ASIAN J. MATH.
Vol. 9, No. 2, pp. 257–260, June 2005

010

THE CANONICAL SUBGROUP OF E IS $\mathbf{Spec\,R[x]/(x^p + \frac{p}{E_{p-1}(E,\omega)}x)}$*

ROBERT F. COLEMAN†

Key words. Canonical subgroups, group schemes of order p

AMS subject classifications. 14L15, 11G07

Let p be a prime. In this note we make explicit some results on the canonical subgroup of an elliptic curve E over the ring of integers $\mathbf{R}_p$ of $\mathbf{C}_p$ implicit in [K-pPMF]. In particular, if ω generates $\Omega^1_{E/\mathbf{R}_p}$ and E has a canonical subgroup C_E, knowlege of the Hasse invariant of the reduction of (E,ω) modulo p is equivalent to knowledge of the pair $(C_E, \omega|_{C_E})$.

1. Group Schemes of order p. Let μ denote the group of $(p-1)$-st roots of unity in $\mathbf{Z}_p$ and A the subring of $\mathbf{Q}_p$

$$\{r \in \mathbf{Z}_p : \exists n \in \mathbf{N}, p^n r \in \mathbf{Z}[\mu, 1/(p-1)]\}.$$

Suppose R is an A-algebra, e.g., a p-adically complete ring with identity. For $a \in R$, let $R_a = R[x]/(x^p + ax)$ and $B_a = \operatorname{Spec} R_a$ and for $\epsilon \in \mu_{p-1}(R)$, $[\epsilon]_a$ the automorphism of B_a corresponding to $x \mapsto \epsilon x$.

If $a \neq 0$, the automorphisms α of B_a such that $\alpha \circ [\epsilon]_a = [\epsilon]_a \circ \alpha$ for $\epsilon \in \mu$ are the $[\gamma]_a$ for $\gamma \in \mu_{p-1}(R)$. Suppose $\exists b \in R$ such that $ab = p$. Because then, $\mathrm{d}(x^p + ax) = a(1+bx^{p-1})\mathrm{d}x$ and $(1+bx^{p-1})(1-bx^{p-1}/(1-p)) = 1$, $\Omega^1_{B_a/R} \cong B_a/aB_a$.

PROPOSITION 1.1. *Suppose G is a group scheme of order p over R. Then the R-module of invariant differentials $\Omega_{G/R}$ on G over R is cyclic and if ω is a generator, there are $a, b \in R$ such that $ab = p$ and a unique isomorphism of schemes $h: B_a \to G$ such that $h \circ [\epsilon]_a = [\epsilon]_G \circ h$, for $\epsilon \in \mu$, and $h^*\omega = (1 + bx^{p-1})^{-1}\mathrm{d}x$. Moreover, $\Omega_{G/R} \cong R/aR$, a is determined modulo a^2R and b is determined modulo pR. In particular, if R is integrally closed and G is self-dual both a and b are determined modulo pR.*

Proof. We know from [O-T, pp.13-14] that there are universal constants $w_i \in A$, $i \geq 1$, such that $w_1 = 1$, $w_j \in \mathbf{Z}_p^*$, $j < p$, $w_p = pw_{p-1}$ and there are $u, v \in R$ such that $uv = w_p$, an isomorphism $g: B_{-u} \to G$ over R for which the pullback of the group law on G to B_{-u} is

$$F^v(X,Y) = X + Y + \frac{1}{1-p}\sum_{i=1}^{p-1} \frac{v}{w_i w_{p-i}} X^i Y^{p-i}. \tag{1}$$

(Call the group scheme, (B_{-u}, F^v), $G_{v\,u}$.) In particular, $g \circ [\epsilon]_{-u} = [\epsilon]_G \circ g$, for $\epsilon \in \mu$. Suppose $f(x)\mathrm{d}x$ is a differential on B_{-u} invariant with respect to this group law. Then,

$$f(x)\mathrm{d}x + f(y)\mathrm{d}y = f(F^v(x,y))(F^v_1(x,y)\mathrm{d}x + F^v_2(x,y)\mathrm{d}y). \tag{2}$$

---

*Received July 27, 2004; accepted for publication January 31, 2005.

†Department of Mathematcis, University of California, Berkeley, CA 94720-3840, USA (coleman @math.berkeley.edu).

In particular, after equating coefficients of $\mathrm{d}y$ and then setting $y = 0$, we have

$$f(0) \equiv f(x)(1 + \frac{vx^{p-1}}{w_{p-1}}) \bmod uR_{-u}.$$

Thus $\Omega_{G/R}$ is isomorphic to a sub-R-module of R/uR. We claim it is isomorphic to R/uR. This is true when $u = p$ and $v = w_{p-1}$ and $R = \mathbf{Z}_p$, for then $G = \mu_p$. The claim is equivalent to the statement that $\omega_{v\,u} := \mathrm{d}x/(1 + vx^{p-1}/w_{p-1})$ is an invariant differential on $G_{u\,v}$. Let $F = F^{w_{p-1}}$. Since $\mathrm{d}x/(1 + x^{p-1})$ is an invariant differential on $G_{p\,w_{p-1}}$, (2) implies

$$\frac{dx}{1 + x^{p-1}} = \frac{F_1(x,y)\mathrm{d}x}{1 + F(x,y)^{p-1}} \quad \text{on } B_p \text{ over } \mathbf{Z}_p.$$

