CUBIC RINGS AND FORMS

ILA VARMA

The study of the link between integral forms and rings that are free of finite rank as $\mathbb{Z}$-modules is generally motivated by the study and classification of such rings. Here, we see what the ring structure can tell us about representation of integers by certain forms, particularly in the case of cubics. This lecture is derived from a question posed by Manjul Bhargava at the Arizona Winter School on quadratic forms in March 2009.

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

The usual example for rings of rank n will be orders in number fields of degree n. However, note that these rings are a priori also integral domains, i.e. not the most generic of examples.

In studying all rings of rank n, the basic question to ask is how one can classify them (up to ring isomorphism) for a fixed rank. As we will see, the answer for small n is very much related to integral binary forms.

1. $n < 3$

For $n = 0$, we have the zero ring consisting of 1 element, the additive and multiplicative identity. For $n = 1$, the free $\mathbb{Z}$-module structure restricts us to having only one possibility, $\mathbb{Z}$. The story becomes a bit more interesting for $n = 2$.

To start as simply as possible, note that the information on the structure of a unique (up to isomorphism) ring of rank 2 is in its multiplication table. Let Q be an arbitrary ring, and let $\langle 1, \tau \rangle$ be a $\mathbb{Z}$-basis. For some $b, c \in \mathbb{Z}$,

$$\tau \cdot \tau = b\tau + c.$$

We can put further restrictions on b and c as follows. If b is even, let $b = 2k$. Then

$$(\tau - k)^2 = \tau^2 - 2k\tau + k^2 = b\tau + c - 2k\tau + k^2 = c + k^2 \in \mathbb{Z}$$

Thus, we can assume that $\tau^2 \in \mathbb{Z}$ since $\langle 1, \tau - k \rangle$ is another $\mathbb{Z}$-basis for S. If b is odd, let $b = 2k + 1$. Then

$$(\tau - k)^2 = \tau^2 - 2k\tau + k^2 = b\tau + c - 2k\tau + k^2 = \tau + (c + k^2)$$

Similarly, we can assume that $\tau^2 = \tau + n$ with $n \in \mathbb{Z}$. We can conclude that $b = 0, 1$ and use the integral part of τ^2 to characterize the types of quadratic rings.

$$\{\text{quadratic rings } Q\} \,/\sim \quad \overset{1-1}{\longleftrightarrow} \quad \{\tau^2 = c \text{ or } \tau^2 = \tau + c \quad c \in \mathbb{Z}\} \quad \overset{disc}{\longleftrightarrow} \quad \mathbb{D} = \{D \in \mathbb{Z} : D \equiv 0, 1 \bmod 4\}$$

$$\begin{array}{ccccc} [Q] & \longmapsto & \tau^2 = c \text{ or } \tau + c & \longmapsto & 4c \text{ or } 4c+1 \\ \left[\mathbb{Z}[\frac{D+\sqrt{D}}{2}]\right] & \longmapsto & \tau^2 = \frac{D}{4} \text{ or } \tau^2 = \tau + \frac{D-1}{4} & \longmapsto & D \equiv 0 \bmod 4 \text{ or } D \equiv 1 \bmod 4 \end{array}$$

One can check that this correspondence does not depend on the choice of basis. Thus, we see that isomorphism classes of quadratic rings can be enumerated by the integers that are congruent to 0 or 1 mod 4. The map between such rings Q and these integers is the *discriminant map.* Thus, we have just seen that the discriminant, which is an invariant of any ring of rank n, is a *complete* invariant for $n = 2$, i.e. a quadratic ring is completely determined (up to isomorphism) by its discriminant.

2. Rings of Rank 3

Next, we try to classify rings of rank 3 in two analogous manners, first using the multiplication table, and then using the discriminant (when S is an order). Let S be a cubic ring with $\mathbb{Z}$-basis $\langle 1, \alpha, \beta \rangle$. Note first

we can assume that $\alpha\beta \in \mathbb{Z}$ by exchanging α, β with suitable $\mathbb{Z}$-translations. From the multiplication table, there exists $a, b, c, d, n, m, l \in \mathbb{Z}$ such that

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

Using associativity of multiplication for 3 elements, we can conclude that

$$n = -ac \quad m = -bd \quad l = -ad$$

Thus, the quadruple (a, b, c, d) can be associated to the ring structure of S. Conversely, if we start with (a, b, c, d) we can produce a ring with the above multiplication table using the formulas for n, m, l in terms of the quadruple. However, the quadruples do not treat potential isomorphisms between rings so nicely, hence we replace (a, b, c, d) with the binary cubic form

