25. Appendix: The cohomology of the Fermat group scheme

by B. Mazur

25.1. Let p be a prime number

$$\pi = 1 - \zeta_p$$

A = ring of integers in $\mathbb{Q}(\pi)$; $S = \operatorname{Spec} A$

B = ring of integers in $\mathbb{Q}(\sqrt{\pi})$; $T = \operatorname{Spec} B$.

Proposition 25.1.1. *Up to isomorphism in the category of finite flat group schemes over* T , *there is a unique diagram*

$$\mathbb{Z}/p \xrightarrow{i} C \xrightarrow{j} \mu_p$$

such that $j \circ i$ *brings the section* "1" *of* $\mathbb{Z}/p$ *to the section* "ζ_p" *of* μ_p , *the morphisms* i *and* j *are isomorphisms of group schemes when restricted to the base* $T[1/p]$, *and either one of the following conditions hold:*

a) *Neither* i *nor* j *are isomorphisms over* T .

b) *The above diagram is self-dual with respect to Cartier duality.*

Proof. A diagram of the above sort is "rigid" and therefore an elementary descent (and approximation) argument will show existence and uniqueness over T provided we have demonstrated existence and uniqueness over the complete local base T_p . Note that C/T_p is an Oort-Tate group scheme $G_{a,b}$ where a,b are elements of B_p such that $a \cdot b = p$. Since $G_{a,b}$ has its sections rational over T_p we must have $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$ both divisible by $p - 1$ (ord is normalized so that $\operatorname{ord}(\sqrt{\pi}) = 1$). Since $\operatorname{ord}(p) = 2(p-1)$ this leaves 3 possibilities for $(\operatorname{ord}(a),\operatorname{ord}(b))$, two of which account for the group schemes $\mathbb{Z}/p$ and μ_p .

Let j be a non-negative integer and let $(A_p^*)^{(j)}$ and $(B_p^*)^{(j)}$ denote the j^{th} "upper index" sub-group of the units in A_p and B_p respectively. Let

$$U(j) = (A_p^*)^{(j)} A_p^{*p}/A_p^{*p}$$
$$V(j) = (B_p^*)^{(j)} B_p^{*p}/B_p^{*p} \quad . \tag{25.1.2}$$

Proposition 25.1.3. The map $C \xrightarrow{j} \mu_p$ induces an isomorphism of $H^1(T_p,C)$ with the subgroup $V(p)$ in $V(0) = H^1(T_p,\mu_p)$

Proof. Theorem 1 of Roberts' Thesis ([4]; see also, [3, Prop. 9.3] identifies $H^1(T_p,C)$ with $V(j)$ where $j = 2p - \frac{\text{ord}(\text{disc } C)}{p-1}$. But an elementary computation gives that the discriminant of C/T_p is $(\sqrt{\pi})^{p(p-1)}$

To compute the global cohomology of C we need:

Lemma 25.1.4. The following square is Cartesian:

$$\begin{array}{ccc} H^1(T,C) & \longrightarrow & H^1(T_p,C) \\ \downarrow & & \downarrow \\ H^1(T,\mu_p) & \longrightarrow & H^1(T_p,\mu_p) \end{array}$$

Proof. Standard. Either by comparison of global to local exact sequences, or by a geometric argument interpreting H^1 as isomorphism classes of torseurs.

25.2. We will now compute the action of $G = \text{Gal}(T/S)$ on the cohomology of C. Over $S[1/p]$ the group scheme C descends to the constant group scheme $\mathbf{Z}/p$. Thus we have a natural action of G on $H^1(T[1/p],C)$. It is perhaps surprising that G leaves the subspace $H^1(T,C)$ stable; the proof that G does so comes from a combination of (25.1.3) and (25.1.4). Indeed, G preserves ord and consequently leaves the upper indexing filtration stable; it follows that G stabilizes

$H^1(T_p,C)$ in $H^1(T_p,\mu_p)$. We define

$$\tilde{H}^1(S,C) = H^1(T,C)^G . \tag{25.2.1}$$

Theorem 25.2.2. If p is odd

$$\tilde{H}^1(S,C) \simeq \{\alpha \in \mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p)^{*p} : (\alpha)=\underline{a}^p \text{ and } \alpha \equiv 1 \mod \pi^{\frac{p+1}{2}} \} .$$

Proof. From (25.1.4) one obtains that the square

$$\begin{array}{ccc} \tilde{H}^1(S,C) & \longrightarrow & \tilde{H}^1(S_p,C) \\ \downarrow & & \downarrow \\ \tilde{H}^1(S,\mu_p) & \longrightarrow & \tilde{H}^1(S_p,\mu_p) \end{array}$$

is Cartesian, where $\tilde{H}^1(S,\_) = H^1(T,\_)^G$. By Kummer theory

$$H^1(T,\mu_p) = \{\beta \in \mathbb{Q}(\sqrt{\pi})^*/\mathbb{Q}(\sqrt{\pi})^{*p} : (\beta) = \underline{b}^p\} .$$

Taking invariants gives

$$\tilde{H}^1(S,\mu_p) = H^1(S;\mu_p) = \{\alpha \in \mathbb{Q}(\mu_p)^*/\mathbb{Q}(\mu_p)^{*p} : (\alpha) = \underline{a}^p\}$$

as p is prime to $|G|$. Similarly $V(0)^G = U(0)$ and $V(p)^G = U(\frac{p+1}{2})$. This gives the theorem.