Because $rF^{w_{p-1}r^{p-1}}(x,y) = F(rx,ry)$ in $\mathbf{Z}_p[x,y,r]$, this means as elements of $\mathbf{Z}_p[[x,y,z]]$,

$$\frac{1}{1 + zx^{p-1}} \equiv \frac{F_1^{w_{p-1}z}(x,y)}{1 + zF^{w_{p-1}z}(x,y)^{p-1}} \bmod (p, x^p)$$

which implies

$$\frac{dx}{1 + vx^{p-1}/w_{p-1}} = \frac{F_1^v(x,y)\mathrm{d}x}{1 + vF^v(x,y)^{p-1}/w_{p-1}}$$

on B_{-u} over R. This implies $dx/(1 + vx^{p-1}/w_{p-1})$ is an invariant differential on $G_{u\,v}$. Thus $\Omega_{G/R} \cong R/uR$ and $g^*\omega = r(1 + vx^{p-1}/w_{p-1})\mathrm{d}x$ for some $r \in R^*$. Let $a = -ur^{1-p}$ and $b = -v/(w_{p-1}r^{p-1})$. Then $j\colon B_{-u} \cong B_a$ via $x \mapsto x/r$ and $(g \circ j)^*\omega = \mathrm{d}x/(1 + bx^{p-1})$. So take $h = g \circ j$. The uniqueness follows from the comments before the proposition. The determination of the congruence classes follows the fact that $\Omega^1_{B_a} \cong B_a/aB_a$.

Finally, the dual of G is isomorphic to B_b and if G is isomorphic to its dual we must have $b = au^{p-1}$ fo some unit u. $\square$

In particular, when G is potentially self dual (i.e., self dual after a finite flat base extension) a and b are both determined $\bmod p$. Indeed, in this case, b is a unit times a. In [OT, pp. 13-14], without fixing a differential, it is shown that there exist a and b determined up to $(p-1)$-st powers of units and an isomorphism $B_a \to G$.

We can rephrase the above as follows:

Let $\check{G}$ denote the Cartier dual of G so that if S is an R-scheme, $\check{G}(S) = \underset{S}{Hom}(G_S, (\mu_p)_S)$. We have a collection of natural homomorphisms

$$\check{G}(S) \to \Omega_{G_S/S},$$
$$h \mapsto h^*\frac{\mathrm{d}T}{T}.$$

This determines an isomorphism of group schemes over R/aR

$$\check{G}_{R/aR} \to V(\Omega_{G/R})$$

where for a ring B and a B-module M, $V(M)$ denotes the associated vectorial group scheme over B. Giving a generator ω of $\Omega_{G/R}$ is equivalent to giving an isomorphism $V(\Omega_{G/R}) \to (\mathbf{G}_a)_{R/aR}$ and so, an isomorphism

$$\lambda_\omega\colon \check{G}_{R/aR} \to (\mathbf{G}_a)_{R/aR}.$$

One knows $\check{G}_{v\,u} \cong G_{u\,v}$ [O-T] and from (1) we see there is an evident isomorphism from $(G_{u\,v})_{R/uR}$ onto $(\mathbf{G}_a)_{R/uR}$. It is easy to see that this isomorphism is $\lambda_{\omega_{v\,u}}$ and

$$\lambda^*_{\omega_{v\,u}}\mathrm{d}T = \omega_{u\,v} \bmod uR.$$

We conclude from this discussion,

Proposition 1.2. *Suppose G is a group scheme of order p, ω generates $\Omega_{G/R}$, $\check{\omega}$ generates $\Omega_{\check{G}/R}$ and*

$$\lambda^*_{\omega}\mathrm{d}T \equiv \check{\omega} \ mod \ Ann_R(\Omega_{G/R}).$$

Then there exist $u, v \in R$, $uv = w_{p-1}$ and an isomorphism $h\colon G_{v\,u} \to G$ such that

$$h^*\omega = \omega_{v\,u} \quad and\ \check{h}^*\omega_{u\,v} = \check{\omega}.$$

Moreover, u and v are both determined modulo p.

2. Canonical subgroups.

Theorem 2.1. *Suppose R is a subring of $\mathbf{C}_p$, E is an elliptic curve over R and ω generates $\Omega^1_{E/R}$. Suppose $\mathcal{H}$ is a lifting of the Hasse invariant of (E,ω) mod$p$ to R and $v(\mathcal{H}) < p/(p+1)$. Then E has a canonical subgroup C_E and there is a unique isomorphism h from $B_{p/\mathcal{H}}$ onto C_E such that $h \circ [\epsilon]_{p/\mathcal{H}} = [\epsilon]_{C_E} \circ h$, for $\epsilon \in \mu$ and ω pulls back to $\mathrm{d}x/(1+\mathcal{H}x^{p-1})$.*

