5. Structure of the cubic C-forms

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **46 (2000)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **28.04.2024**

LEMMA 4.8. *Suppose that* $C \otimes K$ *is étale over* K *and let* (M, F) *and* (M', F') *be cubic* C*-forms. Assume that the determining mappings* $q_F, q_{F'}$ *are nonzero. Then every* R*-linear isomorphism* $f\colon (M, F) \to (M', F')$ *is either* C*-linear or* C*-sesquilinear.*

Proof. The map f will induce an isomorphism of determining quadratic mappings of type C. We conclude by Proposition 2.3. $\square$

5. STRUCTURE OF THE CUBIC C-FORMS

We shall describe below the C-module structure of $S^3_C(M^*)$ and the corresponding C-isomorphism classes.

THEOREM 5.1. *Let* M *be a rank-one projective* C*-module. For each* $\phi \in \mathrm{Hom}_C(M_C^{\otimes 3}, C^*)$ *we define a cubic form by* $F_\phi(\mathbf{x}) = \phi(\mathbf{x} \otimes \mathbf{x} \otimes \mathbf{x})(1)$. *Then*

(i) *The correspondence* $\phi \mapsto F_\phi$ *is an isomorphism of* C*-modules* $\mathrm{Hom}_C(M_C^{\otimes 3}, C^*) \to S^3_C(M^*)$.

(ii) *The determining mapping* q_{F_ϕ} *is primitive if and only if* ϕ *is an isomorphism.*

(iii) *Two cubic* C*-forms* F *and* F_1 *on* M *are equivalent over* C *if and only if there exists* $c \in C^\times$ *such that* $F_1 = c^3 F$.

Proof. (i) This is a restatement of Proposition 3.7. The map $\phi \mapsto F_\phi$ is a C-isomorphism by definition of the structure of C-module on $S^3_C(M^*)$ in Section 3.

(ii) It is enough to prove our assertion locally, so we assume that M is free over C. Write $M = C\mathbf{m}$ for some $\mathbf{m} \in M$. Let $\lambda = \phi(\mathbf{m} \otimes \mathbf{m} \otimes \mathbf{m})$. Then we have $\phi(x\mathbf{m} \otimes y\mathbf{m} \otimes z\mathbf{m}) = \lambda(xyz)$. Let $\beta(y\mathbf{m}, z\mathbf{m}) = \lambda(yz)$ and observe that λ is a basis of C^* over C if and only if the symmetric bilinear form β is unimodular. We have

$$\begin{aligned} q_{F_\phi}(x\mathbf{m}) &= n(x) q_{F_\phi}(\mathbf{m}) \\ &= n(x) \wedge^2 \beta . \end{aligned}$$

It follows from this equality that q_{F_ϕ} is primitive if and only if β is unimodular, that is, if and only if ϕ is an isomorphism.

(iii) Let F and F_1 be cubic C-forms on M. Suppose that they are C-isomorphic. Then there exists $c \in C^\times$ such that $F_1 = F \circ l_c$. Let T be the symmetric trilinear form associated to F. Since $T(c\mathbf{x}, c\mathbf{y}, c\mathbf{z}) = T(c^3\mathbf{x}, \mathbf{y}, \mathbf{z})$, we get $F_1 = c^3 F$. Conversely, if $F_1 = c^3 F$ we may reverse these steps to conclude that $F_1 = F \circ l_c$ $\square$

We shall henceforth denote by $\mathrm{Cubic}_C(M)$ the set of C-isomorphism classes of cubic C-forms on M with primitive determining mapping. Recall that when M is an invertible C-module, there is a *unique* primitive quadratic mapping (M, q, N) of type C on M ([11]). If $F \in \mathrm{Cubic}_C(M)$, then necessarily

$$(M, q_F, \mathcal{D}(M)) = (M, q, N) \text{ in } H(C), \quad \text{and} \quad C = C^+(M, q_F, \mathcal{D}(M)),$$

by Corollary 4.7 (ii); in particular, all members of $\mathrm{Cubic}_C(M)$ have isomorphic determining mappings.