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

We have a twisted action of $\mathrm{GL}_2(\mathbb{Z})$ on such integral binary cubic forms:

$$\gamma(p)(x, y) = \frac{p\left((x, y) \cdot \gamma\right)}{\det(\gamma)} \quad \forall \gamma \in \mathrm{GL}_2(\mathbb{Z}).$$

Under the given correspondence of forms $f(x, y)$ and cubic rings S, $\mathrm{GL}_2(\mathbb{Z})$-equivalences of cubic forms naturally coincide with ring isomorphisms. We see this by considering two isomorphic rings S_1 and S_2 with bases $\langle 1, \alpha_1, \beta_1 \rangle$ and $\langle 1, \alpha_2, \beta_2 \rangle$. If we project the ring isomorphism to the quotient rings $S_i/\mathbb{Z} = \langle \alpha_i, \beta_i \rangle$, we can represent the map by an element of $\mathrm{GL}_2(\mathbb{Z})$ (and its inverse). This same matrix will give the equivalence between associated $f_1(x, y)$ and $f_2(x, y)$. Thus, we get the following equivalence (due to Delone-Faddeev in the case of integral domains, and generalized by Gan-Gross-Savin to arbitrary cubic rings):

$$\{\text{cubic rings } S\}/\sim \quad \overset{1-1}{\longleftrightarrow} \quad \{\text{integral binary cubic forms }\}/\,\mathrm{GL}_2(\mathbb{Z})\text{-equivalence}$$

Interpretation via resolvent rings. To every ring S, we can naturally associate a quadratic "resolvent" ring via the discriminant map. Recall that there is a unique (up to isomorphism) quadratic ring attached to each $D \in \mathbb{D}$. Hence, we associate to S the quadratic ring Q such that $\mathrm{disc}(S) = \mathrm{disc}(Q)$. However, we have not yet defined the discriminant map in the case of rings of rank greater than 2.

For an arbitrary ring R, if $\alpha \in R$, consider the $\mathbb{Z}$-linear transformation on R defined by multiplication by α,

$$\cdot\alpha : R \to R$$

which we can represent by a matrix $A_\alpha \in M_n(R)$. Define the trace and norm of an element α by

$$\mathrm{Tr}(\alpha) := \mathrm{Tr}(A_\alpha) \quad \text{and} \quad N(\alpha) := \det(A_\alpha).$$

We can also define a bilinear form

$$R \times R \longrightarrow \mathbb{Z} \qquad (x, y) \mapsto \mathrm{Tr}(xy)$$

If $\langle \alpha_0, \alpha_1, ..., \alpha_{n-1} \rangle$ is a $\mathbb{Z}$-basis for R, then

$$\mathrm{disc}(R) = \det\left(\{\mathrm{Tr}(\alpha_i\alpha_j)\}_{0 \le i,j \le n-1}\right).$$

Note that this is equivalent to defining the discriminant in terms of the corresponding quadratic form $\mathrm{Tr}(x^2)$ for elements $x \in R$. One important property due to Stickelberger is that this discriminant is always 0 or 1 mod 4.

For a cubic ring S, let Q be the (equivalence class of) quadratic ring such that $\mathrm{disc}(S) = \mathrm{disc}(Q)$. We call Q the *quadratic resolvent* of S. We can produce a map (not necessarily linear)

$$\varphi : S \longrightarrow Q \qquad x \mapsto \frac{\mathrm{disc}(x) + \sqrt{\mathrm{disc}(x)}}{2}$$

When S is an order, we define the discriminant of an element as follows: $x \in S$ has Galois conjugates x, x', x'' in the Galois closure of the fraction field of S, thus we can define

$$\mathrm{disc}(x) := (x - x')^2(x' - x'')^2(x'' - x)^2$$

The reason we are interested in φ is because it is discriminant-preserving, i.e. the product of pairwise differences of the conjugates of x is equal to their discriminant in Q. Furthermore, we can project φ down to a map

$$\overline{\varphi} : S/\mathbb{Z} \longrightarrow Q/\mathbb{Z}$$

which is well-defined. Note that $S/\mathbb{Z} \cong \mathbb{Z}^2$ and $Q/\mathbb{Z} \cong \mathbb{Z}$ as $\mathbb{Z}$-modules, so we can represent $\overline{\varphi}$ in terms of $\mathbb{Z}$-bases (if we choose our bases for $S = \langle 1, \alpha, \beta \rangle$ and $Q = \langle 1, \tau \rangle$, then $S/\mathbb{Z} = \langle \alpha, \beta \rangle$ and $Q/\mathbb{Z} = \langle \tau \rangle$). The fact that φ preserves discriminants gives that $\overline{\varphi}$ is a cubic map, hence $\overline{\varphi}(x, y) := \overline{\varphi}(x\alpha + y\beta)$ is a homogeneous polynomial of degree 3, hence a cubic form. It is not hard to check that this is the same integral binary cubic form $f(x, y)$ from the above correspondence.

