Math. Ann. 284, 307–327 (1989)

Mathematische Annalen

Idempotent relations and factors of Jacobians

E. Kani[1,*] and M. Rosen[2,**]

[1] Department of Mathematics, Queen's University, Jeffrey Hall, Kingston, Ontario, Canada K7L 3N6
[2] Department of Mathematics, Brown University, Providence, RI 02912, USA

Introduction

Let C be a (smooth, projective, geometrically connected) curve defined over an arbitrary field K and let $\pi_i: C \to C_i$, $1 \leqq i \leqq N$, be a collection of subcovers of C, all defined over K. The present paper was motivated by the following question: *what general relations, if any, exist between the (numerical) invariants attached to the curves* $C, C_1, \ldots, C_N$?

The basic numerical invariant of a curve C is, of course, its *genus* g_C but in $\mathrm{char}(K) = p \neq 0$ there are also other invariants, notably the *Hasse-Witt invariant* (or *p-rank*) σ_C. All these invariants, however, are subsumed in a universal invariant, $h^1(C) = [J_C]$, the 1-*motive* of C/K, which by definition is the K-isogeny class of the Jacobian variety of C, and therefore we focus our attention here on this motivic invariant.

The first evidence of such relations was furnished by Accola [Ac1, Ac2] who provided some useful sufficient conditions which force relations among the g_{C_i}'s. In [Ka2] it was shown that Accola's relations also hold for the σ_{C_i}'s, and this was further generalized by Frey and Rück [FR]. However, Accola's relations are not the only general relations that exist among these invariants: it was pointed out in [Ka2] that Accola's hypotheses are a special case of certain *idempotent relations* in a suitable group ring $\mathbb{Q}[G]$ which in turn determine idempotent relations in the endomorphism algebra $\mathrm{End}^0(J_C) = \mathrm{End}_K(J_C) \otimes \mathbb{Q}$.

The main stimulus for this paper stems from the suggestion of Accola (private communication) that such idempotent relations should also determine relations among the motivic invariants. In carrying out this suggestion, we made two further observations. The first is that this phenomenon is not only restricted to the idempotents $\varepsilon_{\pi_i} \in \mathrm{End}^0(J_C)$ attached to morphisms of curves but is, in fact, true for any set of idempotents $\varepsilon_i \in \mathrm{End}^0(A)$ of an arbitrary abelian variety A; in this case one has to replace $[J_{C_i}]$ by $[\varepsilon_i(A)]$, the isogeny class of the "image" $\varepsilon_i(A)$ of A under

* NSERC University Research Fellow
** Partially supported by a grant from the Natural Science Foundation

ε_i. The second observation is that, conversely, every relation among the motivic invariants actually comes from an idempotent relation, provided that the concept of an "idempotent relation" is slightly generalized. To this end, let us call two elements $a, b \in \mathrm{End}^0(A)$ *character equivalent* (notation: $a \sim b$) if we have $\chi(a) = \chi(b)$, for all $\mathbb{Q}$-rational characters $\chi \in \mathbf{ch}(\mathrm{End}^0(A))$. We then have the following general result.

Theorem A. *Let $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon'_1, \ldots, \varepsilon'_m \in \mathrm{End}^0(A)$ be (not necessarily distinct) idempotents. Then the idempotent relation*

$$\varepsilon_1 + \ldots + \varepsilon_n \sim \varepsilon'_1 + \ldots + \varepsilon'_m \tag{1}$$

holds in $\mathrm{End}^0(A)$ if and only if we have the isogeny relation

$$\varepsilon_1(A) \times \ldots \times \varepsilon_n(A) \sim \varepsilon'_1(A) \times \ldots \times \varepsilon'_m(A). \tag{2}$$

Actually, this theorem is an immediate consequence of a slightly more precise result (Theorem 1) proven below in Sect. 1.

The usefulness of Theorem A rests ultimately on our ability to exhibit such idempotent relations (1) explicitly. In the case that all the coverings π_i are galois, i.e., $C_i = C/H_i$ for some subgroup $H_i \leqq G = \mathrm{Aut}(C)$, a powerful method of producing such relations is to study relations among the idempotents

$$\varepsilon_{H_i} = \frac{1}{|H_i|} \sum_{h \in H_i} h \in \mathbb{Q}[G]$$

in the rational group ring $\mathbb{Q}[G]$. Indeed, it is easy to get a complete overview of all such idempotent relations; the *Burnside ring* $\mathbf{B}(G)$ offers a convenient framework for studying such relations (cf. Sect. 3).

As was already remarked, the relations which Accola established for the g_{C_i}'s stem from such idempotent relations in $\mathbb{Q}[G]$, and we therefore obtain such "Accola relations" for the motivic invariants as well (cf. Sect. 3). A particularly simple yet useful special case of these is the following:

Theorem B. *Let $G \leqq \mathrm{Aut}(C)$ be a (finite) subgroup such that $G = H_1 \cup \ldots \cup H_t$, where the subgroups $H_i \leqq G$ satisfy $H_i \cap H_j = \{1\}$ for $i \neq j$. Then we have the isogeny relation*

$$J_C^{t-1} \times J_{C/G}^{g} \sim J_{C/H_1}^{h_1} \times \ldots \times J_{C/H_t}^{h_t} \tag{3}$$

where $g = |G|$, $h_i = |H_i|$ and, as usual, $J^n = J \times \ldots \times J$ (n times).

The groups G satisfying the hypothesis of Theorem B (with $t > 1$) are called "groups with a partition" and have been (more or less) completely classified (cf. Baer [Ba], Kegel [Ke] and Suzuki [Su]). These include the elementary abelian p-groups $G = \mathbb{Z}/p\mathbb{Z} \times \ldots \times \mathbb{Z}/p\mathbb{Z}$, the projective linear groups $PSl_2(p^n)$, Frobenius groups, dihedral groups, etc.

If we apply Theorem B to the *Fermat curve* $C: x^p + y^p = 1$ and $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (where p is an odd prime $\neq \mathrm{char}(K)$), then we obtain the well-known decomposition (cf. e.g. Lang [La, p. 43ff]):

$$J_C \sim J_{C_1} \times \ldots \times J_{C_{p-2}}, \tag{4}$$

where C_i denotes the (normalization of) the curve $y^p = x^i(1-x)$. It is interesting to note that the isogeny (4) is defined over the prime subfield Q of K, even though the automorphism group G is only defined over $Q(\zeta_p)$ (cf. Sect. 5).

Similarly, if we consider the case that C is the *modular curve* $C = X(p)$ *of level* p (defined over $K = \mathbb{Q}(\zeta_p)$) and $G = PSl_2(p)$, then Theorem B yields the K-isogeny relation

$$J(p)^2 \sim J_1(p)^2 \times J_{sp}(p)^{\frac{p-1}{2}} \times J_{nsp}(p)^{\frac{p-1}{2}} \tag{5}$$

which we haven't found in literature. Here, $J(p) = J_{X(p)}$, $J_1(p) = J_{X_1(p)}$ etc. have their usual meaning (cf. Sect. 5).

Still another example is furnished by a suitable quotient C of the *Drinfeld curve* $D: xy^q - x^q y = 1$ defined over $K = \mathbb{F}_{q^2}$. Here we apply Theorem B to $G = PSl_2(q)$ and hence obtain a decomposition analogous to (5). As a consequence we derive the curious fact that if q is even (i.e., $q = 2^f$), then the Jacobian of the Drinfeld curve is a $(q-1)$-st power,

$$J_D \sim A^{q-1},$$

where A is some abelian variety (of dimension $q/2$).

Another method of producing idempotent relations is presented in Sect. 4. This method is based on the fact that it is possible to characterize the validity of a *strict* idempotent relation

$$\sum n_i \varepsilon_{\pi_i} = 0 \tag{6}$$

by a purely *numerical* criterion. A useful special case of these results (cf. Theorem 7) is the following.

Theorem C. *Let $H_1, \ldots, H_t \leqq \mathrm{Aut}(C)$ be (finite) subgroups with $H_i \cdot H_j = H_j \cdot H_i$, for all i, j, and let g_{ij} denote the genus of the quotient curve $C/(H_i \cdot H_j)$. Then, for $n_1, \ldots, n_t \in \mathbb{Z}$, the conditions*

$$\sum n_i n_j g_{ij} = 0, \tag{7}$$

$$\sum_j n_j g_{ij} = 0, \quad 1 \leqq i \leqq n, \tag{8}$$

are each equivalent to (6) and hence both imply the isogeny relation

$$\prod_{n_i > 0} J_{C/H_i}^{n_i} \sim \prod_{n_j < 0} J_{C/H_j}^{|n_j|}. \tag{9}$$

In particular, if $g_{ij} = 0$ for $2 \leqq i < j \leqq t$ and if

$$g_C = g_{C/H_2} + \ldots + g_{C/H_t}, \tag{10}$$

then we have (by taking $H_1 = \{1\}$ above):

$$J_C \sim J_{C/H_2} \times \ldots \times J_{C/H_t}. \tag{11}$$

Theorem C applies in particular to the Fermat curves above and hence gives another proof of the decomposition (4). Moreover, as is shown in Sect. 5, it also applies to the *Humbert curves* (of genus 5) to yield the decomposition

$$J_C \sim J_{C_1} \times \ldots \times J_{C_5} \tag{12}$$

of J_C into a product of five elliptic curves. It is interesting to observe that this decomposition does *not* follow from Theorem B.