THEOREM 5.2. *Let M be a projective C-module of rank one.*

(i) *The set* $\mathrm{Cubic}_C(M)$ *is nonempty if and only if* $3[M] = [C^*]$ *in* $\mathrm{Pic}(C)$.

(ii) *If* $3[M] = [C^*]$ *in* $\mathrm{Pic}(C)$, *then the group* $C^\times/C^{\times 3}$ *acts simply transitively on the set* $\mathrm{Cubic}_C(M)$.

Proof. (i) By Part (ii) of Theorem 5.1, the module M admits a cubic C-form with primitive determining mapping if and only if there is an isomorphism $M_C^3 \to C^*$.

(ii) Since $M_C^{\otimes 3}$ and C^* are invertible C-modules, $\mathrm{Isom}_C(M_C^{\otimes 3}, C^*)$ is either empty or it is a torsor for $C^\times$ (i.e., a simply transitive $C^\times$-set). It is nonempty if and only if $\mathrm{Cubic}_C(M)$ is nonempty, by Part (i). Suppose this is so, and choose an isomorphism $\phi\colon M_C^3 \to C^*$. Each cubic C-form on M with primitive determining mapping is uniquely of the shape $F_{c\phi}$ with $c \in C^\times$ by Parts (i) and (ii) of Theorem 5.1. By Part (iii) of Theorem 5.1, the form $F_{c\phi}$ will be isomorphic with F_ϕ if and only if $c \in (C^\times)^3$. $\square$

We discuss next the relation between R-isomorphism and C-homomorphism of cubic forms.

Let $\mathrm{Cubic}_R(M)$ be the set of R-isomorphism classes of binary Gaussian cubic forms on M with primitive determining mapping of type C. Set

$$\mathcal{S}_R(C) = \coprod_{[M]} \mathrm{Cubic}_R(M) \quad \text{and} \quad \mathcal{S}(C) = \coprod_{[M]} \mathrm{Cubic}_C(M),$$

where $[M]$ runs over the elements of $\mathrm{Pic}(C)$ satisfying $3[M] = [C^*]$ and $\coprod$ means disjoint union.

The set $\mathcal{S}(C)$ carries a natural involution given by

$$[M,F] \mapsto \overline{[M,F]} := [\overline{M},F],$$

where $\overline{M}$ is defined as follows: $\overline{M} = M$ as R-modules with C acting by $c \cdot \mathbf{x} = \overline{c}\mathbf{x}$, where $c \mapsto \overline{c}$ is the canonical involution of C. This is well-defined because q_F depends only on the R-module structure of M, and it will be of type C for M if and only if it is so for $\overline{M}$ since $n(c) = n(\overline{c})$. Note that $[M,F] = \overline{[M,F]}$ if and only if (M,F) possesses a C-sesquilinear automorphism.

PROPOSITION 5.3. *With the previous notation we have*

(i) $\mathcal{S}_R(C) = \mathcal{S}(C)/\sim$, *where* $\sim$ *identifies* $[M,F]$ *with* $\overline{[M,F]}$.

(ii) *If* $[M] = [\overline{M}]$ *and* $3[M] = [C^*]$, *then* $\mathrm{Cubic}_C(M)$ *has an element* $[M,F_0]$ *fixed under the involution.*

(iii) *If* $[M] \neq [\overline{M}]$ *and* $3[M] = [C^*]$ *in* $\mathrm{Pic}(C)$, *then* $\mathrm{Cubic}_C(M) = \mathrm{Cubic}_R(M)$. *In particular,* $\mathrm{Cubic}_R(M)$ *is a simply transitive* $(C^\times/C^{\times 3})$*-set.*

Proof. (i) Let $\psi\colon (M,F) \to (M',F')$ be an R-isomorphism. Then ψ is an isomorphism of quadratic mappings $(M, q_F, \mathcal{D}(M)) \to (M', F', \mathcal{D}(M'))$. By Proposition 2.3, the map ψ is either C-linear or C-sesquilinear. Hence either $[M,F] = [M',F']$ or $[M,F] = \overline{[M',F']}$.

