

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 46 (2000)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ARITHMETIC OF BINARY CUBIC FORMS
Autor: HOFFMAN, J. William / MORALES, Jorge
Kapitel: 3. Cubic forms
DOI: <https://doi.org/10.5169/seals-64795>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 26.04.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

3. CUBIC FORMS

We shall assume henceforth that the ground ring R is an integral domain of characteristic not dividing 6. The field of fractions of R will be denoted by K as previously.

Let M be a projective R -module of rank 2, and let $M^* = \text{Hom}_R(M, R)$ be its dual. Consider the symmetric algebra

$$\text{Sym}_R(M^*) = \bigoplus_n \text{Sym}_R^n(M^*).$$

In this paper, a binary n -form is a pair (M, F) , where M is a projective R -module of rank 2, and $F \in \text{Sym}_R^n(M^*)$. A morphism $(M, F) \rightarrow (M', F')$ is an R -linear map $\phi: M \rightarrow M'$ such that $F'\phi = F$.

DEFINITION 3.1. An element $F \in \text{Sym}_R^n(M^*)$ will be called a *Gaussian n -form* if there is a symmetric n -linear form $T: M \times \cdots \times M \rightarrow R$ with $F(\mathbf{x}) = T(\mathbf{x}, \dots, \mathbf{x})$.

The set of Gaussian n -forms is a submodule of $\text{Sym}_R(M^*)$ and will be denoted by $S^n(M^*)$. The module $\text{Sym}_R^n(M^*)$ is projective of rank $n+1$ over R . If no binomial symbol $\binom{n}{i}$ is zero in R for $0 < i < n$, then $S^n(M^*)$ is also a projective R -module of rank $n+1$. If each of these binomial symbols is invertible in R then $S^n(M^*) = \text{Sym}_R^n(M^*)$. Note that for any R -homomorphism $M \rightarrow M'$, the induced map $\text{Sym}_R^n(M'^*) \rightarrow \text{Sym}_R^n(M^*)$ sends $S^n(M'^*)$ to $S^n(M^*)$.

In this section we shall concentrate on binary cubic forms ($n = 3$). Unless otherwise stated all the binary cubic forms we shall consider are assumed to be Gaussian forms.

Let $F \in S^3(M^*)$ and let T be the symmetric trilinear form such that $F(\mathbf{x}) = T(\mathbf{x}, \mathbf{x}, \mathbf{x})$. For fixed $\mathbf{x} \in M$ we consider the homomorphism

$$\begin{aligned} T_{\mathbf{x}}: M &\longrightarrow M^* \\ \mathbf{y} &\longmapsto [\mathbf{z} \rightarrow T(\mathbf{x}, \mathbf{y}, \mathbf{z})]. \end{aligned}$$

Applying the second alternating power functor \wedge^2 we get a homomorphism

$$\wedge^2 T_{\mathbf{x}}: \wedge^2 M \rightarrow \wedge^2 M^*,$$

thus an element of $\mathcal{D}(M) := \text{Hom}_R(\wedge^2 M, \wedge^2 M^*)$. We define

$$(14) \quad q_F(\mathbf{x}) := \wedge^2 T_{\mathbf{x}}.$$

It is immediate from the definitions that

$$(15) \quad (M, q_F, \mathcal{D}(M))$$

is a binary quadratic mapping in the sense of Section 2. It is also evident that if (M, F) is isomorphic to (M', F') , then $(M, q_F, \mathcal{D}(M))$ is isomorphic to $(M', q_{F'}, \mathcal{D}(M'))$.

DEFINITION 3.2. The quadratic mapping $(M, q_F, \mathcal{D}(M))$ is called the *determining mapping* of (M, F) .

By abuse of language, we shall refer sometimes to q_F as the determining mapping of F , without referring explicitly to the underlying modules M and $\mathcal{D}(M)$.

Over any open subset of $\text{Spec } R$ where M is free, the choice of a local basis $\mathbf{m} = \{\mathbf{m}_1, \mathbf{m}_2\}$ of M allows us to write

$$(16) \quad F(\mathbf{x}) = a_0x_1^3 + 3a_1x_1^2x_2 + 3a_2x_1x_2^2 + a_3x_2^3,$$

where $\mathbf{x} = x_1\mathbf{m}_1 + x_2\mathbf{m}_2$. Let $\mathbf{m}^* = \{\mathbf{m}_1^*, \mathbf{m}_2^*\}$ be the dual basis of M^* . An easy computation gives

$$T_{\mathbf{x}}(\mathbf{m}_1) = (a_0x_1 + a_1x_2)\mathbf{m}_1^* + (a_1x_1 + a_2x_2)\mathbf{m}_2^*,$$

$$T_{\mathbf{x}}(\mathbf{m}_2) = (a_1x_1 + a_2x_2)\mathbf{m}_1^* + (a_2x_1 + a_3x_2)\mathbf{m}_2^*.$$

In the bases $\mathbf{m}_1 \wedge \mathbf{m}_2$ for $\wedge^2 M$ and $-\mathbf{m}_1^* \wedge \mathbf{m}_2^*$ for $\wedge^2 M^*$ (note the sign change), the determining form q_F is given by

$$(17) \quad q_F(\mathbf{x}) = - \begin{vmatrix} a_0x_1 + a_1x_2 & a_1x_1 + a_2x_2 \\ a_1x_1 + a_2x_2 & a_2x_1 + a_3x_2 \end{vmatrix} \\ = (a_1^2 - a_0a_2)x_1^2 + (a_1a_2 - a_0a_3)x_1x_2 + (a_2^2 - a_1a_3)x_2^2,$$

which shows that (15) coincides locally with Eisenstein's determining form (2).

Now let C be a quadratic R -algebra as in Section 2 and let M be a projective C -module of rank one.