This paper is organized as follows. In Sect. 1 we present (a sharpening of) Theorem A, which is then applied in Sect. 2 to idempotent relations arising from coverings of curves. In Sect. 3 we study idempotent relations in the group ring $\mathbb{Q}[G]$ and derive some specific isogeny relations (e.g. Theorem B). In Sect. 4 we study strict idempotent relations in terms of certain numerical invariants and prove (a generalization of) Theorem C. Finally, in Sect. 5 we illustrate the above theorems with the help of the specific examples such as the Fermat curves, modular curves etc. which were mentioned above.

We would like to express our appreciation to R. Accola whose initial suggestion was the original stimulus of this paper. We would also like to thank D. Hayes for drawing our attention to the Drinfeld curve which is discussed in Sect. 5.

This research was supported in part by a grant from the Natural Sciences and Engineering Research Council of Canada (NSERC) held by the first author and by an NSF grant held by the second author.

1. Factors of Abelian varieties

Let A be an abelian variety defined over a field K. By Poincaré's complete reducibility theorem (cf. [Mu, p. 173] or [Mi, Proposition 12.1]), A is K-isogeneous to a product

$$A \sim B := B_1^{n_1} \times \ldots \times B_r^{n_r}, \tag{1}$$

where the B_i are K-simple abelian varieties (i.e., B_i has no proper abelian subvariety defined over K) which are pairwise non-K-isogeneous.

Let $\mathrm{End}_K(A)$ denote the ring of K-rational endomorphisms of A and let

$$\mathscr{A} := \mathrm{End}_K^0(A) := \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$

be its associated $\mathbb{Q}$-Algebra, which is known to be finite-dimentional (cf [Mi, Theorem 12.5]). Moreover, $\mathscr{A}$ is semi-simple, for (1) induces a ring isomorphism

$$\mathscr{A} \cong M_{n_1}(S_1) \oplus \ldots \oplus M_{n_r}(S_r) \tag{2}$$

where $S_i := \mathrm{End}_K^0(B_i)$ is a skewfield. Thus, for each i, $1 \leqq i \leqq r$, there exists an irreducible $\mathscr{A}$-module V_i with the property that V_i is faithful on the subalgebra $M_{n_i}(S_i)$. Let $\varrho_i : \mathscr{A} \to \mathrm{End}_{\mathbb{Q}}(V_i)$ denote the representation afforded by V_i and let

$$\chi_i(a) = \mathrm{tr}(\varrho_i(a))$$

denote its character (which is defined since $\dim_{\mathbb{Q}} \mathscr{A} < \infty$).

We now want to study *K-quotients* of A up to isogeny. It is easy to see that each such quotient (or factor) A' is of the form

$$A' \sim \varepsilon(A), \tag{3}$$

for some idempotent $\varepsilon \in \mathscr{A}$. (Here and below, $\varepsilon(A)$ denotes any representative of the isogeny class containing the abelian subvarieties $(n\varepsilon)(A) \subset A$, where $n \in \mathbb{N}$ is chosen such that $n\varepsilon \in \mathrm{End}_K(A) \subset \mathscr{A}$.)

It turns out that the structure of $\mathcal{E}(A)$ is completely determined by the set of values $\{\chi_i(\varepsilon)\}$; more precisely, we have:

Theorem 1. *Let $\varepsilon \in \mathrm{End}_K^0(A)$ be an idempotent. Then*

$$\mathcal{E}(A) \sim B_1^{m_1} \times \ldots \times B_r^{m_r}, \tag{4}$$

where the m_i's are determined by the formula

$$\chi_i(\varepsilon) = m_i \dim_{\mathbb{Q}}(S_i), \quad 1 \leqq i \leqq r. \tag{5}$$

Proof. a) $r = 1$.

Without loss of generality $A = B^n$. Let $\varepsilon_i \in \mathrm{End}(A) \subset \mathscr{A}$ denote the composition $\varepsilon_i = \mathrm{j}_i \circ p_i$, where

$$p_i : B^n \to B, \quad p_i(b_1, \ldots, b_n) = b_i$$

denotes the projection map onto the i^{th} factor and

$$j_i : B \to B^n, \quad j_i(b) = (0, \ldots, 0, b, 0, \ldots, 0)$$

denotes the inclusion map into the i^{th} component. Clearly, $\varepsilon_1, \ldots, \varepsilon_n$ are pairwise orthogonal idempotents (i.e., $\varepsilon_i^2 = \varepsilon_i$, $\varepsilon_i \cdot \varepsilon_j = 0$ for $i \neq j$) and $1 = \varepsilon_1 + \ldots + \varepsilon_n$. Since $\mathscr{A} \cong M_n(S)$, where S is a skewfield, it follows that each ε_i is a primitive idempotent of $\mathscr{A}$. (Use e.g. Albert [Al, II, Theorem 16 and III, Theorem 9].)

Now let $\varepsilon \in \mathscr{A}$ be an arbitrary idempotent. Then by [Al, IV, Theorem 2], there exists $\alpha \in \mathscr{A}^\times$ such that

$$\alpha \varepsilon \alpha^{-1} = \varepsilon_1 + \ldots + \varepsilon_s,$$

for some s, $1 \leqq s \leqq n$. ($s = \mathrm{rk}(\varepsilon)$ is called the rank of ε.) Clearly

$$(\varepsilon_1 + \ldots + \varepsilon_s)(A) = B^s.$$

On the other hand, since $\alpha \in \mathscr{A}^\times$ is invertible, we have $\alpha^{-1}(A) \sim A$, so $\mathcal{E}(A) \sim \varepsilon\alpha^{-1}(A) \sim \alpha(B^s) \sim B^s$. Thus (4) holds with

$$m = s = \mathrm{rk}(\varepsilon). \tag{6}$$

It remains to compute $\chi(\varepsilon)$. Since all ε_i's are conjugate, we have

$$\chi(\varepsilon) = m\chi(\varepsilon_1) = \frac{m}{n}\chi(1) = \frac{m}{n}\dim_{\mathbb{Q}}(V),$$

where V denotes the (irreducible) left $\mathscr{A}$-module affording χ. Now $V \cong \mathscr{A}\varepsilon_i$, $\forall i$ and $\mathscr{A}\varepsilon_1 \oplus \ldots \oplus \mathscr{A}\varepsilon_n = \mathscr{A} = M_n(S)$, so

$$\dim_{\mathbb{Q}} V = \frac{1}{n}\dim_{\mathbb{Q}} M_n(S) = \frac{1}{n}(n^2 \dim_{\mathbb{Q}}(S)),$$

and we obtain (5).

b) $r > 1$.

Without loss of generality $A = A_1 \times \ldots \times A_r$, where $A_i = B_i^{n_i}$, $1 \leqq i \leqq r$. Let $e_i \in \mathrm{End}(A) \subset \mathscr{A}$ denote the composition $e_i = \mu_i \circ \pi_i$, where

$$\pi_i : A_1 \times \ldots \times A_r \to A_i$$

denotes the projection onto the i^{th} factor and

$$\mu_i : A_i \to A_1 \times \ldots \times A_r$$

denotes the inclusion map into the i^{th} component: $\mu_i(a_i) = (0, \ldots, 0, a_i, 0, \ldots, 0)$. Clearly, $e_1, \ldots, e_r$ are pairwise orthogonal (central) idempotents and $1 = e_1 + \ldots + e_r$.

For any $\alpha \in \mathrm{End}_K(A)$, $\alpha_i := \pi_i \circ \alpha \circ \mu_i \in \mathrm{End}_K(A_i)$ and we have

$$\alpha(A) \cong \alpha_1(A_1) \times \ldots \times \alpha_r(A_r)$$

(because $\mu_i \alpha_i(A_i) = e_i \alpha e_i(A)$, and $\alpha = e_1 \alpha e_1 + \ldots + e_r \alpha e_r$), and so for $\alpha \in \mathscr{A}$ we have

$$\alpha(A) \sim \alpha_1(A_1) \times \ldots \times \alpha_r(A_r).$$

Now if $\alpha = \varepsilon$ is an idempotent of $\mathscr{A}$, then each $\alpha_i = \varepsilon_i$ is an idempotent of $\mathrm{End}^0(A_i)$. Thus, by a) we have $\varepsilon_i(A_i) \sim B_i^{m_i}$, where

$$\chi_i'(\varepsilon_i) = m_i \dim_{\mathbb{Q}}(S_i),$$

if χ_i' denotes the unique irreducible character of $\mathscr{A}_i = \mathrm{End}^0(A_i)$. Now $\varphi_i : \mathscr{A}_i \to \mathscr{A}$, given by $\varphi_i(a) = \mu_i \circ a \circ \pi_i$, is an injective $\mathbb{Q}$-algebra homomorphism with image $e_i \mathscr{A} e_i$, and so $\chi_i' = \chi_i \circ \varphi_i$. Since $\varphi_i(\varepsilon_i) = e_i \varepsilon e_i$, we obtain $\chi_i'(\varepsilon_i) = \chi_i(e_i \varepsilon e_i) = \chi_i(\varepsilon)$, and the assertion follows.

