ON CUBIC RINGS AND QUATERNION RINGS

BENEDICT H. GROSS AND MARK LUCIANOVIC

In this paper, we show that the orbits of some simple group actions parametrize cubic rings and quaternion rings.

Let R be either a local ring or a principal ideal domain. A cubic ring A over R is, by definition, a commutative, associative R-algebra with unit, which is free of rank 3 as an R-module. We will show that the isomorphism classes of cubic rings over R correspond bijectively to the orbits of the group $\mathrm{GL}_2(R)$ acting on a free R-module M of rank 4. This action is faithful, and arises from a twist of the usual action on binary cubic forms. The case when $R = \mathbb{Z}$ was treated in [DF, §15] for non-zero discriminants, and in [GGS, §4] in general.

A quaternion ring A over R is, by definition, an associative R-algebra with unit, which is free of rank 4 as an R-module. We further require A to have an anti-involution $\alpha \mapsto \alpha^*$ fixing R, with $t_A(\alpha) = \alpha + \alpha^*$ and $n_A(\alpha) = \alpha\alpha^* = \alpha^*\alpha$ in R. Then α satisfies the quadratic polynomial

$$f_\alpha(x) = x^2 - t_A(\alpha)x + n_A(\alpha)$$

over R. Finally, we insist that the characteristic polynomial of left multiplication by α on A is equal to $f_\alpha(x)^2$.

We will show that the isomorphism classes of quaternion rings over R correspond bijectively to the orbits of the group $\mathrm{GL}_3(R)$ acting on a free R-module M of rank 6. The action is faithful, and arises from a twist of the usual action on ternary quadratic forms. The correspondence for forms of non-zero discriminant was first made explicit in [Lat], [Bra], and [Pal] (following [H]) in the case $R = \mathbb{Z}$, where the corresponding quaternion rings are orders in rational quaternion algebras; see [Llo] for a recent survey of this case. In this paper, as previously in [L], the correspondence is described in a uniform manner for forms of arbitrary discriminant; the condition on the characteristic polynomial was suggested by M. Bhargava, and it simplifies the final results.

1. Free R-algebras of finite rank

We recall that R is either a local ring or a principal ideal domain. Let A be an associative R-algebra with unit, which is free of rank $n \geq 1$ as an R-module. Let 1 denote the unit element of A, and consider the R-module homomorphism $f : R \to A$ mapping r to $f(r) = r \cdot 1$.

Lemma 1.1. *The map f is an injection, and the quotient R-module $A/(R \cdot 1)$ is free of rank $(n - 1)$.*

Proof. If $f(r) = 0$, then $r \cdot a = r \cdot (1 \cdot a) = (r \cdot 1) \cdot a = 0 \cdot a = 0$ for any a in A. Hence r annihilates A. Since the R-action on a non-zero free R-module is faithful, $r = 0$.

Now assume R is local, with maximal ideal $\mathfrak{m}$. Let $k = R/\mathfrak{m}$ be the quotient field, and let $\mathfrak{m}A$ be the associated sub-module of A. Then $V = A/\mathfrak{m}A$ is a k-vector space of dimension n. We claim that $1 \pmod{\mathfrak{m}}$ is a non-zero vector in V. If not, 1 lies in $\mathfrak{m}A$. Since $a = 1 \cdot a$, this would imply that $A = \mathfrak{m}A$, which by Nakayama's Lemma implies that $A = 0$, a contradiction.

Since $1 \neq 0$ in V, we can extend it to a basis $\langle 1, v_2, v_3, \dots, v_n\rangle$ of V over k. Lift these vectors to elements $\langle 1, a_2, \dots, a_n\rangle$ of A. By Nakayama's Lemma, these lifts give an R-basis for A. Hence $\langle a_2, \dots, a_n\rangle$ give an R-basis for the quotient $A/(R\cdot 1)$.

The case when R is a principal ideal domain is similar. $\square$

2. Cubic rings

Let R be a local ring or a principal ideal domain, and let N be a free R-module of rank 2. We will identify the orbits of the group $\mathrm{Aut}(N) \simeq \mathrm{GL}_2(R)$ acting on the R-module $M = \mathrm{Sym}^3(N) \otimes (\bigwedge^2 N)^{-1}$ with the isomorphism classes of cubic rings A over R.

