell}^{ij} = \lambda_{k\ell}^{ij}(A, B)$ by

$$\lambda_{k\ell}^{ij}(A, B) = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{k\ell} & b_{k\ ell} \end{vmatrix}; \tag{18}$$

the $\lambda_{k\ell}^{ij}$ thus take up to 15 possible nonzero values up to sign. Then we find that the unique solution to the system $p = q$ is given as follows. For any permutation (i, j, k) of $(1, 2, 3)$, we have

$$\begin{aligned} c_{ii}^i &= \pm\lambda_{ij}^{ik} + C_i, \\ c_{ii}^j &= \pm\lambda_{ik}^{ii}, \\ c_{ij}^i &= \pm\tfrac{1}{2}\lambda_{jj}^{ik} + \tfrac{1}{2}C_j, \\ c_{ij}^k &= \pm\lambda_{ii}^{jj}, \end{aligned} \tag{19}$$

where we have used $\pm$ to denote the sign of the permutation (i, j, k) of $(1, 2, 3)$, and where the constants C_i are given by

$$C_1 = \lambda_{11}^{23}, \quad C_2 = -\lambda_{22}^{13}, \quad C_3 = \lambda_{33}^{12}. \tag{20}$$

Note that the c_{ij}^0 are still undetermined. However, it turns out that the associative law for Q now uniquely determines the c_{ij}^0 from the other c_{ij}^k. Indeed, computing the expressions $(\alpha_i\alpha_j)\alpha_k$ and $\alpha_i(\alpha_j\alpha_k)$ using (12), and then equating the coefficients of α_k, yields the equality

$$c_{ij}^0 = \sum_{r=1}^{3} \left(c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k\right) \tag{21}$$

for any $k \in \{1, 2, 3\} \setminus \{j\}$. One easily checks using the explicit values given in (19) that the above expression is independent of k, and that with these values of c_{ij}^0 all relations among the c_{ij}^k implied by the associative law are completely satisfied. Thus we have completely determined the ring structure of $Q = Q(A, B)$ from (A, B); it is given in sum by (12), (19), (20), and (21).

To determine the structure of R from (A, B), we may simply use the relation

$$\mathrm{Ind}_Q(1, x, x^2, x^3) = \mathrm{Ind}_R(1, \phi(x), \phi(x)^2), \tag{22}$$

since the multiplicative structure of Q is now in place. (This identity amounts to the fact that the map ϕ is discriminant-preserving!) Let $x = r_1\alpha + r_2\beta + r_3\gamma \in Q$.

Then

$$\mathrm{Ind}_Q(1, x, x^2, x^3) = p(r_1, r_2, r_3)$$

and

$$\mathrm{Ind}_R(1, \phi(x), \phi(x)^2) = q(r_1, r_2, r_3),$$

where p and q are determinantal expressions similar to (15) and (16).

As before, we argue that the polynomials p and q must take the same values for all integer choices of r_1, r_2, r_3, and consequently are identical. Equating coefficients of like terms, we obtain several linear and quadratic equations in a, b, c, d. Solving these equations for a, b, c, d, we find that there is a unique solution whenever the image of ϕ generates R. This occurs, in particular, whenever $\mathrm{Disc}(A, B) \neq 0$. In that case the unique solution is given by

$$ax^3 + bx^2y + cxy^2 + dy^3 = 4 \cdot \mathrm{Det}(Ax - By) \tag{23}$$

and hence the structure of R is determined, at least whenever $\mathrm{Disc}(A, B) \neq 0$.

It is interesting to ask what the discriminant of the resulting quartic ring $Q(A, B)$ and cubic ring $R(A, B)$ is in terms of the pair of ternary quadratic forms (A, B). As an explicit calculation shows, the answer is happily that $\mathrm{Disc}(Q(A, B)) = \mathrm{Disc}(A, B) := \mathrm{Disc}(4 \cdot \mathrm{Det}(Ax - By))$.