(ii) We start out with an element $[M,F] \in \mathcal{S}(C)$, which exists by hypothesis on M and by Theorem 5.2(i), and we choose a C-sesquilinear automorphism $\sigma\colon M \to M$. We know by Theorem 5.2 that all the C-forms on M are of the form wF with $w \in C^\times$. In particular $F\circ\sigma = wF$ for some $w \in C^\times$. An easy computation using (21) shows $(wF)\circ\sigma = \overline{w}(F\circ\sigma)$, so $F\circ\sigma^2 = \overline{w}wF$. Since σ^2 is C-linear, it follows from Theorem 5.2 that $\overline{w}w \in C^{\times 3}$. Using the fact that the cohomology of $\mathbf{Z}/2\mathbf{Z}$ with coefficients in a group of odd exponent (in this case $C^\times/C^{\times 3}$ with $\mathbf{Z}/2\mathbf{Z}$ acting via the canonical involution of C) is trivial, we conclude that $w = \overline{u}^{-1}uv^3$ for some $u, v \in C^\times$. Let $F_0 = uF$. By direct computation we have $F_0\circ\sigma = v^3F_0$; thus $\overline{[M,F]} = [M, F\circ\sigma] = [M,F]$ as claimed.

(iii) If $[M] \neq [\overline{M}]$, by Part (i), no two distinct elements of $\mathrm{Cubic}_C(M)$ can be identified in $\mathrm{Cubic}_R(M)$, that is, the canonical projection

$$\mathrm{Cubic}_C(M) \to \mathrm{Cubic}_R(M)$$

is a bijection. The second assertion follows from Theorem 5.2. $\square$

COROLLARY 5.4. *Let* $[M] \in \operatorname{Pic}(C)$ *be as in Part (ii) of Theorem 5.3. Let* $[M, F_0] \in \operatorname{Cubic}_C(M)$ *be a the fixed point of the involution. Then the map* $(C^\times/C^{\times 3}) \to \operatorname{Cubic}_C(M)$ *given by* $u \mapsto [M, uF_0]$ *is an isomorphism of* $\mathbf{Z}/2\mathbf{Z}$*-sets. In particular, this correspondence induces a bijection* $\operatorname{Cubic}_R(M) \simeq (C^\times/C^{\times 3})/\!\sim$*, where* $\sim$ *identifies* c *with* $\bar{c}$.

Proof. By Theorem 5.2, it is enough to show that the map $u \mapsto [M, uF_0]$ commutes with the action of $\mathbf{Z}/2\mathbf{Z}$ via the involutions. Let $\sigma\colon (\overline{M}, F_0) \to (M, F_0)$ be a C-isomorphism and let $u \in C^\times$. Since $(uF_0)\circ\sigma = \bar{u}(F_0 \circ \sigma)$, we have $\overline{[M, uF_0]} = [\overline{M}, uF_0] \overset{\sigma}{=} [M, (uF_0)\circ\sigma] = [M, \bar{u}(F_0 \circ \sigma)] = [M, \bar{u}F_0]$. □

The above proposition applies in particular to the case of fields. We can summarize our results in this case as follows:

PROPOSITION 5.5. *Let* K *be a field of characteristic not 2 or 3. Let* $\mathcal{S}_K$ *be the set of* K*-isomorphism classes of all binary cubic forms over* K *with nonzero discriminant. Then there is a natural partition*

$$\mathcal{S}_K = \coprod_C \operatorname{Cubic}_K(C)\,, \tag{25}$$

where C *ranges over the quadratic étale* K*-algebras and each* $\operatorname{Cubic}_K(C)$ *is in one-to-one correspondence with the quotient of* $C^\times/(C^\times)^3$ *by the involution* $c \mapsto \bar{c}$.