With the aid of Theorem 1 it is now easy to prove Theorem A of the introduction. In order to avoid notational confusion, let us repeat (and generalize slightly) the definition of character equivalence presented in the introduction:

Definition. Let $\mathscr{A}$ be a finite dimensional $\mathbb{Q}$-algebra. We call two elements $a_1, a_2 \in \mathscr{A}$ *character equivalent* (in $\mathscr{A}$) and write $a_1 \sim a_2$ (in $\mathscr{A}$), if we have $\chi(a_1) = \chi(a_2)$, $\forall \chi \in \mathbf{ch}(\mathscr{A})$. Here, as usual, $\mathbf{ch}(\mathscr{A}) = \mathbf{ch}(\mathscr{A}/\mathbb{Q})$ denotes the *ring of virtual* $\mathbb{Q}$*-characters* of $\mathscr{A}$ which, as an abelian group, is given by

$$\mathbf{ch}(\mathscr{A}) = \mathbb{Z}\chi_1 \oplus \ldots \oplus \mathbb{Z}\chi_r,$$

if $\{\chi_1, \ldots, \chi_r\}$ denotes the set of $\mathbb{Q}$-characters afforded by a basic set of irreducible left $\mathscr{A}$-modules (each viewed as a $\mathbb{Q}$-vector space).

Proof of Theorem A. By Theorem 1 we have, for each i, $1 \leqq i \leqq n$:

$$\varepsilon_i(A) \sim B_1^{n_{i1}} \times \ldots \times B_r^{n_{ir}},$$

where $n_{ij} = \chi_j(\varepsilon_i)/\dim_{\mathbb{Q}}(S_j)$, $1 \leqq j \leqq r$. Thus

$$\varepsilon_1(A) \times \ldots \times \varepsilon_n(A) \sim B_1^{s_1} \times \ldots \times B_r^{s_r}, \tag{7}$$

with

$$s_j = \sum_{i=1}^{n} \chi_j(\varepsilon_i)/\dim_{\mathbb{Q}}(S_j) = \chi_j(\varepsilon_1 + \ldots + \varepsilon_n)/\dim_{\mathbb{Q}}(S_j), \tag{8}$$

and similarly,

$$\varepsilon_1'(A) \times \ldots \times \varepsilon_1'(A) \sim B_1^{t_1} \times \ldots \times B_r^{t_r}, \tag{9}$$

with

$$t_j = \chi_j(\varepsilon_1' + \ldots + \varepsilon_m')/\dim_{\mathbb{Q}}(S_j). \tag{10}$$

Comparing (7)–(10) yields the equivalences

$$\begin{aligned}&\varepsilon_1(A)\times\ldots\times\varepsilon_n(A)\sim\varepsilon'_1(A)\times\ldots\times\varepsilon'_m(A)\\&\Leftrightarrow\chi_j(\varepsilon_1+\ldots+\varepsilon_n)=\chi_j(\varepsilon'_1+\ldots+\varepsilon'_m),\quad 1\leqq j\leqq n\\&\Leftrightarrow\varepsilon_1+\ldots+\varepsilon_n\sim\varepsilon'_1+\ldots+\varepsilon'_m\quad(\text{in }\mathrm{End}^0(A)).\end{aligned}$$

This concludes the proof of Theorem A. Fof future reference, it is useful to append the following remarks, most of which pertain to the notion of character equivalence.

Remarks. 1) Let $f:\mathscr{A}\to\mathscr{B}$ be a ring homomorphism of finite dimensional $\mathbb{Q}$-algebras and let $a_1, a_2\in\mathscr{A}$. Then:

$$a_1\sim a_2\ (\text{in }\mathscr{A})\Rightarrow f(a_1)\sim f(a_2)\ (\text{in }\mathscr{B}).$$

2) If $\mathscr{A}$ is a finite dimensional semi-simple $\mathbb{Q}$-algebra and ε_1, $\varepsilon_2\in\mathscr{A}$ are idempotents, then

$$\varepsilon_1\sim\varepsilon_2\ (\text{in }\mathscr{A})\Leftrightarrow\varepsilon_1=a\varepsilon_2a^{-1},\ \text{for some}\quad a\in\mathscr{A}^\times.$$

This is implicit in the proof of Theorem 1 and follows from [Al, IV, Theorem 2].

3) Let $\mathscr{A}$ be a finite dimensional semi-simple $\mathbb{Q}$-algebra. As was suggested in the introduction, a relation of the form

$$\sum n_i\varepsilon_i\sim 0\ (\text{in }\mathscr{A})\qquad(n_i\in\mathbb{Z},\ \varepsilon_i^2=\varepsilon_i)\tag{11}$$

will be called an "idempotent relation" in $\mathscr{A}$. It is of some interest to know whether each such idempotent relation is a *strict* idempotent relation $\sum n_i\varepsilon_i=0$; i.e., whether the implication

$$\sum n_i\varepsilon_i\sim 0\ (\text{in }\mathscr{A})\Rightarrow\sum n_i\varepsilon_i=0\tag{12}$$

always holds in $\mathscr{A}$. Since each matrix algebra $M_n(S_i)$ has for $n>1$ (many!) distinct yet conjugate idempotents, it is clear that a necessary condition for the validity of (12) is that $\mathscr{A}$ be *of multiplicity one*, i.e.,

$$\mathscr{A}\cong S_1\times\ldots\times S_r,\tag{13}$$

where the S_i are (skew)fields. In fact, this condition is also sufficient, for in this case each idempotent $\varepsilon_i\in\mathscr{A}$ has the form $\varepsilon_i=\sum_{j=1}^{r}t_{ij}\sigma_j$ where $t_{ij}=0$ or $=1$ $\forall i,j$ and σ_j denotes the (unique) idempotent $\neq 0$ of S_i. Thus, if (11) holds, then applying χ_j to $\sum r_i\varepsilon_i$ yields $\sum_i r_it_{ij}=0$, $1\leqq j\leqq r$, which means $\sum r_i\varepsilon_i=0$. We therefore see that (12) and (13) are equivalent; i.e., that *every idempotent relation* (11) *is strict if and only if* $\mathscr{A}$ *is of multiplicty one.*

4) If L is an extension field of K, then clearly $\mathscr{A}_L:=\mathrm{End}^0_L(A)\supset\mathscr{A}:=\mathrm{End}^0_K(A)$, and so we have for $a_1, a_2\in\mathscr{A}$:

$$a_1\sim a_2\ (\text{in }\mathscr{A})\Rightarrow a_1\sim a_2\ (\text{in }\mathscr{A}_L).$$

The converse, however, is false in general. For example, suppose $A=E_1\times E_2$ where E_1, E_2 are two elliptic curves defined over K which are not K-isogeneous but which

are L-isogeneous; such E_i's exist (for $K=\mathbb{Q}$ and $L=\mathbb{Q}(i)$); cf. e.g., Serre [Se1, p. IV.22]. If $\varepsilon_1, \varepsilon_2 \in \mathrm{End}_K^0(A)$ denote the idempotents belonging to E_1, E_2 then clearly $\varepsilon_1 \sim \varepsilon_2$ (in $\mathscr{A}$) but $\varepsilon_1 \not\sim \varepsilon_2$ (in $\mathscr{A}_L$).

In particular, we see that "idempotent relations do not descend under base-field extensions", i.e.,

$$\sum r_i \varepsilon_i \sim 0 \text{ (in } \mathscr{A}_L), \qquad \varepsilon_i \in \mathscr{A} \not\Rightarrow \sum r_i \varepsilon_i \sim 0 \text{ (in } \mathscr{A}).$$

Note, however, that strict idempotent relations do descend.

2. Idempotents via coverings of curves

Given a covering (=surjective morphism)

$$\pi : C \to C'$$

of curves, we have two induced homomorphisms between their respective Jacobian varieties:

$$\pi^* : J_{C'} \to J_C, \qquad \pi_* : J_C \to J_{C'}$$

obtained by the pull-back resp. push-forward of divisor (classes) $D' \in \mathrm{Pic}^0(C') = J_{C'}$ resp. $D \in \mathrm{Pic}^0(C) = J_C$. Since

$$\pi_* \pi^*(D') = \deg(\pi) D', \qquad \forall D' \in \mathrm{Pic}^0(J_{C'}), \tag{1}$$

we see that

$$\varepsilon_\pi = \frac{1}{\deg(\pi)} \pi^* \circ \pi_* \in \mathrm{End}^0(J_C) \tag{2}$$

is an *idempotent* and that

$$\varepsilon_\pi(J_C) \sim \pi^*(J_{C'}) \sim J_{C'}. \tag{3}$$

Thus, by Theorem A we have

Theorem 2. *If $\pi_i : C \to C_i$, $1 \leqq i \leqq n$, and $\pi'_j : C \to C'_j$, $1 \leqq j \leqq m$, are coverings, then*

$$\sum_i \varepsilon_{\pi_i} \sim \sum_j \varepsilon_{\pi'_j} \Leftrightarrow \prod J_{C_i} \sim \prod J_{C'_j}. \tag{4}$$

Since $g_{C_i} = \dim J_{C_i}$ and $\dim(A_1 \times A_2) = \dim A_1 + \dim A_2$, we obtain:

Corollary 1. $\sum n_i \varepsilon_{\pi_i} \sim 0 \Rightarrow \sum n_i g_{C_i} = 0$.