Proof. By [K-pPMF, p. 118], we can choose a local parameter X at 0 on E so that

$$\omega = (1 + \text{ higher order terms})\mathrm{d}X$$

and

$$[p](X) = Xg(X^{p-1})$$

where

$$g(T) = p + \mathcal{H}T + \sum_{r\geq 2} c_r T^r$$

and $c_r \equiv 0 \bmod p$ unless $r \equiv 1 \bmod p$. Let

$$h(T) = \frac{1}{p}g(\frac{p}{\mathcal{H}}T).$$

Because $v((p/\mathcal{H})^{p+1}) > (p+1)(1-p/(p+1)) = 1$,

$$h(T) = 1 + T + \sum_{r\geq 2} d_r T^r$$

where $|d_r| < 1$ and $d_r \to 0$ as $r \to \infty$. It follows from Weierstrass preparation that $h(T)$ has a zero u in R such that $|u+1| < 1$ so g has a zero which equals $-p/\mathcal{H}$ times a $(p-1)$-st power. Thus there is an isomorphism h of $B_{p/\mathcal{H}}$ onto C_E such that $h \circ [\epsilon]_{p/\mathcal{H}} = [\epsilon]_{C_E} \circ h$ for $\epsilon \in \mu$. The theorem follows from this and the fact that ω pulls back to a differential which is $\mathrm{d}x$ modulo $x\Omega_{B_{p/\mathcal{H}}/R}$. $\square$

The statement in the title makes sense for $p > 3$ and follows from the theorem since in this case $E_{p-1}(E, \omega)$ is a lifting of the Hasse invariant of the reduction of (E, ω) modulo p [K-pPMF, p. 98]. That the Hasse invariant of (E, ω) is determined by $(C_E, \omega|_{C_E})$ follows from the proposition.

3. E[p]; an example. Let notation be as in Theorem 2.1. Then, $E[p]$ is an extension of C_E by its Cartier dual. This, the above and results of Breuil (eg. [B, §3.1]) lead one to ask whether $E[p]$ may have a presentation in the form

$$\mathrm{Spec} R[x,y]/\big(x^p + \mathcal{H}x, y^p + (p/\mathcal{H})y - bx\big),$$

for some $b \in R$. This is true when E has CM by the maximal order in an imaginary quadratic field in which p splits (in which case E has ordinary reduction and one can take b to be 0). We verify that it also true in some other cases.

First, suppose R is the ring of integers in an extension K of $\mathbf{Q}_q$ and $q > 2$. Then E has a model with good reduction over R if the j-invariant is integral and all the 2-torsion is defined over K. Indeed, after possibly a quadratic twist, it has a model $y^2 = x(x-1)(x-\lambda)$ which has good reduction iff λ is not near 0, 1 or infinity iff the j-invariant is integral.

Second, if E has CM by an order S, 2 splits in S and $S \subset K$ then all the 2-torsion of E is defined over K. Indeed, for each prime ideal b above 2, there is only one non-trivial b-torsion point which must therefore be defined over K.

Now suppose p is a prime and $F = \mathbf{Q}(\sqrt{-p})$. Then because the prime $P := (\sqrt{-p})$ of the maximal order S of F is principal it splits completely in the Hilbert class field of F. Therefore, there is an elliptic curve defined over $F_P \cong \mathbf{Q}_p(\sqrt{-p})$ with potential CM by S. In fact, by a Galois argument it must have actual CM by S.

In conclusion, if $p + 1 \equiv 0 \mod 8$, there exists an elliptic curve E over $K := \mathbf{Q}_p[\sqrt{-p}]$ with CM by $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$ and a model over $R := \mathbf{Z}_p[\sqrt{-p}]$ with good reduction $\bar{E}$.

Since $\mathrm{End}_K E \cong \mathrm{End}_{\mathbf{F}_p} \bar{E}$, $[\sqrt{-p}]_E$ must reduce to plus or minus Frobenius. We may suppose it reduces to Frobenius. It follows that $\hat{E}$ is a Lubin-Tate group over R and respect to some parameter T, $[\sqrt{-p}]_F(T) = f(T) := \sqrt{-p} \cdot T + T^p$.

Theorem 3.1. *Suppose $p + 1 \equiv 0$ mod8 and A is a model with good reduction over the ring of integers R of a finite extension K of $\mathbf{Q}_p(\sqrt{-p})$ of an elliptic curve with CM by $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$. Then there exists a choice of $\sqrt{-p}$ so that*

$$A[p] \cong \mathit{Spec}\bigg(R[x,y]/\big(x^p + \sqrt{-p} \cdot x, y^p + \sqrt{-p} \cdot y - x\big)\bigg).$$

REFERENCES

[B] Breuil, C., *Groupes p-divisibles, groupes finis et modules filtrés*, Annals of Mathematics, 152 (2000), pp. 489–549.

[K-pPMF] Katz, N., *p-adic properties of modular forms*, Modular Functions of one Variable III, SLN 350 (1972), pp. 69–190.

[O-T] Oort, F. and J. Tate, *Group schmes of prime order*, Ann. Sci. Ecole Norm. Sup., 3 (1970), pp. 1–21.