We may summarize our discussion as follows:

Theorem 4 *There is a canonical bijection between the set of* $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$*-orbits on the space* $(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ *of pairs of integral ternary quadratic forms and the set of isomorphism classes of pairs* (Q, R)*, where* Q *is a quartic ring and* R *is a cubic resolvent ring of* Q*.*

Under this bijection, the discriminant of an element $(A, B) \in (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ *is equal to the discriminant of the quartic ring* Q*. Furthermore, the binary cubic form corresponding to the cubic ring* R *by the Delone-Faddeev correspondence is* $4 \cdot \mathrm{Det}(Ax - By)$*.*

Although we have proven the above theorem only for those quartic rings Q that are orders in S_4-quartic fields, it is possible to define cubic resolvent rings R for a general quartic ring appropriately so that Theorem 4 extends to general quartic rings.

Definition 4 Let Q be a quartic ring. Then $R = (R, \bar{\phi}, \delta)$ is a cubic resolvent ring of Q if

(a) $\bar{\phi} : Q/\mathbb{Z} \to R/\mathbb{Z}$ is a quadratic map

(b) $\delta : \wedge^4 Q \to \wedge^3 R$ is an isomorphism

(c) $\delta(1 \wedge x \wedge y \wedge xy) = 1 \wedge \bar{\phi}(x) \wedge \bar{\phi}(y)$

(d) If we write $\bar{\phi} = (A, B)$, then R is the cubic ring corresponding to $4 \cdot \mathrm{Det}(Ax - By)$ under the Delone–Faddeev–Gan–Gross–Savin correspondence.

Using Definition 4, the proof of Theorem 4 for general Q is then essentially identical.

It remains to understand whether a quartic ring even possesses a single cubic resolvent ring! Using a study of the invariant theory of pairs of ternary quadratic forms, it is proven in [3] that

Proposition 1 *The number of cubic resolvents of a quartic ring Q is the number of sublattices of $\mathbb{Z}^2$ of index $\mathrm{ct}(Q)$, where*

$$\mathrm{ct}(Q) = \sup\{n : \exists \text{ quartic ring } Q' \text{ s.t. } Q = \mathbb{Z} + nQ'\}.$$

It follows that every quartic ring has a cubic resolvent!

Corollary 1 *Every quartic ring has a cubic resolvent ring. For a maximal quartic ring, the cubic resolvent ring is unique.*

Thus Theorem 4 is a bijection on maximal quartic rings, and so in particular on the rings of integers in quartic number fields!

Finally, we remark that one can characterize local properties of a quartic ring (e.g., maximality, prime splitting, etc.) by explicit congruence conditions on the corresponding pair of ternary quadratic forms. See [3] for details. One may also treat these matters entirely geometrically, as hinted at in Exercise 14 below. See Melanie's lecture notes for more on this perspective!

We end this section again with some exercises:

Exercise 12 What pair of ternary quadratic forms corresponds to the quartic ring $\mathbb{Z}^4$? To $\mathbb{Z}[x]/(x^4)$? To $\mathbb{Z}[x, y, z]/(x, y, z)^2$? To $\mathbb{Z}[\sqrt[4]{n}]$? To $\mathbb{Z}[\sqrt{a}, \sqrt{b}]$? Or your favorite quartic ring?

Exercise 13 (*) Find pairs of ternary quadratic forms corresponding to quartic rings that have some special kind of structure – for example, those lying inside $K \oplus \mathbb{Q}$ where K is a cubic field. How does this relate to cubic rings and binary cubic forms? What about other types of special structure, such as the various possible Galois groups? Can you find nice representatives for the pairs of ternary quadratic forms corresponding to these? Can you find a parametrization space for quartic rings with one of these structures?

Exercise 14 Show that the quartic ring given by a pair of ternary quadratic forms lies in the field generated by the coordinates of the points cut out in $\mathbb{P}^2$ by these forms. In particular, what happens in some of the special cases considered in Exercise 13?

Exercise 15 (*) What can you say about the pairs of integers represented by a pair of ternary quadratic forms in terms of the corresponding quartic ring?

5 $n = 5$

The key to understanding the parametrization of quintic rings is first understanding the combinatorics of the numbers 5 and 6.