Similarly, if $\mathrm{char}(K) = p \neq 0$, then the Hasse-Witt invariant σ_{C_i} of C_i is given by $\sigma_{C_i} = \dim_{\mathbb{Q}_p}(T_p(J_{C_i}) \otimes \mathbb{Q}_p)$ and hence we have

Corollary 2. $\sum n_i \varepsilon_{\pi_i} \sim 0 \Rightarrow \sum n_i \sigma_{C_i} = 0$.

We therefore see that Theorem 3 of [Ka2] (i.e., Corollaries 1 and 2 above) is a special case of Theorem 2. Similarly, Statement A_3 of Frey-Rück [FR] (which generalizes Corollary 2) is an immediate consequence of Theorem 2.

To state this result, let $\mathrm{char}(K) = p \neq 0$ and assume (for simplicity) that K is algebraically closed. If A is an abelian variety over K, let $A(p)$ denote the p-divisible

group (=Barsotti-Tate group) associated to A, and let $D=D(A(p))$ be its Dieudonné module with Frobenius endomorphism $F: D \to D$. Then (D, F) is an F-crystal (cf. Berthelot [Be]) which gives rise to an F-isocrystal (D_Q, F_Q), where $Q=\mathrm{Quot}(W(K))$ is the quotient field of the ring $W(K)$ of Witt vectors over K. By the fundamental structure theorem of F-isocrystals (cf. [Be], Demazure [De]), (D_Q, F_Q) has a unique decomposition (as F-isocrystals)

$$D(A)_Q = \bigoplus_{\lambda \in \mathbb{Q}} (D(A)_Q)_\lambda \tag{5}$$

into isotypic components $(D(A)_Q)_\lambda$ which are a direct sum of the simple F-isocrystals "of slope λ", (cf. [Be, De]) and

$$m_\lambda(A) = \dim_Q (D(A)_Q)_\lambda \tag{6}$$

is called the *multiplicity of the slope* λ. (Note that actually $m_\lambda(A)=0$ for $\lambda \notin [0,1]$; cf. [Be].) Since $A \sim B \Rightarrow D(A)_Q \cong D(B)_Q \Leftrightarrow m_\lambda(A)=m_\lambda(B)$, $\forall \lambda \in \mathbb{Q}$, (and since clearly $m_\lambda(A \times B)=m_\lambda(A)+m_\lambda(B)$, $\forall \lambda \in \mathbb{Q}$, because $D(A \times B) \cong D(A) \times D(B)$), we obtain from Theorem 2:

Corollary 3. $\sum n_i \varepsilon_{\pi_i} \sim 0 \Rightarrow \sum n_i m_\lambda(J_{C_i})=0$, $\forall \lambda \in \mathbb{Q}$.

3. Idempotent relations via Galois theory

Fix a (finite) subgroup $G \leqq \mathrm{Aut}(C)$. Each subgroup $H \leqq G$ defines a galois covering

$$\pi_H : C \to C_H = C/H$$

and an idempotent

$$\varepsilon_H = \frac{1}{|H|} \sum_{h \in H} h \in \mathbb{Q}[G]$$

in the rational group ring $\mathbb{Q}[G]$. If

$$\alpha : \mathbb{Q}[G] \to \mathrm{End}^0(J_C)$$

denotes the canonical map of $\mathbb{Q}$-algebras induced by $\alpha(g)=g_*$ for $g \in G$, then we have the formula

$$\alpha(\varepsilon_H) = \varepsilon_{\pi_H}. \tag{1}$$

This follows from the well-known facts that $\deg(\pi_H)=|H|$ and that $\pi_H^*(\pi_H)_* D = \sum_{h \in H} h_* D$, for all $D \in \mathrm{Div}(C)$.

In view of Theorem 2 (and Remark 1) we therefore see that every relation among the idempotents $\varepsilon_H \in \mathbb{Q}[G]$ induces an isogeny relation among the Jacobians $J_H = J_{C/H}$ of the quotient curves C/H. It is interesting to observe that each such idempotent relation can be equivalently expressed as a *character relation*; i.e., we have

$$\sum n_H \varepsilon_H \sim 0 \text{ (in } \mathbb{Q}[G]) \Leftrightarrow \sum n_H 1_H^* = 0 \quad \text{in} \quad \mathbf{ch}(\mathbb{Q}[G]) \tag{2}$$

where, as usual, $1_H^* = \mathrm{Ind}_H^G(1_H)$ denotes the induced character. To see this, note that by Frobenius Reciprocity we have

$$\chi(\varepsilon_H) = (\chi_{|H}, 1_H)_H = (\chi, 1_H^*)_G, \tag{3}$$

and hence (2) follows since $(,)_G$ is non-degenerate. Summing up, we have shown:

Theorem 3. *If $H_1, \ldots, H_s$, $H_1', \ldots, H_t'$ are subgroups of $G \leqq \mathrm{Aut}(C)$, then every idempotent/character relation*

$$\sum n_i \varepsilon_{H_i} \sim \sum m_j \varepsilon_{H_j'} \Leftrightarrow \sum n_i 1_{H_i}^* = \sum m_j 1_{H_j'}^* \tag{4}$$

(with $n_i, m_j \in \mathbb{N}$) induces an isogeny relation

$$J_{H_1}^{n_1} \times \ldots \times J_{H_s}^{n_s} \sim J_{H_1'}^{m_1} \times \ldots \times J_{H_t'}^{m_t}. \tag{5}$$

Let us now determine how many independent idempotent/character relations actually exist in $\mathbb{Q}[G]$. To this end, consider the $\mathbb{Q}$-vector space

$$\mathbf{A}(G) = \bigoplus_{H \leqq G} \mathbb{Q} \cdot H$$

which is freely generated by the subgroups H of G. We are interested in determining the dimension of the *space of idempotent relations.*

$$\mathbf{IR}(G) = \{\sum n_H H \in \mathbf{A}(G) : \sum n_H \varepsilon_H \sim 0\} = \mathrm{Ker}(\mathbf{ch}),$$

where

$$\mathbf{ch} : \mathbf{A}(G) \to \mathbb{Q} \otimes \mathbf{ch}(\mathbb{Q}[G])$$

is defined by $\mathbf{ch}(\sum n_H H) = \sum n_H 1_H^*$. Since **ch** is surjective by Artin's Induction theorem, we obtain

$$\begin{aligned} \dim_{\mathbb{Q}} \mathbf{IR}(G) &= \dim_{\mathbb{Q}} \mathbf{A}(G) - \dim_{\mathbb{Q}}(\mathbb{Q} \otimes \mathbf{ch}(\mathbb{Q}[G])) \\ &= \#(\text{subgroups of } G) - \#(\text{conjugacy classes of} \\ &\quad \text{cyclic subgroups of } G), \end{aligned} \tag{6}$$

the latter equality following again from Artin's theorem (cf. [CR1, 39.5]).

It is interesting to compare this formula to the one obtained by Rehm [Re] for the dimension of the space

$$\mathbf{SIR}(G) = \{\sum n_H H \in \mathbf{A}(G) : \sum n_H \varepsilon_H = 0\}$$

of *strict idempotent relations:*

$$\dim_{\mathbb{Q}} \mathbf{SIR}(G) = \#(\text{non-cyclic subgroups of } G). \tag{7}$$

(In fact, he establishes an explicit basis for $\mathbf{SIR}(G)$ $(= \mathbf{U}(G) \otimes \mathbb{Q}$, in his notation); cf. [Re, 1.1] or Remark 5 below). Comparing (6) and (7) yields in view of Remark 3:

$\mathbb{Q}[G]$ is of multiplicity $1 \Leftrightarrow G$ is a hamiltonian group.

Recall that a hamiltonian group is a group G in which every subgroup is normal; these have been characterized by Dedekind (cf. [Hu, p. 308]).

