Tôhoku Math. J.
40 (1988), 613-616.

A REMARK ON THE RANK OF JACOBIANS OF HYPERELLIPTIC CURVES OVER $\boldsymbol{Q}$ OVER CERTAIN ELEMENTARY ABELIAN 2-EXTENSIONS

JAAP TOP*

(Received June 8, 1987)

1. Introduction. A nice question in arithmetic geometry is whether for a given abelian variety A over a number field K, relatively small extensions $L \supset K$ exist such that $\operatorname{rank}(A(L))$ is "much" bigger than $\operatorname{rank}(A(K))$. Already in 1938, Billing (see [5; p. 157] for a reference) showed that the elliptic curve $E/\boldsymbol{Q}$ given by the equation $y^2 = x^3 - x$ has rank at least m over infinitely many fields of the form $\boldsymbol{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})$.

Also Néron studied these matters; his result is (see [5; p. 157]):

FACT. Given a hyperelliptic curve $\mathscr{C}$ over a number field K and a point $P \in \mathscr{C}(K)$, there exist infinitely many extensions of K of the form $L = K(\sqrt{d_1}, \cdots, \sqrt{d_m})$ such that $\operatorname{rank}(\mathscr{J}(\mathscr{C})(L)) \geqq m$.

Néron uses a specialization argument to prove this. Our aim in this paper is to show that it is quite easy to construct such extensions explicitly without using any deep theory.

2. Statement of the result and preliminaries. We give a proof of the following:

THEOREM. *Let $f \in \boldsymbol{Z}[X]$ be a separable polynomial of odd degree $\geqq 3$. Let $\mathscr{C}$ be a smooth model of the curve given by $y^2 = f(x)$ and let $\mathscr{J}$ be the jacobian of $\mathscr{C}$. For every $m \geqq 1$ one can explicitly construct infinitely many extensions of $\boldsymbol{Q}$ of the form $K = \boldsymbol{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})$ for which* $\operatorname{rank}(\mathscr{J}(K)) \geqq \operatorname{rank}(\mathscr{J}(\boldsymbol{Q})) + m$.

The proof (which in fact works with $\boldsymbol{Q}$ replaced by any number field) is based on the simple observation that we have a degree two morphism $\mathscr{C} \to \boldsymbol{P}^1$ defined over $\boldsymbol{Q}$. If $x \in \boldsymbol{P}^1(\boldsymbol{Q})$, then the fiber over x in general consists of two points defined over a quadratic extension of $\boldsymbol{Q}$. The class of one such point minus the point lying over infinity yields a point in $\mathscr{J}(\mathscr{C})$. The only thing we have to check is that we can choose the points in $\boldsymbol{P}^1(\boldsymbol{Q})$ in such a way that the points in $\mathscr{J}(\mathscr{C})$ we obtain are linearly

* Supported by the Dutch Organization for the Advancement of Pure Research (ZWO).