

Generalization of a theorem of Tankeev polynomials and difference sets

by RIBET, K. A.

in Seminaire de Théorie des Nombres de Bordeaux

volume 11; pp. 1 - 4



Göttingen State and University Library

Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Göttingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online-systems to access or download a digitized document you accept these Terms and Conditions.

Reproductions of materials on the web site may not be made for or donated to other repositories, nor may they be further reproduced without written permission from the Göttingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:

Niedersächsische Staats- und Universitätsbibliothek Göttingen

Digitalisierungszentrum

37070 Göttingen

Germany

E-Mail: gdz@www.sub.uni-goettingen.de

Purchase a CD-ROM

The Göttingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:

Niedersächsische Staats- und Universitätsbibliothek Göttingen

Digitalisierungszentrum

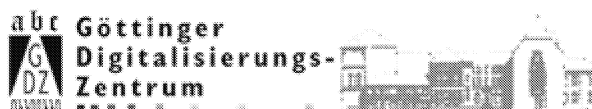
37070 Göttingen

Germany

E-Mail: gdz@www.sub.uni-goettingen.de



Göttingen State and University Library



GENERALIZATION OF A THEOREM OF TANKEEV

by

K. A. RIBET

Let E be a CM field, and let $2d$ be the degree of E over \mathbb{Q} . Let \mathcal{S} be the set of field embeddings $E \rightarrow \mathbb{C}$, and define W to be the free \mathbb{Q} -vector space on \mathcal{S} :

$$W = \left\{ \sum_{\sigma \in \mathcal{S}} n_{\sigma} \sigma \mid n_{\sigma} \in \mathbb{Q} \right\}.$$

We view W as a left G module, where $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $\bar{\mathbb{Q}}$ is the algebraic closure of \mathbb{Q} in \mathbb{C} . For each subset S of \mathcal{S} , we identify S with $\sum_{\sigma \in S} \sigma \in W$ and let W_S be the G -submodule of W generated by S .

Consider the special case where S is a CM type, a subset of \mathcal{S} such that \mathcal{S} is the disjoint union of S and its complex conjugate \bar{S} . We see easily that W_S is contained in

$$V = \left\{ \sum n_{\sigma} \sigma \in W \mid n_{\sigma} + n_{\bar{\sigma}} \text{ is independent of } \sigma \right\},$$

a $(d+1)$ -dimensional G -stable subspace of W . The CM types S for which

$W_S = V$ are called non-degenerate [1], [3]. To motivate interest in such S , we mention the following easily proved property that they possess : suppose that Δ is a subset of \mathfrak{S} such that all intersections

$$\Delta \cap g S \quad (g \in G)$$

have the same number of elements. Then Δ is stable under complex conjugation.

According to H. Pohlmann [2], the Hodge conjecture is therefore true for all CM abelian varieties having complex multiplication by E and CM type S .

It is obvious that a non-degenerate CM type must be primitive in the sense that it arises from no CM subfield of E which is strictly smaller than E ([4, § 8.2]). Conversely, one may ask for sufficient conditions for a primitive CM type to be non-degenerate. If S is primitive, we have the double inequality [3]

$$(*) \quad \log_2(4d) \leq \dim W_S \leq d+1 .$$

Clearly, (*) implies that a primitive CM type is non-degenerate whenever $d=1, 2$, or 3 .

An example of Mumford [2] shows that there exist primitive CM types with $d=4$ which are not non-degenerate. It is tempting to guess that such examples must exist for each $d \geq 4$. Surprisingly, Tankeev showed recently [5] that primitive CM types are non-degenerate if $d=5$. Here we present a generalization, suggested by F. Hazama :

THEOREM. - If d is a prime number and S is primitive, then S is non-degenerate.

(Because of (*), we may assume that d is an odd prime.)

Proof. - Let L be the Galois closure of E in \mathbb{C} , i. e. the smallest subfield of \mathbb{C} containing all $\sigma(E)$ with $\sigma \in \mathfrak{S}$. The action of G on W_S factors through $\text{Gal}(L/\mathbb{Q})$. Moreover, the assumption that S is primitive implies that $\text{Gal}(L/\mathbb{Q})$ acts faithfully on W_S . (A priori, the kernel of the action of G on W_S corresponds to the Galois closure L' of the CM subfield of \mathbb{C} which is "dual" to (E, S) . We have $L = L'$ when S is primitive.)

Because d divides $[E : \mathbb{Q}]$, d divides the order of $\text{Gal}(L/\mathbb{Q})$. Let $g \in G$ be such that g induces an element of $\text{Gal}(L/\mathbb{Q})$ of order d . Then g induces an automorphism of W_S of order d . To prove that $W_S = V$ we must show that the dimension of W_S is at least $d+1$. Now the action of g on W_S is semi-simple (because of finite order), and any g -stable subspace of W_S on which g acts non-trivially has (by a well known lemma) dimension at least $(d-1)$. To prove the theorem, it suffices to exhibit two linearly independent vectors of W_S which are fixed by g .

Consider

$$v = S + gS + \dots + g^{d-1}S \in W_S$$

and the "norm" element \mathfrak{S} of W . The latter belongs to W_S because it may be written as the sum of S and its complex conjugate.

Both elements are visibly fixed by g . Moreover, when d is odd, v cannot be a rational multiple of \mathfrak{S} . Indeed, if it were such a multiple, it would have to be an integral multiple of \mathfrak{S} . Writing

$$v = \sum_{\sigma \in \mathfrak{S}} n_{\sigma} \sigma,$$

we would find a divisibility $2d \mid n_{\sigma}$. Since $\sum n_{\sigma} = d^2$ is not divisible by $2d$, v and \mathfrak{S} are linearly independent and the theorem is proved.

:-:-:-

REFERENCES

- [1] T. KUBOTA, On the field extension by complex multiplication, Trans. AMS 118 n° 6 (1965), 113-122.
- [2] H. POHLMANN, Algebraic cycles on abelian varieties of complex multiplication type, Ann. of Math. 88 (1968), 161-180.
- [3] K. RIBET, Division fields of abelian varieties with complex multiplication, Mémoire de la S. M. F. (2e série) 2 (1980), 75-94.

- [4] G. SHIMURA and Y. TANIYAMA, Complex Multiplication of Abelian Varieties and its Applications to Number Theory, Publ. Math. Soc. Japan n° 6, Tokyo, 1961.
- [5] S. G. TANKEEV, Sur les cycles algébriques des variétés abéliennes simples de dimension 5 (en russe), Izvestija Math. 45, n° 4 (1981).

(texte reçu le 17 mars 1982)

--:--:--

K. A. RIBET
U. C. Math. Dept.
Berkeley, Ca. 94720
U. S. A.