In the above formula (6), the obvious relations $\varepsilon_H \sim \varepsilon_{g^{-1}Hg}$ resulting from conjugacy contribute significantly to the count. Discarding these leads to

considering the image of $\mathbf{IR}(G)$ in the *Burnside ring* (cf. e.g., [CR3]):

$$\mathbf{B}(G)_{\mathbb{Q}} = \otimes \mathbb{Q} cl(H)$$

under the natural map

$$cl: \mathbf{A}(G) \to \mathbf{B}(G)$$

which maps each subgroup $H \leqq G$ to its conjugacy class $cl(H) = \{g^{-1}Hg : g \in G\}$. By (6) we therefore see that the number of "truly independent" idempotent relations is

$$\dim_{\mathbb{Q}} cl(\mathbf{IR}(G)) = \#(\text{conjugacy classes of non-cyclic subgroups of } G). \quad (8)$$

It therefore follows from (6), (7), or (8) that non-trivial relations exist whenever G is non-cyclic. This can also be seen directly. If G is non-cyclic, then we can write

$$G = H_1 \cup \ldots \cup H_t \quad (9)$$

with proper subgroups $H_i < G$, and an inclusion-exclusion count shows that

$$|G|\varepsilon_G = \sum_{r=1}^{t} (-1)^{r+1} \sum_{1 \leqq i_1 < \ldots < i_r \leqq t} |\mathbf{H}_{i_1} \cap \ldots \cap H_{i_r}| \varepsilon_{H_{i_1} \cap \ldots \cap H_{i_r}} \quad (10)$$

which is a non-trivial relation. By Theorem 3 we therefore have:

Theorem 4. *If $G = H_1 \cup \ldots \cup H_t$, then we have the isogeny relation*

$$J_G^{|G|} \times \prod_{r=1}^{[t/2]} \prod_{1 \leqq i_1 < \ldots < i_{2r} \leqq t} J_{H_{i_1} \cap \ldots \cap H_{i_{2r}}}^{|H_{i_1} \cap \ldots \cap H_{i_{2r}}|}$$
$$\sim \prod_{r=0}^{[t/2]} \prod_{1 \leqq i_1 < \ldots < i_{2r+1} \leqq t} J_{H_{i_1} \cap \ldots \cap H_{i_{2r+1}}}^{|H_{i_1} \cap \ldots \cap H_{i_{2r+1}}|}. \quad (11)$$

A nice feature of the above formula is that it holds for an arbitrary covering (9). One of its disadvantages is, however, that since often many of the intersections $H_{i_1} \cap \ldots \cap H_{i_r}$ coincide, considerable cancellation takes place in (10), and this is somewhat awkward to keep track of. For example, in the case that the covering (9) is actually a *partition*, i.e., $H_i \cap H_j = \{1\}$ for $i \neq j$, then (10) reduces to

$$|G|\varepsilon_G = \sum_{r=1}^{t} |H_r|\varepsilon_{H_r} - (t-1)\varepsilon_{\{1\}}, \quad (12)$$

but it is easier to prove (12) directly than to deduce it from (10). (Note that Theorem B of the introduction follows immediately from (12) and Theorem 3.) Similarly, if the covering (9) consists of all (maximal) cyclic subgroups of G, then (10) reduces to the *Brauer-Rehm* relation (cf. [Re, 1.1])

$$|G|\varepsilon_G = \sum_{H \in \mathscr{Z}(G)} a_H |H| \varepsilon_H, \quad (13)$$

in which $\mathscr{Z}(G)$ denotes the set of cyclic subgroups of G, and

$$a_H = a_H^G = \sum_{\substack{Z \in \mathscr{Z}(G) \\ Z \geqq H}} \mu([Z : H]), \quad (14)$$

where μ denotes the Möbius function. Note that (13) implies the relation

$$1_G = \sum_{H \in \mathscr{Z}(G)} a_H \frac{|H|}{|G|} 1_H^*$$

which is a special case of Brauer's formula (concerning his explicit version of Artin's induction theorem); cf. [CR2, 15.4].

We thus have

Theorem 5. *If $G \leqq \mathrm{Aut}(C)$, then we have the isogeny relation*

$$J_G^{|G|} \times \prod_{\substack{H \in \mathscr{Z}(G) \\ a_H < 0}} J_H^{-|H| a_H} \sim \prod_{\substack{H \in \mathscr{Z}(G) \\ a_H > 0}} J_H^{|H| a_H}. \tag{15}$$

Remark 5. The relations of the type (13) are particularly interesting because if we let G run over all non-cyclic subgroups of a group $\mathscr{G}$, then the relations (13) form a *basis* of the space $\mathbf{SIR}(\mathscr{G})$ of all strict idempotent relations (cf. [Re, 1.1]).

Another useful relation is

Theorem 6. *Let $H_1, \ldots, H_t \leqq G \leqq \mathrm{Aut}(C)$ be subgroups such that:*

1) $H_i \cdot H_j = H_j \cdot H_i$, $\forall i, j$.

2) *For every (complex) irreducible character $\chi \in \mathbf{ch}(\mathbb{C}[G])$ there exists a subgroup $H_i \subset \mathrm{Ker}(\chi)$. Then we have the isogeny relation*

$$\begin{aligned} J_C \times \prod_{r=1}^{[t/2]} \prod_{1 \leqq i_1 < \ldots < i_{2r} \leqq t} J_{H_{i_1} \cdot \ldots \cdot H_{i_{2r}}} \\ \sim \prod_{r=0}^{[t/2]} \prod_{1 \leqq i_1 < \ldots < i_{2r+1} \leqq t} J_{H_{i_1} \cdot \ldots \cdot H_{i_{2r+1}}}. \end{aligned} \tag{16}$$

Proof. As is shown in [Ka2], the hypotheses imply the idempotent relation

$$\sum_{r=1}^{t} (-1)^{r+1} \prod_{1 \leqq i_1 < \ldots < i_r \leqq t} \varepsilon_{H_{i_1} \cdot \ldots \cdot H_{i_r}} = 1, \tag{17}$$

and so the result follows by Theorem 3.

Remark 6. Note that Theorem B, 4, 5, and 6 are all deduced from *strict* idempotent relations. Thus, by Remark 4 the isogeny relations (0.3), (11), (15), and (16) are valid over any field for which the morphisms involved are all defined (even if the automorphisms groups G, H_i are not.)

4. Strict idempotent relations

As in Sect. 2, let $\pi_i : C \to C_i$, $1 \leqq i \leqq N$, be a family of (not necessarily galois) coverings. Here we wish to study *strict* idempotent relations among the ε_{π_i}, viz. relations of the form

$$\sum n_i \varepsilon_{\pi_i} = 0, \tag{1}$$

and derive a *numerical criterion* for such relations.

This is based on the fact that $\mathrm{End}^0(J_C)$ is endowed with a *positive definite* quadratic form σ which can be (more or less) explicitly calculated. To define σ, we shall make use of the identification

$$\beta : \mathscr{C}(C) \xrightarrow{\sim} \mathrm{End}(J_C) \tag{2}$$

of $\mathrm{End}(J_C)$ with the *ring of correspondences*

$$\mathscr{C}(C) = \mathrm{Pic}(C \times C)/(pr_1^* \mathrm{Pic}(C) + pr_2^* \mathrm{Pic}(C))$$

(cf. [We] or [Ka1]). For divisors $D_1, D_2 \in \mathrm{Div}(C \times C)$, put

$$\sigma(D_1, D_2) = d_1(D_1)d_2(D_2) + d_1(D_2)d_2(D_1) - (D_1 \cdot D_2),$$

where, as usual, $(\cdot)$ denotes the intersection number of two divisors and, for $i = 1, 2$,

$$d_1(D_i) = (D_i \cdot (A \times C))/\deg(A),$$
$$d_2(D_i) = (D_i \cdot (C \times A))/\deg(A),$$

for any divisor $A \in \mathrm{Div}(C)$ with $\deg(A) \neq 0$. Then *Castelnuovo's Theorem* states that σ is positive-definite:

$$\sigma(D, D) \geqq 0; \quad \sigma(D, D) = 0 \Leftrightarrow D \in pr_1^* \mathrm{Pr}(C) + pr_2^* \mathrm{Pic}(C) \tag{3}$$

(cf. e.g., [Ka1]) and hence σ induces via the identification β a positive definite quadratic form on $\mathrm{End}^0(J_C)$, also denoted by σ.

We remark that σ is compatible with the multiplication in $\mathrm{End}^0(J_C)$ in the sense that

$$\sigma(D \circ D_1, D_2) = \sigma(D_1, D' \circ D_2), \tag{4}$$
$$\sigma(D_1 \circ D, D_2) = \sigma(D_1, D_2 \circ D'), \tag{5}$$

where $'$ denotes the Rosati involution (i.e., $D' = \tau^* D$, where $\tau : C \times C \to C \times C$ denotes the morphism which exchanges the factors); cf. [We, p. 38]. Note that by [We] we could have alternately defined σ as the trace

$$\sigma(D_1, D_2) = \mathrm{tr}(\varrho_\ell(\beta(D_2' \circ D_1))),$$

where $\varrho_\ell : \mathrm{End}(J_C) \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(J_C))$ denotes the ℓ-adic representation ($\ell \neq \mathrm{char}(K)$), but this (more complicated) definition does not allow us to readily compute σ.

Let us now put

$$g_{ij} = g(\pi_i, \pi_j) = \tfrac{1}{2}\sigma(\varepsilon_{\pi_i}, \varepsilon_{\pi_j}). \tag{6}$$

From (2) and (3) we therefore obtain the following two criteria for a strict idempotent relation (1):

$$\sum n_i \varepsilon_{\pi_i} = 0 \Leftrightarrow \sum_{i,j} n_i n_j g_{ij} = 0$$
$$\Leftrightarrow \sum_j n_j g_{ij} = 0, \quad 1 \leqq i \leqq N. \tag{7}$$

In particular, we see that a non-trivial relation (1) exists if and only if $\det(g_{ij}) = 0$.