5.1 Six pentagons and a hexagon

The complete graph on five vertices contains twelve 5-cycles. The symmetric group S_5 acts naturally on this set of twelve 5-cycles, and under this action, the unique S_5-orbit of twelve elements splits up into two A_5-orbits consisting of six elements each. One such A_5-orbit of 5-cycles is illustrated in Figure 1, while the other A_5-orbit can be obtained simply by taking the graph complements of the 5-cycles shown in Figure 1. Together these two A_5-orbits, viewed as six pairs of complementary graphs, yield the six ways of partitioning the complete graph on five vertices into pairs of 5-cycles. The "metacyclic" subgroup $M^{(i)}$ is defined to be the set of all elements in S_5 that map the 5-cycle in Figure 1ⓘ to either itself *or* its complement.

We observe that any two 5-cycles in Figure 1 share exactly two common edges; moreover, these two edges always involve four distinct vertices, so that there is exactly one vertex that neither edge passes through. For example, the 5-cycles labelled ① and ② in Figure 1 share precisely the edges $\overline{2\ 3}$ and $\overline{4\ 5}$ involve the four distinct vertices 2, 3, 4 and 5. Vertex 1 does not arise. Thus in Figure 2, we label the edge connecting ① and ② by the number "1". In general, the edge connecting ⓘ and ⓙ in Figure 2 is labelled by the number of the unique vertex that does not lie on a common edge of the cycles labelled ⓘ and ⓙ in Figure 1. In this way, we obtain in Figure 2 a complete graph on six vertices whose 15 edges are labelled by numbers in the set $\{1, 2, \ldots, 5\}$, and where each of the 5 numbers occurs as the

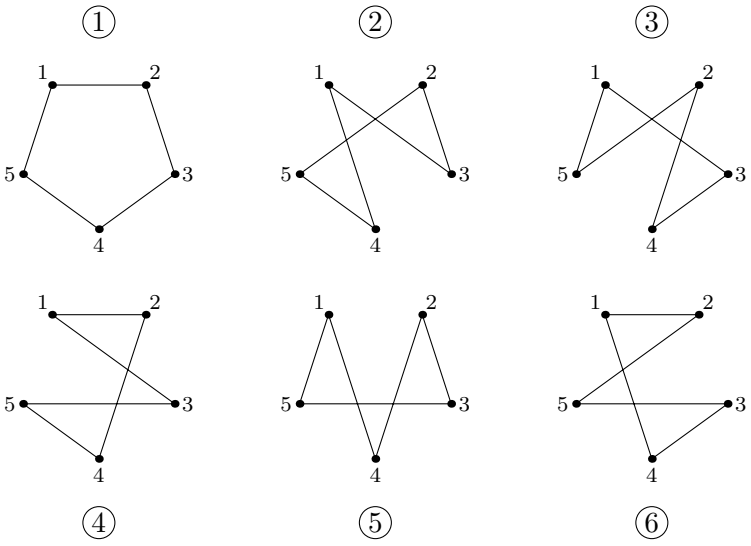

Figure 1: Six pentagons.

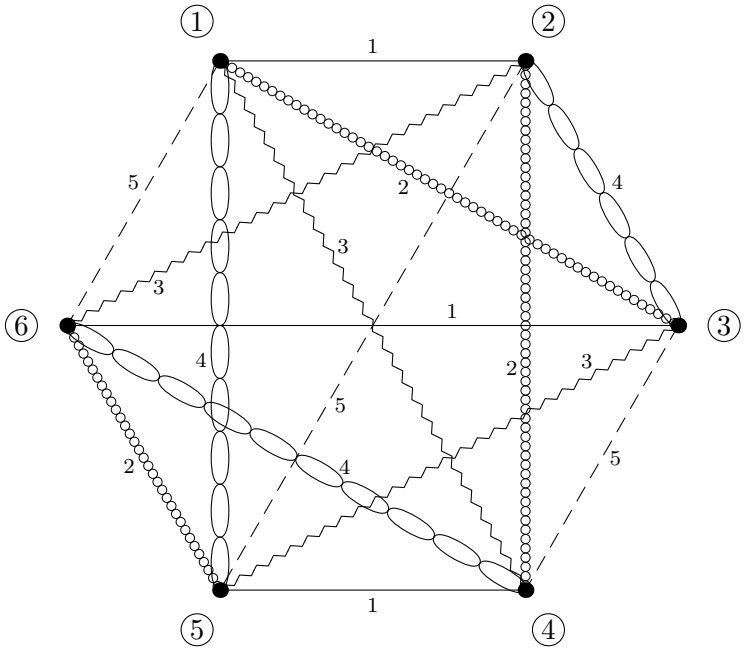

Figure 2: A hexagon.