Remark. Using the name *quadratic resolvent ring* stays true to the field analogy of quadratic resolvent fields to cubic fields, which gave rise to the classical solution of cubic equations.

We can briefly describe other interpretations of this Delone-Faddeev-Gan-Gross-Savin correspondence. In each of these, we distinctly derive the integral binary cubic form associated to a given cubic ring S in a manner that is well-defined up to ring isomorphism (and analogously, up to $\mathrm{GL}_2(\mathbb{Z})$-equivalences of the forms)

(1) Multiplication table of S written in terms of good $\mathbb{Z}$-basis $\langle 1, \alpha, \beta \rangle$ gives coefficients a, b, c, d of cubic form.
(2) We can define a map $S/\mathbb{Z} \longrightarrow \bigwedge^3 S$ which sends an element $s \mapsto 1 \wedge s \wedge s^2$ (recall that since S is rank 3, $\bigwedge^3 S \cong \mathbb{Z}$). If we think of $S/\mathbb{Z}$ as a free rank-2 $\mathbb{Z}$-module, this cubic map gives rise to the form $f(x, y)$.
(3) If S is an order, the map derived from the quadratic resolvent ring Q, $\overline{\varphi} : S/\mathbb{Z} \longrightarrow Q/\mathbb{Z}$ gives $(x, y) \longmapsto f(x, y)$.
(4) Again assume S is an order. For any element $s = x\alpha + y\beta + z$ of S (with good $\mathbb{Z}$-basis $\langle \alpha, \beta, 1 \rangle$),

$$f(x, y) = \sqrt{\frac{\mathrm{disc}(s)}{\mathrm{disc}(S)}}$$

(5) For $s \in S$ as in (4), consider the ring $\mathbb{Z}[s] = \langle 1, s, s^2 \rangle$. Then the index of $\mathbb{Z}[s]$ inside S gives the form, i.e. if $s = x\alpha + y\beta + z$, then $f(x, y) = \mathrm{Ind}_R(s)$.

Remark. Note that the discriminant of the ring S is the discriminant of the cubic form associated to f, and can be written explicitly in terms of the coefficients a, b, c, d :

$$\mathrm{disc}(S) = \mathrm{disc}(f) = b^2c^2 - 4ac^3 - 4db^3 - 27a^2d^2 + 18abcd$$

It is also true that if we consider the curve $C = \{f(x, y) = 0\}$ in $\mathbb{P}^1$, then the cubic ring S is contained in the field generated by the coordinates of points on C.

We now want to see what properties the relationship described above tells us about corresponding rings and forms.

Facts. (1) S is an order in a number field if and only if f is irreducible as a polynomial over $\mathbb{Q}$. (note that S is an order if and only if it is an integral domain)
(2) If f has nonzero discriminant, then S has automorphism group inside S_3. If f is irreducible over $\mathbb{Q}$, then S has automorphism group inside C_3.

We can also characterize which cubic rings have automorphism ring isomorphic to C_3 by analyzing the quadratic form $\mathrm{Tr}(x^2)$ on the traceless part of S.

Our main question is to see what we can say about integers represented by a binary cubic form using this associated ring S. We start with an example involving my favorite C_3-cubic field.

Example. Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ which is index 2 inside $\mathbb{Q}(\zeta_7)$, a cyclic extension of degree 6 over $\mathbb{Q}$. It is a well-known fact that $\mathcal{O}_K = \mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$. The minimal polynomial for K is $f(x) = x^3 + x^2 - 2x - 1$, and using $\zeta_7 + \zeta_7^{-1}$ as one of the basis elements gives $f(x, 1) = x^3 + x^2 - 2x - 1$. Homogenizing gives us the associated binary cubic form

$$f(x, y) = x^2 + x^2y - 2xy^2 - y^3.$$

Question. What primes p are represented by $f(x, y)$?