The module M is free of rank 4, and can be identified with the binary cubic polynomials on $N = Re_1 + Re_2$, with a group action twisted by $(\bigwedge^2 N)^{-1}$. A binary cubic polynomial is an expression

$$p(e_1, e_2) = ae_1^3 + be_1^2 e_2 + ce_1 e_2^2 + de_2^3$$

with coefficients a, b, c, d in R. The discriminant $\Delta(p)$ of p is given by the formula:

$$\Delta = b^2c^2 + 18abcd - 4ac^3 - 4db^3 - 27a^2d^2.$$

The group $\mathrm{GL}_2(R)$ acts on M by the formula

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \quad p \mapsto g \cdot p = \frac{1}{\alpha\delta - \beta\gamma}\, p(\alpha e_1 + \gamma e_2, \beta e_1 + \delta e_2).$$

This action is faithful; the diagonal matrices $g = \begin{pmatrix} \alpha & \\ & \delta \end{pmatrix}$ have eigenvalues $\left(\frac{\alpha^2}{\delta}, \alpha, \delta, \frac{\delta^2}{\alpha}\right)$, and the center $g = \begin{pmatrix} \alpha & \\ & \alpha \end{pmatrix}$ acts by $g \cdot p = \alpha p$. Finally, we have

$$\Delta(g \cdot p) = (\det g)^2 \Delta(p).$$

Thus, orbits of cubic polynomials, for the twisted action of $\mathrm{GL}_2(R)$, have a well-defined discriminant in $R/(R^\times)^2$.

Associated to any p in M, we define a cubic ring over R with basis $\langle 1, i, j\rangle$ and multiplication rules

$$\begin{aligned} ij &= -ad, \\ i^2 &= -ac + bi - aj, \\ j^2 &= -bd + di - cj. \end{aligned}$$

We will now show that every cubic ring A has an R-basis whose multiplication laws take this simple form (we call this a *good basis* for A).

By Lemma 1.1, we may choose a basis $\langle 1, \omega_2, \omega_3 \rangle$ of A over R containing 1. Then for some r, s, t in R we may write

$$\omega_2\omega_3 = r + s\omega_2 + t\omega_3$$

(here and in the sequel, using Lemma 1.1, we write r in place of $r \cdot 1$). Let $i = \omega_2 - t$ and $j = \omega_3 - s$. Then $\langle 1, i, j \rangle$ is a basis for which the product

$$ij = r + st$$

lies in R. Write the products as

$$\begin{aligned} ij &= l, \\ i^2 &= m + bi - aj, \\ j^2 &= n + di - cj. \end{aligned}$$

The two associative laws $i^2 j = i(ij)$ and $ij^2 = (ij)j$ then imply that

$$\begin{aligned} l &= -ad, \\ m &= -ac, \\ n &= -bd. \end{aligned}$$

For example,

$$i(ij) = li, \qquad \begin{aligned} i^2 \cdot j &= (m + bi - aj)j \\ &= mj + bij - aj^2 \\ &= mj + bl - a(n + di - cj) \\ &= (bl - an) - adi + (m + ac)j. \end{aligned}$$

Equating coefficients of i and j gives the identities

$$\begin{aligned} l &= -ad, \\ m &= -ac. \end{aligned}$$

Similarly, the associative law $i \cdot j^2 = (ij)j$ implies the identity $n = -bd$. Hence, the multiplication laws for a good basis take the form described above, and every cubic ring A has a good basis.

The association of the multiplicative constants of a good basis to a cubic polynomial p thus establishes a map from cubic rings A with a good basis to binary cubic polynomials in M, and this map is surjective. A short calculation shows that a change of good basis has the form

$$\begin{pmatrix} 1 & 0 & 0 \\ u & \alpha & \beta \\ v & \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 \\ i \\ j \end{pmatrix} = \begin{pmatrix} 1 \\ i' \\ j' \end{pmatrix}$$

with $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $\mathrm{GL}_2(R)$; the binary cubic polynomial p' associated to $\langle 1, i', j' \rangle$ is equal to $g \cdot p$.[1] Hence we have proved the following.