label of an edge exactly 3 times. Thus, for example, "1" occurs as the label on the three disjoint edges (①,②), (③,⑥), and (④,⑤). It is interesting to note that the process of obtaining Fig. 2 from Fig. 1 is completely reversible; i.e., up to taking the graph complements of ①,...,⑥, the 5-cycles labelled ①,...,⑥, in Fig. 1 are completely determined by the labellings in Fig. 2. In particular, the natural action of S_5 on the six elements ①,...,⑥ is completely determined by Fig. 2.

In sum, the elements of $\{1,2,3,4,5,6\}$ correspond to certain 5-cycles on the set $\{1,2,3,4,5\}$ (Fig. 1), while the elements of $\{1,2,3,4,5\}$ correspond to certain disjoint triples of pairs of elements in $\{1,2,3,4,5,6\}$ (Fig. 2). These 'dual" correspondences between the sets $\{1,2,3,4,5\}$ and $\{1,2,3,4,5,6\}$ play a central role in understanding the relationship between quintic rings and their sextic resolvents.

5.2 Sextic resolvents of a quintic ring

Suppose now R is an order in an S_5-quintic field K. Let S be an order in the sextic resolvent field of K, i.e., in the field fixed by the metacyclic group $M = M^{(1)} \subset S_5$ when it acts on the Galois closure of K.

Then there is a natural map $F : R \to S \otimes \mathbb{Q}$ defined by defined by

$$F(\alpha) = \frac{1}{\sqrt{\mathrm{Disc}(R)}}\big(\alpha^{(1)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(4)} + \alpha^{(4)}\alpha^{(5)} + \alpha^{(5)}\alpha^{(1)} - \alpha^{(1)}\alpha^{(3)} - \alpha^{(3)}\alpha^{(5)} - \alpha^{(5)}\alpha^{(2)} - \alpha^{(2)}\alpha^{(4)} - \alpha^{(4)}\alpha^{(1)}\big), \quad (24)$$

called the Cayley-Klein resolvent map. (Check that this map indeed has image in the sextic resolvent field.) This map is very important in the solution of the quintic equation, whenever it is solvable. It is, however, not the most fundamental map between a quintic ring/field and its sextic resolvent!

This most fundamental map f seems to have been missed in the literature, perhaps because the map is not symmetric, but alternating!

This special map f is as follows. One takes S to be an order (to be specified later) in the sextic resolvent field so that f is a map $f : R \to \wedge^2 S$, or equivalently (by taking duals), a map $f : \wedge^3 S \to R^\vee$, where $R^\vee$ denotes the dual lattice in $R \otimes \mathbb{Q}$ of R under the trace form.

Then f is defined on $\wedge^3 S$ as follows. For $s \in S$, let $s^{(1)}, s^{(2)}, \ldots, s^{(6)}$ denote the conjugates of s in $\bar{R} \otimes \mathbb{Q}$, labelled so that they are stabilized by $M^{(1)}, M^{(2)}, \ldots, M^{(6)}$ respectively; then for any $x, y, z \in S$, define $f(x \wedge y \wedge z) \in R^*$ by

$$f(x,y,z) = \frac{1}{16 \cdot \mathrm{Disc}(R)} \begin{vmatrix} x^{(1)} - x^{(2)} & x^{(3)} - x^{(6)} & x^{(4)} - x^{(5)} \\ y^{(1)} - y^{(2)} & y^{(3)} - y^{(6)} & y^{(4)} - y^{(5)} \\ z^{(1)} - z^{(2)} & z^{(3)} - z^{(6)} & z^{(4)} - z^{(5)} \end{vmatrix}. \quad (25)$$

Note that (1,2), (3,6), and (4,5) are the pairs corresponding to the edges labelled "1" in the hexagon in Figure 2.