Assume there exists $x, y \in \mathbb{Z}$ such that $p = x^3 + x^2y - 2xy^2 - y^3$. Then $0 \equiv x^3 + x^2y - 2xy^3 - y^3 \pmod{p}$ has a nontrivial solution. This implies that $p \mid x, y$ or p is NOT inert in K.

(Recall that the splitting of a prime p is related to how the minimal polynomial factors mod p. If p splits, then $f(x, y)$ should factor mod p. Thus, only when p stays inert do we have no solutions mod p.)

If $p \mid x, y$, then $p^3 \mid f(x, y)$ by homogeneity, a contradiction. If p is inert in K, then there is no nontrivial solution to $0 = x^3 + x^2 - 2x - 1 \pmod{p}$. Thus, we can look at the ramification and splitting behavior to describe which primes can be represented by $f(x, y)$.

Facts. Since $\text{disc}(K) = 49$, the only prime which ramifies is 7. Furthermore, p splits completely if and only if $p = \pm 1 \bmod 7$ since $\mathbb{Q}(\zeta_7)$ is the ray class field of conductor 7 and $K = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$ is of index 2 with the nontrivial Galois automorphism being complex conjugation.

Thus, the only primes which can possibly be represented are 7 or of the form $p = \pm 1 \bmod 7$. The natural next question is whether or not the converse is true. It is easy to see that $7 = f(2, 1)$. We can also find integral pairs (x_0, y_0) for each $p < 211$ such that $p \equiv \pm 1 \bmod 7$. No other primes are represented (as expected), but $p = 211$ is also not represented. We checked this by evaluating f for enough integral pairs (x, y), up to a coarse bound using Pari and Sage (with the help of Henri Cohen).

In the general picture of cubic orders, if there exists a root of $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^2 \equiv 0 \pmod{p}$, a suitable change of variables allows us to assume that the root is 0, i.e. $x \mid f(x, y)$, thus $p \mid d$.

Consider the multiplication table on $S = \langle 1, \alpha, \beta \rangle$:

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

Consider the span $\langle 1, p\alpha, \beta \rangle$. This has index p, but is it a subring? Yes!

$$\begin{aligned} (p\alpha)^2 &= p^2n + pb \cdot p\alpha - p^2a\beta \\ \beta^2 &= m + \frac{d}{p} \cdot p\alpha - c\beta \qquad (\text{recall } p \mid d) \\ (p\alpha)\beta &= pl \end{aligned}$$

Remark. When S has full autmorphism group C_3, there are 3 index-p subrings constructed by producing this span and applying automorphisms.

Theorem 1. *There exists a monogenic index-p subring of S (i.e. generated by $\langle 1, s, s^2 \rangle$) if and only if p is representable by the associated cubic form $f(x, y)$.*

Proof. Think of $f(x, y) = \sqrt{\text{disc}(s)/\text{disc}(S)}$ for $s = x\alpha + y\beta + z$. If $\langle 1, p\alpha, \beta \rangle$ is monogenic, then we can find an element $s_0 \in S$ such that another basis for the index-p subring is $\langle 1, s_0, s_0^2 \rangle = \mathbb{Z}[s_0]$. Then $\text{Ind}_S(\mathbb{Z}[s_0]) = p$, thus if $s_0 = x_0\alpha + y_0\beta + z_0$, $f(x_0, y_0) = p$.

Conversely, if $p = f(x_0, y_0)$ for some $x_0, y_0 \in \mathbb{Z}$, then write $s = x_0\alpha + y_0\beta$. We know that $f(x, y) = \text{Ind}_S(\mathbb{Z}[s]) = p$. □

In our example, the only monogenic index p subrings of $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ that can exist are for $p = 0, \pm 1 \bmod 7$, and in fact, they come in triplets since this has automorphism group isomorphic to C_3. From our computations, we know that there does not exist a monogenic subring of index 211.

Remark. We also know that S is monogenic of the form $\mathbb{Z}[s]$ if and only if it represents 1. (Assume $S = \mathbb{Z}[s]$ where $s = x\alpha + y\beta + z$. Then $f(x, y) = \text{Ind}_S(\mathbb{Z}[s]) = 1$. Similarly, if $f(x, y)$ represents 1, then we can produce a $\mathbb{Z}$-generator $x_0\alpha + y_0\beta$ of the ring using the existance of an integral pair such that $f(x_0, y_0) = 1$.)