Proof. If K is a field then $\operatorname{Pic}(C) = 0$ for all quadratic K-algebras C. Each cubic form with nonzero discriminant will be a C-form for a unique quadratic étale algebra, namely the even Clifford algebra of its determining form, by Proposition 2.8 and Theorem 4.5. We finish by applying Proposition 5.3. □

As an illustration of these ideas, we prove a result known to L. E. Dickson [5, page 23]:

PROPOSITION 5.6. *Let* $K = \mathbf{F}_q$ *be a finite field with* q *elements, not of characteristic* 2 *or* 3. *Then the number of* $\mathbf{GL}_2(\mathbf{F}_q)$*-equivalence classes of binary cubic forms over* $\mathbf{F}_q$ *with nonzero discriminant is* 3 *if* $q \equiv 2 \mod 3$, *and is* 9 *if* $q \equiv 1 \mod 3$.

Proof. The étale quadratic algebras over $\mathbf{F}_q$ are

1. $C = \mathbf{F}_q \times \mathbf{F}_q$;
2. $C = \mathbf{F}_{q^2}$.

If $q \equiv 2 \bmod 3$, then $C^\times/(C^\times)^3$ is trivial in the first case and is $\mathbf{Z}/3\mathbf{Z}$ in the second case since $q^2 \equiv 1 \bmod 3$. In the second case the involution $c \to \bar{c}$ fixes the identity element of $C^\times/(C^\times)^3$ and interchanges the other two elements, giving 2 orbits on this. This gives $1+2$ orbits in total, so by Proposition 5.5, we have 3 isomorphism classes of binary cubic forms. If $q \equiv 1 \bmod 3$, then $C^\times/(C^\times)^3$ is $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ in the first case and is $\mathbf{Z}/3$ in the second case. In the second case, the Galois involution acts trivially, since $\mathbf{F}_q^\times/(\mathbf{F}_q{}^\times)^3 = C^\times/(C^\times)^3$. This gives 3 orbits. In the first case, the involution flips the two factors, and there are clearly 6 orbits. This gives a total of 9 orbits, and hence 9 cubic forms. $\square$

REMARK 5.7. When $R = K$ is a field of characteristic not 2 or 3, one can give an alternate description of $\mathcal{S}_R$. Since $\mathbf{GL}_2$ acts threefold transitively on $\mathbf{P}^1$, any binary cubic form with nonzero discriminant is equivalent over the separable closure of K with $\Phi = xy(x-y)$. Therefore, by the usual descent yoga, there is a canonical bijection

$$\mathcal{S}_K \simeq H^1(K, \mathrm{Aut}(\Phi)), \tag{26}$$

where $\mathrm{Aut}(\Phi)$ is the K-group scheme of automorphisms of Φ. The structure of $\mathrm{Aut}(\Phi)$ is easily worked out:

$$\mathrm{Aut}(\Phi) = \mu_3 \times S_3,$$

where S_3 is the symmetric group on 3 letters as a trivial Galois module; it corresponds to the stabilizer in $\mathbf{PGL}_2$ of the set of zeros of Φ in $\mathbf{P}^1$.

The signature $S_3 \to \mu_2$ induces a homomorphism $\delta\colon \mathrm{Aut}(\Phi) \to \mu_2$, which in turn induces a map in Galois cohomology

$$\delta_*\colon H^1(K, \mathrm{Aut}(\Phi)) \to H^1(K, \mu_2) = K^\times/K^{\times 2}. \tag{27}$$

Using (4) and the identification (26), we can show that

$$\delta_*(F) = -3D_F \in K^\times/K^{\times 2}.$$

Thus we can interpret the partition (25) as the partition on $H^1(K, \mathrm{Aut}(\Phi))$ given by the fibers of δ_*, the set $\mathrm{Cubic}_K(C)$ corresponding to the fiber $\delta_*^{-1}(-3D)$, where D is the discriminant of C.

When R is a PID we can give a more precise version of Theorem 5.2. In this case, C is a free R-module, and since $R1$ is a direct factor, $C = R \oplus R\omega = R[\omega]$ is a monogenic R-algebra. Therefore C^* is free of rank one over C (see Section 7), so the condition $3[M] = [C^*]$ of Theorem 5.2 reads simply $3[M] = 0$. Furthermore, since $\mathrm{Pic}\,(R) = 0$, the exact sequence (13) induces an isomorphism

$$G(C)[3] \simeq H(C)[3] = \mathrm{Pic}\,(C)[3] \tag{28}$$

(note that $R^\times / n(C^\times)$ is an elementary abelian 2-group).