One checks using Figures 1 and 2 that the the map f has the following properties:

- f is fixed under the action of $S_4^{(1)} \subset S_5$. Hence $f(x,y,z)$ lies in $R \otimes \mathbb{Q}$.
- $f = f^{(1)}$ has five conjugate maps $f^{(1)}$, $f^{(2)}, \ldots, f^{(5)}$, and

  $$f^{(1)}(x,y,z) + f^{(2)}(x,y,z) + \cdots + f^{(5)}(x,y,z) = 0.$$

  Hence the image of f lies not only in $R^\vee$, but in fact lies in the distinguished four-dimensional sublattice $(R/\mathbb{Z})^\vee \subset R^\vee \subset R \otimes \mathbb{Q}$ consisting of the trace 0 elements.
- $f : \wedge^3 S \to R^\vee$ descends to a map $\bar{f} : R/\mathbb{Z} \to \wedge^3(S/\mathbb{Z})^\vee \cong \wedge^2(S/\mathbb{Z})$. By taking bases of R and S respectively, we get an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ (a quadruple of quinary alternating 2-forms), well-defined up to the action of $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$.

Now the action of $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ on $A \in \mathbb{Z}^4 \otimes \wedge^3\mathbb{Z}^5$ is known to have a unique polynomial invariant, having degree 40, which we denote by $\mathrm{Disc}(A)$. A calculation shows that

$$2^{24} \cdot \mathrm{Disc}(A) = \mathrm{Disc}(S)^{12} \cdot \mathrm{Disc}(R)^{-35}.$$

Since in analogy with previous cases, we want $\mathrm{Disc}(A) = \mathrm{Disc}(R)$, we conclude that we must have $\mathrm{Disc}(S) = 4 \cdot \mathrm{Disc}(R)^3$. We are now led to the definition of a sextic resolvent of a quintic ring:

Definition 5 Let R be an order in an S_5-quintic field K. Then a sextic resolvent ring S of R is an order in the sextic resolvent field of K such that

(a) $f(x \wedge y \wedge z) \in R^\vee$ for all $x, y, z \in S$; and

(b) $\mathrm{Disc}(S) = 4 \cdot \mathrm{Disc}(R)^3$.

Thus, given a quintic ring R and a sextic resolvent ring S of R as above, we obtain an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ ($\cong (R/\mathbb{Z})^\vee \otimes \wedge^2(S/\mathbb{Z})$).

The question now arises: given an $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, can we recover R and S? Again, the answer is yes!

5.3 Quintic rings and quadruples of alternating quinary 2-forms

To recover R from an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, we make the following observations. First, we observe that $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ acts on $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$; the factor $\mathrm{GL}_4(\mathbb{Z})$ acts on the basis of $R/\mathbb{Z}$, while the factor $\mathrm{GL}_5(\mathbb{Z})$ acts on the basis of $S/\mathbb{Z}$. Thus the multiplicative structure constants of R should be $\mathrm{GL}_5(\mathbb{Z})$-invariants of A. So to recover R, we need to look at the $\mathrm{GL}_5(\mathbb{Z})$-invariants on $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$.

How can one construct these invariants? Clearly the determinant of each skew-symmetric 5×5 matrix $A(x)$ for $x \in R/\mathbb{Z}$ is a $\mathrm{GL}_5(\mathbb{Z})$-invariant; however, this determinant is zero (since it's the determinant of a 5×5 skew-symmetric matrix)! So we need a more clever way to make a nonzero invariant.