Of course, the criteria (7) are of use only if we can compute the matrix (g_{ij}) in terms of the geometry of the π_i's. This is indeed possible, as will now be explained.

To begin with, we observe that the diagonal terms are just the genera of the curves C_i; i.e.,

$$g_{ii} = g_{C_i}. \tag{8}$$

This follows easily (cf. [Ka3]) from the projection and adjunction formulae since

$$\varepsilon_{\pi_i} = \frac{1}{\deg(\pi_i)} \beta(\Gamma_{\pi_i}^*), \tag{9}$$

where, as in [Ka3], $\Gamma_{\pi_i}^* = (\pi_i \times \pi_i)^*(\Delta_{C_i})$.

It is somewhat more difficult to obtain explicit expressions for the off-diagonal terms g_{ij}. One such expression was obtained in [Ka3] and involves, aside from the genera $g_i = g_{C_i}$ and the degrees $\deg(\pi_i)$, also the *arithmetic genus* $p_{ij} = p_a(C_{ij})$ of the (possibly singular) curve $C_{ij} = \mathrm{Im}(\pi_{ij}) \subset C_i \times C_j$ which is the image scheme on $C_i \times C_j$ of the morphism

$$\pi_{ij} = \pi_i \times \pi_j \circ \delta_C : C \to C_i \times C_j,$$

where $\delta_C : C \to C \times C$ denotes the diagonal morphism. Explicitly, we have by Theorem 1′ of [Ka3]:

$$g_{ij} = [(d_{ij}-1)(d_{ji}-1) + d_{ij}g_i + d_{ji}g_j - p_{ij}]/(d_{ij}d_{ji}), \tag{10}$$

where $d_{ij} = \deg(\pi_i)/\deg(\pi_{ij})$ $(= [\pi_i^* K(C_i)\pi_j^* K(C_j) : \pi_i^* K(C_i)]$, if $K(C_i)$ denotes the function field of C_i).

A special case of (10) is the following formula, which may also be proved directly:

$$\tfrac{1}{2}\sigma(\varepsilon_{id}, \varepsilon_{\pi_i}) = g_{C_i}. \tag{11}$$

It is interesting to observe that the matrix (g_{ij}), besides being symmetric and positive semi-definite, is also non-negative:

$$g_{ij} \geqq 0, \quad 1 \leqq i, \quad j \leqq N; \tag{12}$$

this follows immediately from (10) and Castelnuovo's inequality (cf. [Ka3]). Alternatively, one can also deduce (12) from the fact that the idempotents ε_{π_i} are *symmetric* with respect to the Rosati involution (i.e., $\varepsilon'_{\pi_i} = \varepsilon_{\pi_i}$), for we obtain then by (4) and (5):

$$\sigma(\varepsilon_{\pi_i}, \varepsilon_{\pi_j}) = \sigma(\varepsilon_{\pi_i} \circ \varepsilon_{\pi_j}, \varepsilon_{\pi_i} \circ \varepsilon_{\pi_j}) \geqq 0. \tag{13}$$

Moreover, it follows from (13) that

$$g_{ij} = 0 \Leftrightarrow \varepsilon_{\pi_i} \circ \varepsilon_{\pi_j} = 0 \quad (\text{in } \mathrm{End}^0(J_C)) \tag{14}$$

i.e., that $g_{ij} = 0$ if and only if the idempotents ε_{π_i} and ε_{π_j} are *orthogonal.*

In the case that the π_i are galois, i.e., $\pi_i = \pi_{H_i} : C \to C_i = C/H_i$, for suitable subgroups $H_i \leqq G \leqq \mathrm{Aut}(C)$, another, possibly more explicit, formula may be given for the g_{ij}'s. This involves the (global) *Artin character* $a_G = \sum_{P \in C} a_P$ which is the sum of the local Artin characters a_P and hence may be computed readily by ramification

theory (cf. Serre [Se2]). To be precise, we have the formula

$$g_{ij}=1+\frac{1}{|H_iH_j|}\left(g_C-1-\tfrac{1}{2}\sum_{\substack{h\in H_iH_j\\ h\neq 1}}a_G(h)\right). \tag{15}$$

This follows easily by combining the formula

$$\varepsilon_{\pi_i}=\frac{1}{|H|}\beta\left(\sum_{h\in H_i}\Gamma_h\right) \tag{16}$$

[which is essentially a restatement of (3.1)] with (8) (for $\pi_i=\mathrm{id}$) and with the well-known formula (cf. [We; Se2]):

$$a_G(g^{-1}h)=(\Gamma_h\cdot\Gamma_g)=2-\sigma(\Gamma_h,\Gamma_g),\quad \text{if}\quad g,h\in G, g\neq h. \tag{17}$$

Here, as usual, Γ_h denotes the graph of the (auto)morphism $h: C\to C$.

It is useful to observe that in the case that $H_i\cdot H_j$ is a subgroup of G, i.e., if $H_i\cdot H_j=H_j\cdot H_i$, then $\sum_{h\neq 1}a_G(h)$ is the degree of the different of $\pi_{H_i\cdot H_j}: C\to C/(H_i\cdot H_j)$ (cf. [Se2, p. 104]) and so by the Riemann-Hurwitz formula, the formula (15) reduces to:

$$g_{ij}=g_{C/(H_i\cdot H_j)},\quad \text{if}\quad H_i\cdot H_j=H_j\cdot H_i. \tag{18}$$

Remark 7. This formula can be extended to the non-galois case as follows. Suppose $\pi_k: C\to C_k$, $k=i,j$ are two coverings which "commute" in the sense that there exist finite morphisms

$$\pi'_k: C_k\to C'_{ij}\qquad (k=i,j)$$

to a curve C'_{ij} such that

a) $\pi'_i\circ\pi_i=\pi'_j\circ\pi_j$

b) $\deg(\pi'_i)=d_{ji}$ $(=\deg(\pi_j)/\deg(\pi_{ij}))$, $\deg(\pi'_j)=d_{ij}$.

It then follows from a) and b) that

$$(\pi'_i\times\pi'_j)^*(\Delta_{C'_{ij}})=C_{i,j}, \tag{19}$$

and hence we obtain from Theorem 1′ of [Ka3] and the projection formula that

$$g_{ij}=g_{C'_{ij}}, \tag{20}$$

which generalizes (18).

Summarizing, we therefore obtain the following theorem which amply contains Theorem C of the introduction:

Theorem 7. *A strict idempotent relation* (1) *holds in* $\mathrm{End}^0(J_C)$ *if and only if we have*

$$\sum_j n_jg_{ij}=0,\qquad 1\leqq i\leqq N, \tag{21}$$

where the g_{ij} *are given by* (10) *in general and by* (15), *if all the* π_i *are galois. Moreover, if the morphisms* π_i *and* π_j *"commute" (cf. Remark 6), then* g_{ij} *is given by* (20).

If such a relation (21) *holds, then we have the K-isogeny relation*

$$\prod_{n_i>0}J_{C_i}^{n_i}\sim\prod_{n_j<0}J_{C_j}^{|n_j|} \tag{22}$$

which is valid for every field K over which the morphisms π_i are defined. In particular, if $g_{ij}=0$ for $2\leqq i<j\leqq N$ (i.e., if the idempotents ε_{π_i} are pairwise orthogonal for $i=2,\ldots,N$) and if

$$g_C=g_{C_2}+\ldots+g_{C_N}, \tag{23}$$

then we have the orthogonal decomposition:

$$J_C\sim J_{C_2}\times\ldots\times J_{C_N}. \tag{24}$$

Proof. The first four assertions are clear by the previous discussion combined with Theorem 2 (and Remark 4). The last assertion follows by applying the first part of the theorem to $\pi_1=\mathrm{id}$, $\pi_2,\ldots,\pi_N$ and using (8) and (11).

5. Examples

We shall now illustrate some of the above theorems by presenting a few explicit examples. We begin by specializing Theorem B to the groups $G=\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}p\mathbb{Z}$ and $G=PSl_2(q)$.

Example 1. $G=\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ (p a prime). Since the $p+1$ subgroups $H_0,\ldots,H_p\leqq G$ of index/order p form a partition of G, we obtain, after cancellation, from Theorem B (or from any one of the Theorem 4–7) the isogeny relation

$$J_C\times J_{C/G}^{p}\sim J_{C/H_0}\times\ldots\times J_{C/H_p}. \tag{1}$$

Example 2. $G=PSl_2(q)$, $q=p^f$ a prime power. By. e.g., Huppert [Hu, II.8.6, p. 193], G has the partition

$$G=\bigcup_{i=1}^{r}\mathfrak{P}_i\cup\bigcup_{j=1}^{s}\mathfrak{C}_j\cup\bigcup_{k=1}^{t}\mathfrak{N}_k, \tag{2}$$

where the $\mathfrak{P}_i$, $1\leqq i\leqq r$, are the (distinct) *p-Sylow subgroups* of G, $\mathfrak{C}_j$, $1\leqq j\leqq s$, are the (distinct) *split Cartan subgroups* of G, $\mathfrak{N}_k$, $1\leqq k\leqq t$, are the (distinct) *non-split Cartan subgroups* of G.