The isomorphism (28) suggests that when R is a PID, it should be possible to use quadratic forms instead of quadratic mappings and develop a theory for binary cubic forms that is completely parallel to Eisenstein's theory over $\mathbf{Z}$. As we mentioned above, any projective R-module is free, so that a quadratic form (M, q) is the same thing as a quadratic form classically understood: a homogeneous polynomial of degree two. If q is of type C then $M = R^2$ becomes an invertible C-module. This C-module is said to be *associated to* q.

We begin by proving an easy technical lemma.

LEMMA 5.8. *Suppose that R is a UFD and let $C = R[t]/(t^2 + bt + c)$. Let $D = b^2 - 4c$ and let ω be the class of t in C. Set $\delta = b + 2\omega$ (note that $\delta^2 = D$) and let $\xi = x + y\delta$ with $x, y \in R$. If $n(\xi) \equiv 0 \pmod{4R}$, then $\xi \equiv 0 \pmod{2C}$.*

Proof. It is enough to prove $x \equiv by \pmod{2R}$. Let $p \in R$ be an irreducible element. For $z \in R - \{0\}$ we denote by $\mathrm{ord}_p(z)$ the largest power of p occurring in the factorization of z. Set $m = \mathrm{ord}_p(x - by)$. If $m < \mathrm{ord}_p(2)$ then, since ord_p is a valuation, $\mathrm{ord}_p(x + by) = \mathrm{ord}_p(x - by + 2by) = m$. Hence $\mathrm{ord}_p(x^2 - b^2y^2) = 2m < \mathrm{ord}_p(4)$, which contradicts our assumption (since $b^2 \equiv D \pmod{4R}$). Therefore $\mathrm{ord}_p(x - by) \geq \mathrm{ord}_p(2)$ for all irreducible p, which proves the lemma. □

Now we can prove:

PROPOSITION 5.9. *Let R be a PID and let F be a cubic form on $M = R^2$ given in the natural basis by (1), with coefficients $a_i \in R$. Suppose that its Eisenstein determining form $q_F(\mathbf{x}) = ax_1^2 + bx_1x_2 + cx_2^2$, as in (2), is primitive of discriminant $D \neq 0$ and let $C := C^+(q_F) = R[t]/(t^2 + bt + ac)$. Then $3[M, q_F] = 0$ in $G(C)$.*

Proof. By the syzygy (7) we have

$$4q_F(\mathbf{x})q_F(\mathbf{y})q_F(\mathbf{z}) = X^2 - DY^2,$$

where X and Y are symmetric R-trilinear forms in $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Applying the lemma to the rings $R' := R[x_1, x_2, y_1, y_2, z_1, z_2]$ and $C' := C \otimes_R R'$ with $\xi = X + \delta Y$ (with δ as in the lemma; the lemma applies since R, hence R', is a UFD), we have

$$q_F(\mathbf{x})q_F(\mathbf{y})q_F(\mathbf{z}) = n(T), \tag{29}$$

where $T = \xi/2 \in C'$, by the lemma. Note that T is symmetric trilinear in $\mathbf{x}, \mathbf{y}, \mathbf{z}$; hence the identity (29) shows that the triplication of q_F is the trivial form, as desired. $\square$

The results below were essentially known in the case $R = \mathbf{Z}$ to Eisenstein [6] and [7], Arndt [1], Pepin [13], Cayley [3] and Hermite [8].