[1]An observation of Bhargava (see [Bha]) helps shorten the calculation: for a cubic ring A, consider the cubic map $A/(R \cdot 1) \to \bigwedge^3 A \simeq R$ given by $\xi \mapsto 1 \wedge \xi \wedge \xi^2$; choosing a good basis for A reproduces its associated cubic form p, and the desired effect of basis change easily follows.

Proposition 2.1. *Let N be a free R-module of rank 2. There is a bijection between the set of orbits of the action of* $\mathrm{GL}(N) \simeq \mathrm{GL}_2(R)$ *on the R-module* $M = \mathrm{Sym}^3(N) \otimes (\bigwedge^2 N)^{-1}$ *and the set of isomorphism classes of cubic rings A over R.* $\square$

We note that the discriminant of the cubic ring A over R can be defined as a class in $R/(R^\times)^2$, using the trace form on a basis of A over R as in [GGS, §4]. This is equal to the discriminant of the orbit of p, as a class in $R/(R^\times)^2$.

This result can be extended to one over an arbitrary ring R, relating projective R-modules N of rank 2 with an element p in $\mathrm{Sym}^3(N) \otimes (\bigwedge^2 N)^{-1}$ to projective R-modules A of rank 3 with a commutative algebra structure.

3. Examples

We now give some examples of the correspondence in the previous section.

1. The form
$$p(e_1, e_2) = 0, \text{ with } \Delta = 0,$$
corresponds to the cubic ring
$$A = R + Ri + Rj$$
with $i^2 = j^2 = ij = 0$. Thus $A = R + I$, with $I^2 = 0$.

2. The form
$$p(e_1, e_2) = e_1^2 e_2 - e_2^2 e_1, \text{ with } \Delta = 1,$$
corresponds to the cubic ring
$$A = R + Ri + Rj$$
with $i^2 = i, j^2 = j, ij = 0$. The map taking
$$1 \mapsto (1, 1, 1), \ i \mapsto (1, 0, 0), \ j \mapsto (0, 1, 0),$$
gives an isomorphism of rings $A \simeq R^3$.

3. Finally, the form
$$p(e_1, e_2) = e_1^3 + be_1^2 e_2 + ce_1 e_2^2 + de_2^3, \text{ with } a = 1,$$
corresponds to the cubic ring
$$A = R + Ri + Rj$$
with $i^2 = -c + bi - j$ and $ij = -d$. Since $j = -i^2 + bi - c$, the ring A is generated by $\alpha = -i$ over R. Since
$$ij = -d = -i^3 + bi^2 - ci,$$
the element α satisfies the monic polynomial $x^3 + bx^2 + cx + d$, and
$$A = R[\alpha] \simeq R[x]/(x^3 + bx^2 + cx + d).$$
The discriminant Δ of p is equal to
$$b^2c^2 + 18bcd - 4c^3 - 4db^3 - 27d^2.$$
If $b = 0$, this simplifies to the classical formula $\Delta = -4c^3 - 27d^2$.

4. Quaternion Rings

Let N be a free R-module of rank 3. We will identify the orbits of the group $\mathrm{Aut}(N) = \mathrm{GL}(N) \simeq \mathrm{GL}_3(R)$ acting on the R-module $M = \mathrm{Sym}^2(N^\vee) \otimes \bigwedge^3 N$ with the isomorphism classes of quaternion rings A over R.

The R-module M is free of rank 6, and can be identified with the module of ternary quadratic forms, with a twisted group action. A ternary quadratic form over R is an expression

$$q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy$$

with coefficients a, b, c, u, v, w in R. The (half-)discriminant $\Delta(q)$ of q is given by

$$\Delta = 4abc + uvw - au^2 - bv^2 - cw^2.$$

The group $\mathrm{GL}_3(R)$ acts on the R-module M of all ternary quadratic forms by the formula:

$$g \cdot q(x, y, z) = (\det g) \cdot q(x', y', z'), \quad \text{where } g^{-1} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

This action is faithful; the diagonal matrices $g = \begin{pmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{pmatrix}$ act by

$$g \cdot q(x, y, z) = \frac{\beta\gamma}{\alpha} ax^2 + \frac{\alpha\gamma}{\beta} by^2 + \frac{\alpha\beta}{\gamma} cz^2 + \alpha uyz + \beta vxz + \gamma wxy$$

and the central elements $g = \begin{pmatrix} \alpha & & \\ & \alpha & \\ & & \alpha \end{pmatrix}$ act by $g \cdot q = \alpha q$. We have

$$\Delta(g \cdot q) = (\det g) \cdot \Delta(q).$$

Thus, orbits of forms for this twisted action of $\mathrm{GL}_3(R)$ have a notion of discriminant that is well defined as a class in $R/R^\times$.

