ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 79–83

CURVES WITH INFINITELY MANY POINTS OF FIXED DEGREE

BY

GERHARD FREY

Institut für Experimentelle Mathematik, Universität GH Essen
Ellernstr. 29, D-45326 Essen 12, Germany
e-mail: mem010@de0hrz1a.bitnet

ABSTRACT

The d-th symmetric product $C^{(d)}$ of a curve C defined over a field K is closely related to the set of points of C of degree $\leq d$. If K is a number field, then a conjecture of Lang [Hi] proved by Faltings [Fa2] implies if $C^{(d)}(K)$ is an infinite set, then there is a K-rational covering of $C \to \mathbb{P}^1_{|K}$ of degree $\leq 2d$. As an application one gets that for fixed field K and fixed d there are only finitely many primes l such that the set of all elliptic curves defined over some extensions L of K with $[L:K] \leq d$ and with L-rational isogeny of degree l is infinite.

Let K be a field with absolute Galois group G_K, and C/K a projective absolutely irreducible regular curve with Jacobian variety $J = J(C)$. For $d \in \mathbb{N}$ let C^d be the direct product of d copies of C. Divide C^d by the symmetric group S_d to get the **d-th symmetric product** $C^{(d)} = C^d/S_d$ of C. Let $\tilde{K}$ be the algebraic closure of K. Then $C^{(d)}(\tilde{K})$, the set of algebraic points of $C^{(d)}$, corresponds one-to-one to the set $\{P_1 + \cdots + P_d;\ P_i \in C(\tilde{K})\}$ of positive $\tilde{K}$-rational divisors of degree d of C. Throughout the whole paper we will assume that C has a K-rational point P_0.

Let L be an extension field of K which is separable over K with $n_L = [L:K] \leq d$. Let Q be an L-rational point of C. We call Q a point of C of degree $\leq d$. Let $\tau_1, \ldots, \tau_{n_L}$ be the different embeddings of L into K_s over K and $Q_i = \tau_i(Q)$. Then $Q_1 + \cdots + Q_{n_L} + (d - n_L) \cdot P_0$ is a K-rational point of $C^{(d)}$. In particular, $C^{(d)}(K)$ is an infinite set if and only if C has infinitely many points of degree $\leq d$ over K.

Received October 31, 1991 and in revised form March 5, 1992

Hence the G_K-conjugacy classes of points of C of degree $\leq d$ can and will be interpreted as subsets of $C^{(d)}(K)$. Define

$$\Phi\colon C^{(d)} \longrightarrow J$$

by $\Phi(P_1+\cdots+P_d) = [P_1+\cdots+P_d-dP_0]$ where [ ] denotes the divisor class. The image W_d of Φ is a closed subscheme of J. Let $n(d)$ be the number of solutions of the equation

$$\sum_{i=1}^{d} \epsilon_i = d \text{ with } \epsilon_i \in \{0,1,2\}.$$

A very easy observation is:

PROPOSITION 1:

i) *Assume that $\Phi_{|C^{(d)}(K)}$ is not injective. Then there is a K-rational covering $\pi\colon C \to \mathbb{P}^1_{|K}$ of degree $\leq d$.*

ii) *Assume that there is a point $\mathbf{P} \in C^{(d)}(K)$ and at least $n(d)+1$ elements $b_0,\ldots,b_{n(d)} \in J(K_s)$ such that $\Phi(\mathbf{P}) \pm b_i \in W_d(K_s)$. Then there is a K-rational covering $\pi : C \to \mathbb{P}^1_{|K}$ of degree $\leq 2d$.*

Proof: i) If $\Phi(P_1+\cdots+P_d) = \Phi(Q_1+\cdots+Q_d)$, then $[P_1+\cdots+P_d-dP_0] = [Q_1+\cdots+Q_d-dP_0]$ and hence the K-rational divisor $P_1+\cdots+P_d$ is linearly equivalent to the (different) divisor $Q_1+\cdots+Q_d$, and so there is a non-constant function $f \in K(C)$, the function field of C, with a pole divisor of degree $\leq d$. Hence $[K(C):K(f)] \leq d$.

ii) By assumption, for each $0 \leq i \leq n(d)$ there exist $Q_{ij}, R_{ij} \in C(K_s)$, $j = 1,\cdots,d$ such that

$$\Phi(Q_{i1}+\cdots+Q_{id}) = \Phi(\mathbf{P}) + b_i,$$
$$\Phi(R_{i1}+\ldots+R_{id}) = \Phi(\mathbf{P}) - b_i.$$

Hence, $[Q_{i1}+\cdots+Q_{id}+R_{i1}+\cdots+R_{id}] = [2\mathbf{P}]$.