Take elements $x, y, z \in R/\mathbb{Z}$. Then $A(x), A(y), A(z)$ are again 5×5 skew-symmetric matrices. All their determinants are zero, but the Pfaffian of the 10×10 skew-symmetric matrix

$$\begin{bmatrix} A(x) & A(y) \\ A(y) & A(z) \end{bmatrix} \tag{26}$$

is clearly a $\mathrm{GL}_5(\mathbb{Z})$-invariant of A (and it's generally nonzero!); indeed, the action of an element $g \in \mathrm{GL}_5(\mathbb{Z})$ on A results in the action of $\left(\begin{smallmatrix} g & \\ & g \end{smallmatrix}\right)$ on the 10×10 skew-symmetric form $\left[\begin{smallmatrix} A(x) & A(y) \\ A(y) & A(z) \end{smallmatrix}\right]$, and hence the value of the Pfaffian does not change. The Pfaffians

$$\mathrm{Pf}(x, y, z) := \mathrm{Pfaff} \begin{bmatrix} A(x) & A(y) \\ A(y) & A(z) \end{bmatrix} \tag{27}$$

are our prototypical $\mathrm{GL}_5(\mathbb{Z})$-invariants.

Now define

$$P^+(X, Y, Z) = \frac{\mathrm{Pf}(X, Y, Z) + \mathrm{Pf}(X, Y, -Z)}{2}, \tag{28}$$

$$P^-(X, Y, Z) = \frac{\mathrm{Pf}(X, Y, Z) - \mathrm{Pf}(X, Y, -Z)}{-2}. \tag{29}$$

Then one checks that $P^+(X, Y, Z)$ and $P^-(X, Y, Z)$ are integer polynomials in the entries of X, Y, Z having homogeneous degrees 2,1,2 and 1,3,1 respectively. By construction, the integer polynomials $P^+(A(x), A(y), A(z))$ for $x, y, z \in R$ are $\mathrm{GL}_5(\mathbb{Z})$-invariants of A. In fact, one can show that all polynomial invariants for $\mathrm{GL}_5(\mathbb{Z})$ acting on $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ must be polynomials in these degree 5 Pfaffians! (However, we shall not need this fact in what follows, and so we omit the proof.)

There is an alternative description of these invariants P^+ and P^- which is also very beautiful. Given a 5×5 skew-symmetric matrix X, let us denote by $Q(X)$ the column vector $[Q_1, \ldots, Q_5]^t$ of 4×4 sub-Pfaffians of A. Thus Q is a quadratic function of the entries of

X. Let $Q(X,Y)$ denote the symmetric bilinear form such that $Q(X,X) = Q(X)$. Then for skew-symmetric 5×5 matrices V, W, X, Y, Z, define the invariant

$$\{VW|X|YZ\} = Q(V,W)^t \cdot X \cdot Q(Y,Z).$$

Then we have

$$P^+(X,Y,Z) = \{XX|Y|ZZ\}, \tag{30}$$

$$P^-(X,Y,Z) = \{XY|Y|YZ\}. \tag{31}$$

We observe the following beautiful identities:

Lemma 2 *For $x, y, z \in R$, we have*

(a) $P^+(A(x), A(y), A(z)) = \mathrm{Ind}_R(1, x, y, z, xz)$

(b) $P^-(A(x), A(y), A(z)) = \mathrm{Ind}_R(1, x, y, z, y^2)$.

In the same way as in the quartic case, Lemma 2 determines uniquely a multiplicative structure on R!

We may write down this multiplicative structure as follows. Let R have $\mathbb{Z}$-basis $\langle 1 = \alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$, where

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{4} c_{ij}^k \alpha_k \,, \tag{32}$$

and the $c_{ij}^k \in \mathbb{Z}$. We use the shorthand $\{ijk\ell m\}$ for $\{A(\alpha_i)A(\alpha_j)|A(\alpha_k)|A(\alpha_\ell)A(\alpha_m)\}$. Then we find that, for any permutation (i,j,k,ℓ) of $(1,2,3,4)$, we have

$$\begin{aligned} c_{ij}^k &= \pm\{ii\ell jj\}/4, \\ c_{ii}^j &= \pm\{\ell iiik\}, \\ c_{ij}^i - c_{ik}^i &= \pm\{jk\ell ii\}/2, \\ c_{ii}^i - c_{ij}^i - c_{ik}^i &= \pm\{ij\ell ki\}, \end{aligned} \tag{33}$$

where we have used $\pm$ to denote the sign of the permutation (i,j,k,ℓ) of $(1,2,3,4)$. By choosing suitable normalizing conditions (as in the cubic and quartic cases), this then determines all c_{ij}^k (for $k \neq 0$) as primitive integer polynomials in the entries of A.