Associated to $q(x, y, z)$ in M, we define a quaternion ring A over R with basis $\langle 1, i, j, k \rangle$ and multiplication laws:

$$\begin{aligned} i^2 &= ui - bc, \\ j^2 &= vj - ac, \\ k^2 &= wk - ab, \\ jk &= ai^*, \\ ki &= bj^*, \\ ij &= ck^*. \end{aligned}$$

We note that since $i^2 - ui + bc = 0$, we have $i + i^* = u$ and $ii^* = i^*i = bc$. Hence we find

$$\begin{aligned} i^* &= u - i, \\ j^* &= v - j, \\ k^* &= w - k. \end{aligned}$$

Also,

$$\begin{aligned}(ij)^* &= (ck^*)^* = ck \\ &= j^*i^* = (v-j)(u-i) = uv - uj - vi + ji.\end{aligned}$$

Hence

$$ji = -uv + vi + uj + ck.$$

We can calculate kj and ik in a similar manner. Finally, we have the formula

$$ijk = jki = kij = abc.$$

The quaternion ring A can be identified with the even part of the Clifford algebra of the quadratic space (N, q), where

$$N = Re_1 + Re_2 + Re_3,$$

and

$$q(xe_1 + ye_2 + ze_3) = q(x, y, z).$$

If

$$C^+(N, q) = R \cdot 1 + Re_2e_3 + Re_3e_1 + Re_1e_2$$

then i corresponds to e_2e_3, j to e_3e_1, and k to e_1e_2. (For example, since in a Clifford algebra $e_i^2 = q(e_i)$, we have $e_1e_2 + e_2e_1 = q(e_1 + e_2) - q(e_1) - q(e_2) = w$, and $ij = e_2e_3^2e_1 = q(e_3)e_2e_1 = c(w - e_1e_2) = c(w - k)$, etc.)

We now show that every quaternion ring A over R arises in this manner. Using the results of §1, we may choose a basis for A over R containing 1, which we denote $\langle 1, i, j, k\rangle$. Adding suitable constants to i, j, and k, we may arrange that the multiplication laws are given by:

$$\begin{aligned}
i^2 &= ui + l & &(\text{so } i^* = u - i)\\
j^2 &= vj + m & &(\text{so } j^* = v - j)\\
k^2 &= wk + n & &(\text{so } k^* = w - k)\\
jk &= -ai + r + \alpha k & &(\text{coeff of } j \text{ is } 0)\\
ki &= -bj + s + \beta i & &(\text{coeff of } k \text{ is } 0)\\
ij &= -ck + t + \gamma j & &(\text{coeff of } i \text{ is } 0)
\end{aligned}$$

We call such a basis a *good basis* for A over R.

The products kj, ik, and ji can be calculated using the anti-involution of A. For example,

$$(ki)^* = i^*k^* = (u - i)(w - k) = uw - wi - uk + ik,$$

but

$$(ki)^* = (-bj + s + \beta i)^* = -b(v - j) + s + \beta(u - i),$$

and hence

$$ik = bj + uk + (w - \beta)i + (s + \beta u - bv - uw).$$

The associativity of A implies the following relation on the structure coefficients for the multiplication of a good basis:

$$\begin{aligned}
l &= -bc, & r &= au,\\
m &= -ac, & s &= bv,\\
n &= -ab, & t &= cw.
\end{aligned}$$

For example, we have

$$j(kk^*) = (jk)k^*.$$

Since $kk^* = -n$, the left-hand side is equal to $-nj$. The right-hand side is equal to

$$(-ai + r + \alpha k)k^* = -ai(w-k) + r(w-k) - \alpha n.$$

Using the formula for ik above, we see that

$$-nj = abj + (au - r)k + (\text{constant})i + \text{constant}.$$

Hence, equating the coefficients of j and k, we find

$$n = -ab \text{ and } r = au.$$

The other identities are obtained in a similar fashion.