Let $Q_1,\ldots,Q_d,R_1,\ldots,R_d$ be points in C such that

$$Q_1+\cdots+Q_d+R_1+\cdots+R_d = 2(P_1+\cdots+P_d). \tag{1}$$

Suppose that $P_1,\ldots,P_d$ are distinct. Denote the number of occurrences of P_j in the d-tuple $(Q_1,\ldots,Q_d)$ by ϵ_j. Then $0 \leq \epsilon_j \leq 2$ and $\sum_{j=1}^{d} \epsilon_j = d$. Hence, the number of $(Q_1,\ldots,Q_d) \in C^{(d)}(K_s)$ for which there exist $(R_1,\ldots,R_d) \in C^{(d)}(K_s)$ such that (1) holds is $n(d)$. If $P_1,\ldots,P_d$ are not necessarily distinct, this number is at most $n(d)$. Since $b_0, \dots, b_{n(d)}$ are distinct, there exists at least one i such that

$$Q_{i1} + \cdots + Q_{id} + R_{i1} + \cdots + R_{id} \neq 2\mathbf{P}.$$

It follows that the dimension of the space $L_{K_s}(2\mathbf{P})$ of K_s-rational functions with pole divisor $\leq 2\mathbf{P}$ has dimension > 1. As this dimension is invariant under separable extensions of the field of constants $\dim_K L_K(2\mathbf{P}) > 1$. Hence there is a K-rational non-constant function f with pole divisor dividing $2\mathbf{P}$ and so $[C(K) : K(f)] \leq 2d$. ∎

COROLLARY 1: *Assume that for a* $\mathbf{P} \in C^{(d)}(K)$ *the scheme*

$$W_d - \Phi(\mathbf{P})$$

contains a subgroup of $J(K_s)$ *of order* $> n(d)$.

i) *If* K *is an infinite field, then* C *has infinitely many points of degree* $\leq 2d$.

ii) *Let* K *be a finite field with* q *elements. Then* $|C(K)| \leq 2d(q+1)$.

Proof: The assumptions of the corollary imply assumption ii) of the proposition and so we know that there is a K-rational covering map

$$\pi \colon C \longrightarrow \mathbb{P}^1_{|K} \text{ of degree} \leq 2d.$$

Hence for all $P_0 \in \mathbb{P}^1(K)$ we have: $\#\{\pi^{-1}(P_0) \cap C(K)\} \leq 2d$ and hence ii) follows, and for $P \in \pi^{-1}(P_0)(K_s)$ we have degree $(P) \leq 2d$, and so i) follows. ∎

Much deeper than proposition 1 is kind of a converse of the corollary for special fields K. We restrict ourselves to number fields.

PROPOSITION 2: *Assume that* K *is a number field and that* C *has infinitely many points of degree* $\leq d$ *over* K. *Then there is a* K*-rational covering* $\pi \colon C \to \mathbb{P}^1_{|K}$ *of degree* $\leq 2d$.

Proof: If $\Phi_{|C^{(d)}(K)}$ is not injective, the assertion of the proposition follows from proposition 1. So we can assume that $W_d(K)$ is an infinite set. Faltings ([Fa2]) proved that there are finitely many elements $x_1, \dots, x_n$ of $W_d(K)$ such that $W_d(K) = \bigcup_{i=1}^n [x_i + A_i(K)]$ with A_i abelian subvarieties of J. Thus, there exists i such that $A_i(K)$ is infinite and $x_i + A_i(K) \subseteq \Phi(C^{(d)}(K))$. In particular there exist $b_0 \in A_i(K)$ and $P \in C^{(d)}(K)$ such that $x_i + b_0 = \Phi(P)$. For each

$a \in A_i(K)$ we have $\Phi(P) \pm a = x_i + (b_0 \pm a) \in W_d(K_s)$. Since $A_i(K)$ is infinite, the assumption of ii) of Proposition 1 is satisfied. Hence, it conclusion is also satisfied. ∎

Remark: There are curves with infinitely many points of degree d and with $2d$ as minimal covering of degree $2d$ over $\mathbb{P}^1$. As examples one can take coverings of degree d of elliptic curves. For $d \leq 3$ these are the only possibilities (cf. [A-H]). D. Abramovich announced in [A] that for large d there are examples of curves C for which $C^{(d)}$ has Abelian subvarieties with minimal covering degree $2d$ over $\mathbb{P}^1$ which have no elliptic subfield. ∎

Now we will give an arithmetical application of the results proved above.

