ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 30, Number 2, Summer 2000

JACOBIANS OF CURVES OVER FINITE FIELDS

JOSÉ FELIPE VOLOCH

Let $C/\mathbf{F}_q$ be a curve over a finite field of genus g at least two. Assume C has a rational point P_0 and consider C embedded in its Jacobian J by sending P_0 to $0 \in J$. So $C(\mathbf{F}_q) \subset J(\mathbf{F}_q)$ and we can consider the subgroup G of $J(\mathbf{F}_q)$ generated by $C(\mathbf{F}_q)$. If G is not the whole of $J(\mathbf{F}_q)$, we will show that we can construct an étale cover of C where every $\mathbf{F}_q$-rational point of C splits completely into $\mathbf{F}_q$-rational points. We will prove that, if q is large enough compared to g, then $G = J(\mathbf{F}_q)$ and will give examples showing that this equality does not always hold and these examples will lead to curves over finite fields with many rational points.

Theorem. *With the notation as above, if $q \geq (8g-2)^2$, then $G = J(\mathbf{F}_q)$.*

Before proving the theorem, we need a lemma.

Lemma. *Let A be an abelian group and α a surjective endomorphism of A. Let G be a subgroup of $\ker \alpha$ and $\varphi : A \to A/G$ the canonical map and $\beta : A/G \to A/G$ the endomorphism induced by α. Finally, let $\psi : A/G \to A$ be the unique homomorphism such that $\alpha = \psi \circ \varphi$. Then $\psi(\ker \beta) = G$.*

Proof. By construction, $\beta \circ \varphi = \varphi \circ \alpha$, that is, $\beta(y) = \varphi(\alpha(x))$ for any $x, \varphi(x) = y$. Also ψ is defined by $\psi(y) = \alpha(x)$ for any $x, \varphi(x) = y$, that is, $\alpha = \psi \circ \varphi$. We also have $\beta = \varphi \circ \psi$. Indeed, given $y \in A/G$ and $x, \varphi(x) = y$, we have $\beta(y) = \beta(\varphi(x)) = \varphi(\alpha(x)) = \varphi(\psi(y))$. It follows that $\psi(\ker \beta) \subset \ker \varphi = G$. On the other hand, given $x \in \ker \varphi$, we can write $x = \alpha(y)$, $y \in A$. Then $\beta(\varphi(y)) = \varphi(\alpha(y)) = \varphi(x) = 0$, so $\varphi(y) \in \ker \beta$ and therefore $x = \psi(\varphi(y)) \in \psi(\ker \beta)$, which proves that $G \subset \psi(\ker \beta)$, proving the lemma. $\square$

Received by the editors on March 24, 1999.