We have therefore obtained the following multiplication formulae of a good basis of A over R:

$$\begin{aligned} i^2 &= ui - bc \\ j^2 &= vj - ac \\ k^2 &= wk - ab \\ jk &= ai^* + \alpha k \\ ki &= bj^* + \beta i \\ ij &= ck^* + \gamma j \end{aligned}$$

To identify A with an even Clifford algebra, we must show that $\alpha = \beta = \gamma = 0$.

To do this, we use the observations above to calculate that the trace of the endomorphism "left multiplication by i" on A is equal to $2u + \gamma$. Since we insist, in the definition of a quaternion ring A, that the characteristic polynomial of this endomorphism is $(x^2 - ux + bc)^2$, its trace is equal to $2u$, and hence $\gamma = 0$. Considering the trace of left multiplication by j and k gives $\alpha = \beta = 0$. Hence, every quaternion ring has a good basis with multiplication given by the six constants a, b, c, u, v, w in R as in the algebra $A = C^+(N, q)$. This establishes a map from quaternion rings A with a good basis to ternary quadratic forms q in M, and this map is surjective.

The good bases for A over R form a principal homogeneous space for the group $\mathrm{GL}_3(R)$. A short calculation reveals that changing to another good basis for A gives the twisted action of $\mathrm{GL}_3(R)$ on the space of ternary forms; see [L] for an argument using the Clifford algebra structure.[2] Thus, we have established the following.

Proposition 4.1. *Let N be a free R-module of rank 3. There is a bijection between the set of orbits of the action of $\mathrm{GL}(N) \simeq \mathrm{GL}_3(R)$ on the R-module $M = \mathrm{Sym}^2(N^\vee) \otimes \bigwedge^3 N$ and the set of isomorphism classes of quaternion rings A over R.* □

---

[2] For a shorter calculation, consider the map $\phi : A/(R \cdot 1) \times A/(R \cdot 1) \to \bigwedge^4 A \simeq R$ given by $\phi(\sigma, \tau) = 1 \wedge \sigma \wedge \tau \wedge \sigma\tau$. This is a ternary quadratic form in each variable separately, and the properties of the anti-involution imply that $\phi(\sigma, \tau) = \phi(\tau, \sigma)$. Furthermore, $\phi(\sigma, \sigma) = 0$, and we find that ϕ determines a (ternary) quadratic map $\bigwedge^2(A/(R \cdot 1)) \to R$, for which it can be checked that a choice of good basis for A reproduces its associated form q. Changing good basis can then easily be seen to produce the twisted action on q.

There is a useful notion of "reduced discriminant" for quaternion rings, and we can show that under the above bijection, this notion corresponds to that of discriminant for the corresponding orbit of ternary quadratic forms. For a quaternion ring A, we define Δ_A to be the ideal of R generated by all values

$$\{x_1, x_2, x_3\} := t_A((x_1x_2 - x_2x_1)x_3^*) = (x_1x_2 - x_2x_1)x_3^* + x_3(x_1x_2 - x_2x_1)^*$$

for x_1, x_2, x_3 in A. By the properties of the anti-involution of A, the form $\{x_1, x_2, x_3\}$ is trilinear and alternating. It vanishes whenever any x_i lies in R, so it descends to a form on the rank-3 module $A/(R \cdot 1)$. It can be seen that if $\langle 1, i, j, k\rangle$ is a basis for A, then $\{i, j, k\}$ generates the ideal Δ_A; if this basis is in fact a good basis with multiplication rules corresponding to some form q, then it can be checked directly that

$$\{i, j, k\} = -\Delta(q).$$

Thus, as classes in $R/R^\times$, a generator of the ideal Δ_A matches the discriminant for the orbit of corresponding ternary quadratic forms. (Note: the square of the ideal Δ_A is the discriminant ideal of A in the usual sense, and $\Delta(q)^2$ is equal to $\operatorname{disc}(A/R)$ as classes in $R/(R^\times)^2$. For details, see [Brz].)