Let K be a number field and $\wp$ a prime divisor of K with residue field $k_\wp$. For each i in a set I let C_i be a curve defined over K of genus g_i. The following definition is motivated by coding theory (cf. [F-P-S]):

Definition: $(C_i)_{i\in I}$ behaves asymptotically good at $\wp$, if

a) all curves C_i have good reduction $C_i^{(\wp)}$mod $\wp$ and
b) $\liminf_{i\in I} |C_i^{(\wp)}(k_\wp)| = \infty$. ∎

PROPOSITION 3: *We assume that $(C_i)_{i\in I}$ behaves asymptotically good at $\wp$. Then for all $d \in \mathbb{N}$ there are only finitely many $i \in I$ such that C_i has infinitely many points of degree $\leq d$.*

Proof: If $(C^i)^{(d)}(K)$ is infinite, then there is a covering

$$\pi_i \colon C^i \to \mathbb{P}^1_{|K}$$

with degree $(\pi_i) \leq 2d$. By reduction theory (cf. [Deu]) this implies that there is a $k_\wp$-rational covering $\pi^\wp : (C^i)^{(\wp)} \to \mathbb{P}^1_{|k_\wp}$ of degree $\leq 2d$, too, and hence $|C^i(k_\wp)| \leq 2d(|k_\wp| + 1)$, and by assumption this can occur only finitely often. ∎

COROLLARY 2: *For $d \in \mathbb{N}$ we have: For all prime numbers $l > 120d$ there are only finitely many elliptic curves defined over number fields L with $[L : \mathbb{Q}] \leq d$ having an L-rational isogeny of degree l.*

Proof: Take $K = \mathbb{Q}(\sqrt{5})$. Then 2 generates a prime ideal in the ring of integers of K with quotient field of 4 elements. The family of curves

$$(X_0(l))_{l \text{ an odd prime}}$$

behaves asymptotically good at the prime corresponding to 2; and one knows that $|X_0(l)^{(\wp)}(k_\wp| \geq [\frac{l}{12}] + 1$. So we can apply the proof of proposition 3 and get: If $2d \cdot 5 < \frac{l}{12}$ then $X_0(l)^{(d)}(K)$ is finite. Since the L-rational points of $X_o(l)$ parametrize elliptic curves defined over L with L-rational isogeny of degree l, the corollary follows. ∎

ACKNOWLEDGEMENT: The author wants to thank W.-D. Geyer, M. Jarden, and E. Kani for helpful discussions.

Part of the paper was written during a visit at the Institute for Advanced Studies of the Hebrew University of Jerusalem. The author would like to thank the Institute for its support and warm hospitality.

References

[A] D. Abramovich, Letter, 1992.

[A–H] D. Abramovich and J. Harris, *Abelian varieties and curves in $W_d(C)$*, Comp. Math. **78** (1991), 227–238.

[Deu] M. Deuring, *Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers*, Math. Z. **47** (1942), 643–654.

[Fa1] G. Faltings, *Diophantine approximation on Abelian varieties*, Annals of Math. **133** (1991), 549–576.

[Fa2] G. Faltings, *The general case of S. Lang's conjecture*, Preprint, Princeton University (1992).

[F] G. Frey, *A remark about isogenies of elliptic curves over quadratic fields*, Comp. Math. **58** (1986), 133–134.

[F–P–S] G. Frey, M. Perret, and H. Stichtenoth, *On the different of Abelian extensions of global fields*, in *Coding Theory and Algebraic Geometry* (H. Stichtenoth and M. Tsfasman, eds.), Proceeding AGCT3, Luminy June 1991, Lecture Notes in Mathematics **1518**, Springer, Heidelberg, 1992, pp. 26–32.

[Hi] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603.