THEOREM 5.10. *Let R be a PID. Let $q = ax_1^2 + bx_1x_2 + cx_2^2$ be a primitive binary quadratic form over R of discriminant $D = b^2 - 4ac \neq 0$. Let $C = C^+(q)$ be the even Clifford algebra of q and let $M := R^2$ be endowed with the natural C-module structure. Let $\tau \in C$ be such that $\tau + \overline{\tau} = 0$ and $\tau^2 = D$. With this notation we have*

(i) *There exists a Gaussian binary cubic form F such that $q_F = q$ (where q_F is given by (2)) if and only if $3[M, q] = 0$ in the group $G(C)$ of C-isomorphism classes of quadratic forms of type C.*

(ii) *If F and F' are Gaussian binary cubic forms with $q_F = q_{F'} = q$, then there exists a unit $c = a + b\tau \in C^\times$ with $n(c) = 1$ such that $F' = cF = aF + bG_F$, where G_F is the cubic covariant defined in (5).*

(iii) *Let two cubic forms F and F' with $q_F = q_{F'} = q$ be given. The following conditions are equivalent:*

   (a) *There exists $d \in C^\times$ with $n(d) = 1$ such that $F' = d^3F$.*

   (b) *There exists $d \in C^\times$ such that $F' = d^3F$.*

   (c) *F and F' are $\mathbf{SL}_2(R)$-equivalent.*

Proof. (i) By Proposition 5.9 the condition $3[M, q] = 0$ is necessary. We shall see that it is sufficient. Suppose $3[M, q] = 0$ in $G(C)$; in particular

$$3[M] = 0 \in \mathrm{Pic}\,(C),$$

thus by virtue of Theorem 5.2, Part (i), there exists a Gaussian cubic form F such that $[M, q_F, R] = [M, q, R]$ in $H(C)$. By Proposition 5.9, the class $[M, q_F]$ is in $G(C)[3]$; hence, by the isomorphism (28), we conclude $[M, q_F] = [M, q]$ in $G(C)$.

(ii) Suppose that $q_F = q_{F'} = q$. $C \otimes K$ is an étale K-algebra since $D \neq 0$. Hence by Corollary 4.7 both F and F' are C-forms and by Theorem 5.2, Part (ii), there exists $c \in C^\times$ such that $F' = cF = (\rho(c)/3)F$ (in the notation of (23)). Writing $c = a + b\tau$ we get $F' = aF + (b/3)(\rho(\tau)F)$. By (24) we have $\rho(\tau)F = 3G_F$ (changing the sign of τ if needed) and direct computation shows $q_{F'} = n(c)q_F$. Thus $n(c) = 1$ as required. Note that in general, the coefficients a, b will have a 2 in the denominator since $\tau = b + 2\omega$ for a generator ω of the algebra C (see Lemma 5.8).

(iii) a)$\Rightarrow$b) is trivial.

b)$\Rightarrow$c). If $F' = d^3F$ with $d \in C^\times$ then, by Part (ii) of Theorem 5.2, F and F' are C-equivalent, the isomorphism being $\mathbf{x} \to d\mathbf{x}$. We have $n(d)^3 = 1$ by the proof of Part (ii) of this theorem, so replacing d by $n(d)d$ we can assume $n(d) = 1$; that is, F and F' are $\mathbf{SL}_2(R)$-equivalent, and this also establishes the implication b)$\Rightarrow$a).

c)$\Rightarrow$a). If $F'(\mathbf{x}) = F(d\mathbf{x})$, where $d \in \mathbf{SL}_2(R)$, then d is in the orthogonal group of $q = q_F = q_{F'}$. Since $\det(d) = 1$, it is in the special orthogonal group of this form, hence given by multiplication by an element $d \in C_1^\times$ by Corollary 2.4. But $F(d\mathbf{x}) = (d^3F)(\mathbf{x})$. □

COROLLARY 5.11. *Now let $R = \mathbf{Z}$, and let D be a nonzero integer congruent to 0 or 1 modulo 4. Let F be an integral Gaussian binary cubic form with primitive determining form of discriminant D.*

(i) *Suppose $D < -3$. If F' is another Gaussian binary cubic form with $q_{F'} = q_F$ then F' is $\mathbf{SL}_2(\mathbf{Z})$-equivalent to F.*

(ii) *Suppose $D > 0$ or $D = -3$. Then there are exactly three $\mathbf{SL}_2(\mathbf{Z})$-equivalence classes of Gaussian binary cubic forms F' such that $q_{F'} = q_F$.*