5. Examples

We now give some examples of the correspondence in §4.

1. The form

$$q(x, y, z) = 0, \text{ with } \Delta = 0,$$

corresponds to the quaternion ring

$$A = R + Ri + Rj + Rk$$

with good basis satisfying $i^2 = j^2 = k^2 = ij = jk = ki = 0$. This is isomorphic to the even exterior algebra $A = \bigwedge^0 N + \bigwedge^2 N$ on the rank-3 R-module N.

2. The form

$$q(x, y, z) = xy + yz + zx, \text{ with } \Delta = 1,$$

corresponds to the quaternion ring

$$A = R + Ri + Rj + Rk$$

with good basis satisfying $i^2 = i, j^2 = j, k^2 = k, jk = ki = ij = 0$. The map taking

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix},$$

identifies A with the ring $M_2(R)$ of 2×2 matrices over R.

3. Finally, the form

$$q(x, y, z) = ax^2 + by^2 + cz^2, \text{ with } \Delta = 4abc,$$

corresponds to the quaternion ring

$$A = R + Ri + Rj + Rk$$

with good basis satisfying

$$i^2 = -bc, \; j^2 = -ac, \; k^2 = -ab, \; jk = -ai, \; ki = -bj, \; ij = -bk.$$

The norm form on elements $Ri + Rj + Rk$ of trace zero in A is given by

$$bcX^2 + acY^2 + abZ^2.$$

If $a = b = c = -1$ and R is the field of real numbers, A is isomorphic to Hamilton's quaternions.

6. The Gorenstein condition

In both the cubic and quaternion case, the ring A is Gorenstein over R (in the sense that the A-module $\mathrm{Hom}(A, R)$ is locally free of rank 1) if and only if the cubic or quadratic form is primitive (in the sense that the ideal generated by its coefficients is equal to R). For cubic rings, see [GGS, §5] for a proof. For quaternion rings, the Gorenstein condition was treated in [Brz] (generalizing a result in [Pet]) in the case of non-zero discriminants, and in [L, §1.9] in general.

For an alternate perspective, we present in this section a self-contained argument in the quaternion case. We will use the following observation about the odd part of the Clifford algebra for rank-3 quadratic spaces.

Proposition 6.1. *Let N be a free R-module of rank 3 and q be a ternary quadratic form. If $A = C^+(N, q)$ is the even part of the Clifford algebra of the quadratic space (N, q), then we have an isomorphism of A-modules*

$$\mathrm{Hom}(A, R) \simeq C^-(N, q).$$

Proof. Consider a form q with coefficients

$$q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy$$

as in §4. If we regard $N = Re_1 + Re_2 + Re_3$ as the degree-1 piece of the full Clifford algebra $C(N, q)$, then $N \subset C^-(N, q)$; now consider the pairing

$$[\ ,\ ] : C^+(N, q) \times C^-(N, q) \to C^-(N, q)/N \simeq R$$

induced by multiplication in $C(N, q)$. This gives an isomorphism of R-modules from $C^-(N, q)$ to $\mathrm{Hom}(C^+(N, q), R)$; for example, it is easily checked on Clifford basis elements that the basis

$$\langle 1, e_2e_3, e_3e_1, e_1e_2\rangle$$

of $A = C^+(N, q)$, is dual via the above pairing to the basis

$$\langle e_1e_2e_3 - ue_1 - we_3, e_1, e_2, e_3\rangle$$

of $C^-(N, q)$, if we associate $re_1e_2e_3 \pmod N$ to $r \in R$. Moreover, the pairing can be used to express the required $C^+(N, q)$-module structure as $[\sigma\tau, \theta] = [\sigma, \tau\theta]$, and this follows from the associativity of multiplication in $C(N, q)$. □

Remarks. The analogous statement is true for any quadratic module of odd rank. We also note that this result differs significantly from the case of binary quadratic forms $q(x, y) = ax^2 + bxy + cy^2$, where $A = C^+(N, q)$ is the quadratic ring of discriminant $D = b^2 - 4ac$, and $C^-(N, q)$ is the rank-1 A-module whose isomorphism class corresponds to $q(x, y)$.