DEFINITION 3.3. Let $F \in S^3(M^*)$ and let T be the symmetric trilinear form associated to F . We will say that F is a C -form if $T(c\mathbf{x}, \mathbf{y}, \mathbf{z})$ is symmetric in $\mathbf{x}, \mathbf{y}, \mathbf{z}$ for any $c \in C$.

REMARK 3.4. The above definition makes sense for forms in $S^n(M^*)$ for any n . In particular, one has the notion of a quadratic C -form. This should not be confused with the concept of a quadratic form of type C . Indeed, it is easy to see that a quadratic form q is of type C if and only if the symmetric bilinear form b attached to q satisfies $b(c\mathbf{x}, \mathbf{y}) = b(\mathbf{x}, \bar{c}\mathbf{y})$; whereas the condition for a C -form reads $b(c\mathbf{x}, \mathbf{y}) = b(\mathbf{x}, c\mathbf{y})$.

We will use throughout the notation

$$M_C^{\otimes 3} = M \otimes_C M \otimes_C M, \quad M_R^{\otimes 3} = M \otimes_R M \otimes_R M.$$

Note that there is a natural epimorphism of R -modules $p: M_R^{\otimes 3} \rightarrow M_C^{\otimes 3}$. We have the following characterization of C -forms:

LEMMA 3.5. *Let $F \in S^3(M^*)$ and let T be the associated symmetric R -trilinear form, viewed as a linear form on $M_R^{\otimes 3}$. Then F is a C -form if and only if there exists a linear map $\lambda: M_C^{\otimes 3} \rightarrow R$ such that $T = \lambda \circ p$. Furthermore, the map λ is unique.*

Proof. It is enough to prove the lemma locally, so we assume that M is free over C .

Let $\lambda: M_C^{\otimes 3} \rightarrow R$ be an R -homomorphism. Write $M = C\mathbf{m}$ for some $\mathbf{m} \in M$ and let $\mathbf{x} = c_1\mathbf{m}$, $\mathbf{y} = c_2\mathbf{m}$, $\mathbf{z} = c_3\mathbf{m}$ with $c_i \in C$.

Then $T(\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z}) = \lambda(c_1c_2c_3(\mathbf{m} \otimes \mathbf{m} \otimes \mathbf{m}))$ is visibly symmetric and satisfies the condition of Definition 3.3.

Conversely, if $T(c\mathbf{x}, \mathbf{y}, \mathbf{z})$ is symmetric then in particular T itself is symmetric ($c = 1$), and hence

$$T(c\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(\mathbf{x}, c\mathbf{y}, \mathbf{z}) = T(\mathbf{x}, \mathbf{y}, c\mathbf{z}),$$

showing the existence of λ . Uniqueness follows from the fact that p is onto. \square

Let $S_C^3(M^*) \subset S^3(M^*)$ be the submodule of cubic C -forms on M . Note that the lemma above can be summarized by saying that the map

$$(18) \quad \begin{aligned} \text{Hom}_R(M_C^{\otimes 3}, R) &\longrightarrow S_C^3(M^*) \\ \lambda &\longmapsto [\mathbf{x} \mapsto \lambda(\mathbf{x} \otimes \mathbf{x} \otimes \mathbf{x})] \end{aligned}$$

is an isomorphism of R -modules.

On the other hand, we also have

LEMMA 3.6. *Let L be any projective C -module of finite rank. Then the map*

$$(19) \quad \begin{aligned} \text{Hom}_C(L, C^*) &\longrightarrow \text{Hom}_R(L, R) \\ f &\longmapsto (\mathbf{x} \mapsto f(\mathbf{x})(1)) \end{aligned}$$

is an isomorphism of C -modules (the dual $P^ = \text{Hom}_R(P, R)$ is made into a C -module by setting $(c\lambda)(x) = \lambda(cx)$ for $\lambda \in P^*$).*

Proof. By localization, it is sufficient to prove the lemma when $L = C$, in which case the map is the identity. \square

Combining the isomorphisms (18) and (19) with $L = M_C^{\otimes 3}$, we obtain

PROPOSITION 3.7. *The map*

$$(20) \quad \begin{aligned} \text{Hom}_C(M_C^{\otimes 3}, C^*) &\longrightarrow S_C^3(M^*) \\ \phi &\longmapsto [F_\phi: \mathbf{x} \mapsto \phi(\mathbf{x} \otimes \mathbf{x} \otimes \mathbf{x})(1)] \end{aligned}$$

is an isomorphism of R -modules.

Using the isomorphism (20) we give $S_C^3(M^*)$ the C -module structure so that this bijection becomes a C -module isomorphism. Note that

$$T_\phi(\mathbf{x}, \mathbf{y}, \mathbf{z}) := \phi(\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z})(1)$$

is the symmetric trilinear form attached to F_ϕ . Hence the C -module structure on $S_C^3(M^*)$ is given explicitly by

$$(21) \quad (cF)(\mathbf{x}) = T(c\mathbf{x}, \mathbf{x}, \mathbf{x}).$$

LEMMA 3.8. *C^* is an invertible C -module.*

Proof. Locally over $\text{Spec } R$, we have $C = R[\omega] = R[x]/(x^2 + bx + c)$. Then the R -module C^* is freely generated by λ_1, λ_2 , where $\lambda_1(1) = 1$, $\lambda_1(\omega) = 0$, $\lambda_2(1) = 0$, $\lambda_2(\omega) = 1$. One sees that $\omega\lambda_2 = \lambda_1 - b\lambda_2$, so that λ_2 is a local C -module basis of C^* . \square

By virtue of (20) and this lemma, $S_C^3(M^*)$ is an invertible C -module.

In the next section we will give alternate characterizations of the cubic C -forms on M , related to their determining mapping.