Proof. We have that $C^+(q_F) = C_D$, the unique quadratic $\mathbf{Z}$-algebra of discriminant D. Note that $(C_D)_1^\times/(C_D)_1^{\times 3}$ is trivial when $D < -3$ and is cyclic of order 3 when $D = -3$ or $D > 0$. The corollary follows immediately from this and Parts (ii) and (iii) of Theorem 5.10. □

COROLLARY 5.12. *Let D be a nonzero integer congruent to 0 or 1 modulo 4. Let $h_3(D)$ be the number of $\mathbf{SL}_2(\mathbf{Z})$-equivalence classes if binary Gaussian cubic forms with primitive determining form of discriminant D. Then $h_3(D) = |\mathrm{Pic}\,(C_D)[3]|$ if $D < -3$ and $h_3(D) = 3|\mathrm{Pic}\,(C_D)[3]|$ if $D = -3$ or $D > 0$.*

Proof. Follows immediately from Corollary 5.11, equation (28) and Part (i) of Theorem 5.10. □

6. Cohomological Interpretation

Let $\mathbf{G}_m$ be the multiplicative group regarded as an affine group scheme over $X := \operatorname{Spec} C$ and let $\mu_3 \subset \mathbf{G}_m$ be the kernel of multiplication by 3. All the cohomology groups below are with respect to the flat topology on X.

THEOREM 6.1. *Suppose $[C^*]$ is divisible by 3 in* $\operatorname{Pic}(C)$. *Then the group $H^1_{\mathrm{fl}}(X, \mu_3)$ acts simply transitively on the set $\mathcal{S}(C)$ of C-equivalence classes of cubic C-forms with primitive determining mapping.*

Proof. Recall that the group $H^1_{\mathrm{fl}}(X, \mu_3)$ can be interpreted concretely as the set of isomorphism classes of pairs (L, ψ), where L is an invertible C-module and where $\psi \colon L_C^{\otimes 3} \to C$ is an isomorphism (see Milne [14, Chap. III, §4]). Let $[L, \psi]$ be an element of $H^1_{\mathrm{fl}}(X, \mu_3)$ and let (M, F) be a cubic C-form. By Theorem 5.1, Part (i), we can assume $F = F_\phi$, where $\phi \colon M^{\otimes 3} \to C^*$ is an isomorphism. We define an action of $H^1_{\mathrm{fl}}(X, \mu_3)$ on $\mathcal{S}(C)$ by

$$[L, \psi] \cdot [M, F_\phi] = [L \otimes M, F_{\psi \otimes \phi}], \tag{30}$$

noting that

$$(L \otimes M)_C^{\otimes 3} = L_C^{\otimes 3} \otimes M_C^{\otimes 3} \xrightarrow{\psi \otimes \phi} C \otimes C^* = C^*$$

is an isomorphism. Let us show first that this action is simple. Suppose $[L \otimes M, F_{\psi \otimes \phi}] = [M, F_\phi]$. Then, $L \cong C$. Choosing an isomorphism $L \to C$, we have $\psi(x \otimes y \otimes z) = uxyz$, where $u \in C^\times$. Hence $[M, F_\phi] = [M, F_{u\phi}]$, and by Part (iii) of Theorem 5.1 we conclude that $u = c^3$ for some $c \in C^\times$. But then $c \colon C \to C$ provides an isomorphism of (C, ψ) with $(C, 1)$, thus $[L, \psi] = [C, 1]$.

We show now that the action is transitive. Let $[M_i, F_{\phi_i}]$ $(i = 1, 2)$ be elements of $\mathcal{S}(C)$. Let $M_2^\bullet = \operatorname{Hom}_C(M_2, C)$ and let $\phi_2^\bullet : (C^*)^\bullet \to (M_2^{\otimes 3})^\bullet$ be the dual of ϕ_2. Let $L = M_1 \otimes M_2^\bullet$ and let $\psi = \phi_1 \otimes {\phi_2^\bullet}^{-1}$. One verifies immediately that $[L, \psi] \cdot [M_2, F_{\phi_2}] = [M_1, F_{\phi_1}]$, which proves that the action is transitive. □