The groups $\{\mathfrak{P}_i\}$ resp. $\{\mathfrak{C}_j\}$ resp. $\{\mathfrak{N}_k\}$ constitute a full conjugacy class of subgroups of G and have a "canonical" representative in $Sl_2(q)$ given by

$$\mathfrak{P}=\left\{\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}\in Sl_2(q):\alpha\in\mathbb{F}_q\right\},$$

$$\mathfrak{C}=\left\{\begin{pmatrix}\beta&0\\0&\beta^{-1}\end{pmatrix}\in Sl_2(q):\beta\in\mathbb{F}_q^{\times}\right\},$$

$$\mathfrak{N}=\left\langle\begin{pmatrix}0&1\\-1&\gamma\end{pmatrix}\right\rangle,$$

where $\gamma=\mathrm{tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta)$, $\zeta\in\mathbb{F}_{q^2}$ a (fixed) primitive $(q+1)$-st root of unity. (Note that since $\zeta^2-\gamma\zeta+1=0$, the matrix $\begin{pmatrix}0&1\\-1&\gamma\end{pmatrix}$ has ζ, ζ^q as eigenvalues and hence has order $q+1$, so $\mathfrak{N}$ is indeed a non-split Cartan subgroup.)

We observe that if we put $n=(q-1, 2)$, then we have (cf. [Hu, pp. 191–192]):

$$|G|=(q-1)q(q+1)/n,$$
$$|\mathfrak{P}_i|=q, \quad r=[G:N_G(\mathfrak{P}_i)]=q+1,$$
$$|\mathfrak{C}_j|=(q-1)/n, \quad s=[G:N_G(\mathfrak{C}_j)]=(q+1)q/2,$$
$$|\mathfrak{N}_k|=(q+1)/n, \quad t=[G:N_G(\mathfrak{N}_k)]=(q-1)q/2.$$

Thus, by Theorem B we obtain

$$J_C^{q(q+1)} \times J_{C/G}^{(q-1)q(q+1)/n} \sim \prod_{i=1}^{r} J_{C/\mathfrak{P}_i}^{q} \times \prod_{j=1}^{s} J_{C/\mathfrak{C}_j}^{(q-1)/n} \times \prod_{k=1}^{t} J_{C/\mathfrak{N}_k}^{(q+1)/n}. \tag{3}$$

Since all the curves $C/\mathfrak{P}_i$ (resp. all $C/\mathfrak{C}_j$, resp. all $C/\mathfrak{N}_k$) are isomorphic, we obtain from (3) (after dividing by $q(q+1/2)$:

$$J_C^2 \times J_{C/G}^{2(q-1)/n} \sim J_{C/\mathfrak{P}_1}^2 \times J_{C/\mathfrak{C}_1}^{(q-1)/n} \times J_{C/\mathfrak{N}_1}^{(q-1)/n}. \tag{4}$$

Note, however, that while the isogeny relation (3) is valid over every field K for which all the morphisms involved are defined, this need not be true for the isogeny relation (4).

We now apply the above "group theoretical examples" to specific curves.

Example 3. Fermat curves. Consider the Fermat curve

$$C_m: x^m+y^m=1$$

of exponent m, which is a smooth curve of genus $\frac{1}{2}(m-1)(m-2)$ if $\mathrm{char}(K)\nmid m$ (which we assume henceforth). Let $p|m$ be a prime and for $0\leqq i\leqq p-1$ let $C_i'=C'_{m,p,i}$ denote the normalization of the curve

$$s^m=t^{im/p}(1-t^{m/p}).$$

Note that the genus of C_i' is given by

$$g_{C_i'}=\frac{m}{p}(p-1)+\left(\frac{m}{2p}-1\right)(m-1), \quad \text{if} \quad 1\leqq i\leqq p-2,$$
$$g_{C_0'}=g_{C_{p-1}'}=\frac{m}{2p}(p-1)+\left(\frac{m}{2p}-1\right)(m-1).$$

If we put $C_p'=C_0'$, then we have the isogeny relation

$$J_{C_m} \times J_{C_{m/p}}^{p} \sim J_{C_0'} \times \ldots \times J_{C_p'}. \tag{5}$$

To prove this, suppose first that K contains a primitive p-th root of unity ζ. Then there exist (unique) automorphisms $\sigma, \tau \in \mathrm{Aut}(C_m)$ such that

$$\sigma(x)=\zeta x, \quad \sigma(y)=y; \quad \tau(x)=x, \quad \tau(y)=\zeta y,$$

and these generate a (sub)group $G\cong \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. Since the coverings

$$\pi_i: C_m \to C_i' \quad (0\leqq i\leqq p)$$

defined by $\pi_i^* t = x^p, \pi_i^* s = x^i y$ for $0 \leqq i \leqq p-1$ and by $\pi_p^* t = x, \pi_p^* s = y^p$ correspond to all the subgroups of index/order p of G, and since the covering

$$\pi_G : C_m \to C_m/G = C_{m/p}$$

is given by $\pi_G^* x = x^p$, $\pi_G^* y = y^p$, the isogeny relation (5) follows from Example 1. Moreover, since all the curves and morphisms are defined over the prime field $Q \subset K$, it follows by Remark 6 that the isogeny relation (5) is valid over every field.

Note that the isogeny relation (0.4) of the introduction is a special case of (5) above since in the case $m=p$, the curves $C_{m/p}$, $C_0 = C'_p$, C'_{p-1} all have genus 0.

Example 4. Modular curves. Let $X(p)$ denote the modular curve of level p (= an odd prime) and $J(p)$ its Jacobian variety which are defined over $K = \mathbb{Q}(e^{2\pi i/p})$. It is well-known that $X(p)$ can be realized as a galois covering

$$j : X(p) \to \mathbb{P}^1$$

of $\mathbb{P}^1$ with group $G = Sl_2(p)/\{\pm 1\} = PSl_2(p)$ defined over K. The quotient of $X(p)$ with respect to the subgroup $\mathfrak{P}$ of Example 2 is usually denoted by $X_1(p) = X(p)/\mathfrak{P}$ and its Jacobian by $J_1(p)$. Moreover, we shall write $X_{sp}(p) = X(p)/\mathfrak{C}$ and $X_{nsp}(p) = X(p)/\mathfrak{N}$, and denote their respective Jacobians by $J_{sp}(p)$ and $J_{nsp}(p)$. (The curves $X_{sp}(p)$ and $X_{nsp}(p)$ should not be confused with Mazur's [Ma] $X_{\text{split}}(p) = X(p)/N_G(\mathfrak{C})$ and $X_{\text{non-split}}(p) = X(p)/N_G(\mathfrak{N})$ which are double subcovers of $X_{sp}(p)$ and $X_{nsp}(p)$.) We therefore obtain by Example 2 the K-isogeny relation

$$J(p)^2 \sim J_1(p)^2 \times J_{sp}^{(p-1)/2} \times J_{nsp}^{(p-1)/2}. \tag{6}$$

Example 5. Drinfeld curves. Let K be a field of characteristic $p \neq 0$, and put $q = p^f$, $f \geqq 1$. The *Drinfeld curve* D is defined by the equation

$$D : xy^q - x^q y = 1.$$

It is easy to see that D is a smooth plane curve and hence has genus $\frac{1}{2}q(q-1)$. If $K \supset \mathbb{F}_q$, which we assume henceforth, then $G = Sl_2(q)$ acts (faithfully) as a group of K-automorphisms on D (or, more precisely, on the function field $F = K(x, y)$) as follows:

$$g(x) = ax + by, \quad g(y) = cx + dy, \quad \text{if} \quad g = \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in G.$$

Thus, if $Z = Z(G)$ denotes the centre of G (i.e., $Z = \{\pm 1\}$ if q is odd and $Z = \{1\}$ if q is even) then $\bar{G} = PSl_2(q)$ acts on $C = D/Z$ and hence we can apply Example 2.

It is a routine (but tedius) calculation to determine explicit equations for the quotients C/H. We summarize these in the following table, in which we put:

$$n = |Z| = gcd(2, q-1), \quad \delta = n - 1;$$
$$s = xy, \quad t = x/y, \quad T = t^{(q-1)/n},$$
$$u = x^{q+1} - \gamma x^q y + y^2, \quad v = x^2 - \gamma xy + y^2$$

where, as in Example 2, $\gamma = \text{tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta)$.