In light of Proposition 6.1, we may now produce an efficient proof of the Gorenstein condition in the quaternion case.

Proposition 6.2. *The quaternion ring $A = C^+(N, q)$ is Gorenstein over R if and only if the quadratic form q is primitive.*

Proof. Suppose for simplicity that R is a local ring with maximal ideal $\mathfrak{m}$. (The case where R is a principal ideal domain is similar, via localizing at each prime.)

First, suppose $q \equiv 0 \pmod{\mathfrak{m}}$. Then the ring $A = C^+(N, q)$ is not Gorenstein over R, which we will establish by passing to quotients modulo $\mathfrak{m}$ and showing that the ring $A' = A/\mathfrak{m}A$ is not Gorenstein over $R/\mathfrak{m}$. Indeed, $A' = A/\mathfrak{m}A$ is isomorphic to the (commutative) ring

$$(R/\mathfrak{m})[i, j, k]/(i^2, j^2, k^2, ij, jk, ki),$$

an instance of Example 1 in §5; that is, A' is the even part of the Clifford algebra C' for the zero ternary form over $R/\mathfrak{m}$. Here, A' is in fact a local ring with maximal ideal $I = (i, j, k)$, satisfying $I^2 = 0$. The ideal I acts via multiplication on the odd part $(C')^-$ of C', and it is easily checked that here $I(C')^-$ is just the degree-3 piece of the Clifford algebra. Thus, the quotient $(C')^-/I(C')^-$ is of dimension 3 over $R/\mathfrak{m}$; however, A'/I has dimension 1 over $R/\mathfrak{m}$. Thus, the A'-module $\mathrm{Hom}(A', R/\mathfrak{m})$, isomorphic to $(C')^-$, is not free, and the local ring A' is not Gorenstein over $R/\mathfrak{m}$.

To show that the primitivity of q implies $A = C^+(N, q)$ is Gorenstein, suppose that the form $q \not\equiv 0 \pmod{\mathfrak{m}}$; we will observe that $C^-(N, q)$ is a free A-module. In fact, it is easily checked that if, for example, $a \not\equiv 0 \pmod{\mathfrak{m}}$, then

$$C^-(N, q) = C^+(N, q) \cdot e_1;$$

if instead $a \equiv b \equiv c \equiv 0 \pmod{\mathfrak{m}}$ and $u \not\equiv 0 \pmod{\mathfrak{m}}$, then

$$C^-(N, q) = C^+(N, q) \cdot (e_2 + e_3).$$

The other cases are analogous, and thus the A-module $C^-(N, q)$ is always free of rank 1, as desired. $\square$

References

[Bha] M. Bhargava, Higher composition laws II: On cubic analogues of Gauss composition, *Annals of Math.* **159** (2004), 865–886.

[Bra] H. Brandt, Zur Zahlentheorie der Quaternionen, *Jber. Deutsch. Math. Verein.* **53** (1943), 23–57.

[Brz] J. Brzeziński, A characterization of Gorenstein orders in quaternion algebras, *Math. Scand.* **50** (1982) no. 1, 19–24.

[DF] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of math. monographs 10 (1964).

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

[H] C. Hermite, Sur la théorie des formes quadratiques, *J. reine angew. Math.* **47** (1854), 307–342.

[Lat] C. G. Latimer, The classes of integral sets in a quaternion algebra, *Duke Math. J.* **3** (1937), 237–247.

[Llo] P. Llorente, Correspondencia entre formas ternarias enteras y órdenes cuaterniónicos, *Rev. R. Acad. Cienc. Exactas Fís. Nat. (Esp.)* **94** (2000), no. 3, 397–416.

[L] M. Lucianovic, Quaternion rings, ternary quadratic forms, and Fourier coefficients of modular forms on PGSp_6, Ph.D. Thesis, Harvard University, 2003.

[Pal] G. Pall, On generalized quaternions, *Trans. Amer. Math. Soc.* **59** (1946), 280–332.

[Pet] M. Peters, Ternäre und quaternäre quadratische Formen und Quaternionenalgebren, *Acta Arith.* **15** (1968/1969), 329–365.