The remaining constant coefficients c_{ij}^0 can also now be uniquely expressed as polynomials in the entries of A, using the associative law in R. Indeed, computing the expressions $(\alpha_i\alpha_j)\alpha_k$ and $\alpha_i(\alpha_j\alpha_k)$, and then equating the coefficients of α_k, yields the equality

$$c_{ij}^0 = \sum_{r=1}^{4} \left(c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k \right) \tag{34}$$

for any $k \in \{1,2,3,4\} \setminus \{j\}$. One checks using the explicit expressions in (33) that the right-hand side of (34) is a polynomial expression in the entries of A that is independent of k. We have thus recovered all structure coefficients of $R = R(A)$ in terms of the SL_5-invariants $\{ijklm\}$ of the quadruple $A = (A_1, \ldots, A_4)$ of 5×5 skew-symmetric matrices.

The sextic resolvent ring $S = S(A)$ can also similarly be recovered from A (though this is a more complicated process). Therefore, we obtain the following theorem:

Theorem 5 *There is a canonical bijection between the* $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$*-orbits on the space* $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *of quadruples* A *of* 5×5 *skew-symmetric matrices and the set of isomorphism classes of pairs* (R, S)*, where* R *is a quintic ring and* S *is a sextic resolvent ring of* R*. Under this bijection, we have* $\mathrm{Disc}(A) = \mathrm{Disc}(R) = \mathrm{Disc}(S)^{1/3}$*.*

Although we have only discussed the above theorem when the quintic ring R is an order in an S_5-quintic field, by defining a sextic resolvent ring appropriately for general quintic rings (as we did in the quartic case), one can extend Theorem 5 to general quintic rings using the identical arguments.

5.4 Pfaffians and the classical resolvent map

In the previous section, we have proven that an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ corresponds to the most fundamental mapping

$$f : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$$

relating the quintic ring $R = R(A)$ and its sextic resolvent $S = S(A)$. However, there are many other beautiful polynomial mappings relating the rings R and S, and any such mapping may be understood in terms of higher covariants of A.

In particular, we may consider the classical resolvent map

$$F : R \to \widetilde{S} \otimes \mathbb{Q}$$

of Cayley-Klein defined by (24). This map, too, is a higher degree covariant of the fundamental map f, namely, it is a degree 2 covariant as follows.

Given an element $A \in (R/\mathbb{Z})^\vee \otimes \wedge^2(S/\mathbb{Z})$, viewed as a quadruple $A = (A_1, A_2, A_3, A_4)$ of 5×5 skew-symmetric matrices, we may form the single 5×5 skew-symmetric matrix $A_1x_1 + A_2x_2 + A_3x_3 + A_4x_4$, where x_1, x_2, x_3, x_4 are indeterminates. Taking the 4×4 sub-Pfaffians of the latter matrix, we obtain 5 quaternary quadratic forms (in x_1, x_2, x_3, x_4). This yields a quadratic map $G : R/\mathbb{Z} \to (S/\mathbb{Z})^\vee$.

The map $4 \cdot G$ is then exactly the Cayley-Klein resolvent map F.

We end with a couple of exercises.

Exercise 16 Give examples of quadruples of quinary alternating 2-forms corresponding to some examples of quintic rings.

Exercise 17 (*) Can you find a parametrization space for quintic rings with some special structure (as in Exercise 13)?

References

[1] M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Ann. of Math.* **159** (2004), no. 1, 217–250.

[2] M. Bhargava, Higher composition laws II: On cubic analogues of Gauss composition, *Ann. of Math.* **159** (2004), no. 2, 865–886.

[3] M. Bhargava, Higher composition laws III: The parametrization of quartic rings and fields, *Ann. of Math.* **159** (2004), no. 3, 1329–1360.

[4] M. Bhargava, Higher composition laws IV: The parametrization of quintic rings and fields, *Ann. Math.* **167** (2008), no. 1, 53–94.

[5] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[6] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), 105–169.