Table 1

Subgroup $H \leqq Sl_2(q)$	$g_{D/H}$	Fix (H)	Equation
1	$\frac{1}{2}q(q-1)$	$K(x,y)$	$xy^q - x^q y = 1$
Centre: $Z = \begin{cases} 1 & q \text{ even} \\ \pm 1 & q \text{ odd} \end{cases}$	$\frac{1}{2}(q-\delta)(q-1)$	$K(x,y)$	$xy^q - x^q y = 1$
		$K(s,t)$	$s^{\frac{q+1}{2}}(t^{q-1}-1) + t^{\frac{q-1}{2}} = 0$
p-Sylow subgroup: $\mathfrak{P}$	0	$K(y)$	–
$Z \cdot \mathfrak{P}$	0	$K(y^n)$	–
Split Cartan subgroup: $\mathfrak{C}$	$\frac{1}{2}(q-\delta)$	$K(s,T)$	$s^{\frac{q+1}{2}}(T^2-1) + T = 0$
Non-split Cartan subgroup: $\mathfrak{N}$	$\frac{1}{2}(q-\delta)$	$K(u,v)$	$v^{q+1} = u^2 - \gamma u + 1$

From this table we see that $D/(Z \cdot \mathfrak{P})$ and hence D/G have genus 0, and so (4) reduces to

$$J_C^2 \sim J_{D/\mathfrak{C}}^{(q-1)/n} \times J_{D/\mathfrak{N}}^{(q-1)/n} \tag{7}$$

where the equations of $C = D/Z$, $D/\mathfrak{C}$ and $D/\mathfrak{N}$ are given in Table 1. (More precisely, C, D/Z etc. are the normalization of the (possibly singular) plane curve given in the table.)

Since $D = C$ if q is even, we obtain from (7) the interesting fact that

$$J_D \sim A^{q-1}, \quad (q \text{ even}) \tag{8}$$

for some abelian variety A of dimension $q/2$.

All the examples up till now were illustrations of Theorem B. We conclude with an example that illustrates Theorem 7 (and which does *not* follow from Theorem B).

Example 6. Humbert curves. By definition (cf. e.g., [Ac3, p. 86]), a Humbert curve is a (smooth) curve C of genus 5 which admits five pairwise non-isomorphic coverings

$$\pi_i : C \to E_i, \quad 1 \leqq i \leqq 5,$$

of degree 2 to curves E_i of genus $g_{E_i} = 1$. (It is possible to show that if $\mathrm{char}(K) \neq 2$, then the normalization of every plane sextic of the form

$$y^4 - 4(x^4 - ax^2 + 1)y^2 + b^2x^4 = 0 \tag{9}$$

with $a, b \in K$, $ab \neq 0$, $(2a \pm b)^2 \neq 16$, has this property, but we do not need this here.)

As we now prove, each Humbert curve has the ("orthogonal") decomposition

$$J_C \sim J_{E_1} \times \ldots \times J_{E_5}. \tag{10}$$

This, in fact, follows immediately from (the last assertion in) Theorem 7 once we have shown

$$g_{ij} = \sigma(\varepsilon_{\pi_i}, \varepsilon_{\pi_j}) = 0, \quad \text{if} \quad i \neq j,\ 1 \leqq i, j \leqq 5 \tag{11}$$

because we obviously have $g_C = g_{E_1} + \ldots + g_{E_5}$. To prove (11), we use formula (4.10). Here $\deg(\pi_{ij}) = 1$ (because $K(C) = \pi_i^* K(E_i) \cdot \pi_j^* K(E_j)$, if $i \neq j$), so $\pi_{ij} : C \to C_{ij}$ is

birational, and hence $p_{ij} \geqq g_C = 5$. Thus, by (4.12) and (4.10),

$$0 \leqq g_{ij} = [(2-1)(2-1) + 2 \cdot 1 + 2 \cdot 1 - p_{ij}]/(2 \cdot 2)$$
$$\leqq \tfrac{1}{4}(5 - g_C) = 0. \tag{12}$$

This proves (11) and therefore (10) follows.

In the introduction it was remarked that the decomposition (10) follows from Theorem C. To see this, let us first observe that each covering π_i, being of degree 2, is automatically galois: $\pi_i = \pi_{\langle \tau_i \rangle}$ for some involution $\tau_i \in \mathrm{Aut}(C)$. Next we note that if we put $C''_{ij} = C/\langle \tau_i, \tau_j \rangle$ then

$$g_{C''_{ij}} = 0, \quad \text{if} \quad i \neq j, \tag{13}$$

because if C''_{ij} had genus $\geqq 1$, then by the Riemann-Hurwitz formula it would follow that $\pi'_k : E_i = C/\langle \tau_k \rangle \to C''_{ij}$ is unramified for $k = i, j$ (and that $g_{C''_{ij}} = 1$), so $\pi'_i \circ \pi_i : C \to C''_{ij}$ is unramified, which is impossible. Thus, to be able to apply Theorem C, it is enough to show

$$\tau_i \cdot \tau_j = \tau_j \cdot \tau_i, \qquad 1 \leqq i, j \leqq k, \tag{14}$$

and this follows easily by an application of Accola's genus relation (cf. [Ac1, p. 479]).

Finally, let us observe that (10) does not follow from an idempotent relation in $\mathbb{Q}[G]$, where $G = \langle \tau_1, \ldots, \tau_5 \rangle$; in other words, we assert that

$$\varepsilon_{\{1\}} \neq \varepsilon_{\langle \tau_1 \rangle} + \ldots + \varepsilon_{\langle \tau_5 \rangle}. \tag{15}$$

(Note that since G is abelian, every idempotent relation is a strict idempotent relation by Remark 3.) But this is clear, for the right hand side equals $(\frac{5}{2}) \cdot 1 + \frac{1}{2} \sum_{i=1}^{5} \tau_i \neq 1$ since the $\tau_i \neq 1$ are pairwise distinct.

Actually, by using Accola's relations, it is not difficult to show that $G = \langle \tau_1 \rangle \times \ldots \times \langle \tau_4 \rangle$ and that $\tau_5 = \tau_1 \cdot \ldots \cdot \tau_4$ (cf. also [Ac3, p. 56]), but we do need this here.

References

[Ac1] Accola, R.D.: Riemann surfaces with automorphism groups admitting partitions. Proc. Am. Math. Soc. **21**, 477–482 (1969)

[Ac2] Accola, R.D.: Two theorems on Riemann surfaces with non-cyclic automorphism groups. Proc. Am. Math. Soc. **25**, 598–602 (1970)

[Ac3] Accola, R.D.: Riemann surfaces, theta functions, and Abelian automorphism groups. (Lecture Notes Mathematics, Vol. 483, 105 pp). Berlin Heidelberg New York: Springer 1975

[Al] Albert, A.A.: Structure of algebras. Am. Math. Soc. Colloq. Publ. Providence, R.I., 1961

[Ba] Baer, R.: Partitionen endlicher Gruppen. Math. Z. **75**, 333–372 (1961)

[Be] Berthelot, P.: Slopes of Frobenius in crystalline cohomology. Proc. Symp. Pure Math. **29**, 315–328 (1975)

[CR1] Curtis, C.W., Reiner, I.: Representation theory of finite groups and associative algebras. New York: Interscience 1962

[CR2] Curtis, C.W., Reiner, I.: Methods of representation theory. I. New York: Wiley 1981

[CR3] Curtis, C.W., Reiner, I.: Method of representation theory. II. New York: Wiley 1987

[De] Demazure, M.: Lectures on p-divisible groups. (Lecture Notes Mathematics, Vol. 302, 98 pp.). Berlin Heidelberg New York: Springer 1972
[FR] Frey, G., Rück, H.-G.: The strong Lefschetz principle in algebraic geometry. Manuscr. Math. **55**, 385–401 (1986)
[Hu] Huppert, B.: Endliche Gruppen. I. Berlin: Springer 1967
[Ka1] Kani, E.: On Castelnuovo's equivalence defect. J. Reine Angew. Math. **352**, 24–70 (1984)
[Ka2] Kani, E.: Relations between the genera and between the Hasse-Witt invariants of galois coverings of curves. Can. Math. Bull. **28**, 321–327 (1985)
[Ka3] Kani, E.: Bounds on the number of non-rational subfields of a function field. Invent. Math. **85**, 185–198 (1986)
[Ke] Kegel, O.: Nicht-einfache Partitionen endlicher Gruppen. Arch. Math. **12**, 170–175 (1961)
[La] Lang, S.: Introduction to algebraic and Abelian functions. (2nd ed.). Berlin Heidelberg New York: Springer 1982
[Ma] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. IHES **47**, 33–186 (1977)
[Mi] Milne, J.S.: Abelian varieties. In: Arithmetic geometry G. Cornell, J. Silverman (eds.). Berlin Heidelberg New York: Springer 1986
[Mu] Mumford, D.: Abelian varieties. London: Oxford University Press 1970
[Re] Rehm, H.P.: Über die gruppentheoretische Struktur der Relationen zwischen Relativnormabbildungen in endlichen Galoisschen Körpererweiterungen. J. Number Theory **7**, 49–70 (1975)
[Se1] Serre, J.-P.: Abelian ℓ-adic representations and elliptic curves. New York: Benjamin 1968
[Se2] Serre, J.-P.: Local fields. Berlin Heidelberg New York: Springer 1979
[Su] Suzuki, M.: On a finite group with a partition. Arch. Math. **12**, 241–254 (1961)
[We] Weil, A.: Courbes algébriques et variétés abéliennes. Paris: Hermann 1971

Received November 4, 1988