Corollary 25.2.3. If p is an odd regular prime,

$$\dim_{\mathbb{Z}/p\mathbb{Z}} \tilde{H}^1(S,C) = \begin{cases} \frac{p-5}{4} & \text{if } p \equiv 1 \pmod 4 \\ \frac{p-3}{4} & \text{if } p \equiv 3 \pmod 4 . \end{cases}$$

Proof. Let $U = A^*$ be the units of $\mathbb{Q}(\mu_p)$. Since $Cl(A)_p = (0)$ by assumption, $H^1(S,\mu_p) = U/U^p$. The eigenspace of U/U^p on which $Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts via the character $\varepsilon_{\mu_p}^i$ is non-trivial for $i = 1, 2, 4, 6, \ldots, p-3$. In each case $U/U^p(i)$ is one-dimensional; since p is regular it can be generated by a unit $u \equiv 1 + a\pi^i \pmod{\pi^{i+1}}$ where $a \not\equiv 0 \pmod{\pi}$ (compare (22.3.4)). The number of such $i \leq \frac{p+1}{2}$ is therefore the dimension of $\tilde{H}^1(S,C)$.

25.3. We shall apply the above computation to retrieve (part of) a result of Faddeev [1]. Let $K = \mathbb{Q}(\mu_p) = \mathbb{Q}(\pi)$ and let J/K be an abelian variety with complex multiplication by π, possessing a non-trivial point of order π rational over K. Suppose further that:

(i) p is an odd regular prime.

(ii) J achieves good reduction everywhere over T.

Examples of abelian varieties with multiplication by π satisfying (ii) are known for $p \equiv 1 \pmod 3$ and, more generally, for those primes p where the Jacobian of the Fermat curve of exponent p has a "tame" quotient (Gross-Rohrlich [2]). Define the π-Selmer number of J by

$$s_\pi = \dim_K J(K)\otimes_A K + \dim_{\mathbb{Z}/p\mathbb{Z}} Ш(J/K)_\pi .$$

Theorem 25.3.1. Under the above hypotheses:

$$s_\pi = \begin{cases} \frac{p-9}{4} & \text{if } p \equiv 1 \pmod 4 \\ \frac{p-7}{4} & \text{if } p \equiv 3 \pmod 4 . \end{cases}$$

Proof. Over T we have the following short exact sequence of group schemes:

$$0 \longrightarrow \ker \pi \longrightarrow J/T \xrightarrow{\pi} J/T \longrightarrow 0 \tag{25.3.2}$$

where J/T is the Néron model, which is an abelian scheme by hypothesis. Note

that π is an isogeny of abelian schemes, and therefore $\ker \pi$ is a finite flat group scheme over T of order $p = \deg \pi$. By the assumption that $J(K)$ has a non-trivial point of order π, it follows that $\ker \pi$ is isomorphic over $T[1/p]$ to the constant group $\mathbb{Z}/p$. By the discussion in (26.1) we may conclude that, over T, $\ker \pi$ is either isomorphic to $\mathbb{Z}/p$, C, or μ_p. Since $\ker \pi$ is isogenous to its dual, it cannot be either étale or of multiplicative type. It follows that $\ker \pi$ is isomorphic to C, and the exact sequence (26.3.2) gives the sequence:

$$0 \longrightarrow J(T)/\pi J(T) \longrightarrow H^1(T,C) \longrightarrow Ш(J/T)_\pi \longrightarrow 0$$

in flat cohomology. The $G = \mathrm{Gal}(T/S)$ invariants of this sequence remain exact, as p is prime to the order of G. A similar argument shows that

$$J(T)/\pi J(T)^G = J(K)/\pi J(K)$$

$$Ш(J/T)_\pi^G = Ш(J/K)_\pi .$$

The asserted formula then follows from $\dim_{\mathbb{Z}/p\mathbb{Z}} J(K)/\pi J(K) = 1 + \dim_K J(K) \otimes_A K$.

References:

1. Faddeev, D. K. Invariants of divisor classes for the curves $x^k(1-x) = y^\ell$ in an ℓ-adic cyclotomic field. Trudy Math. (in Russian) Inst. Steklov 64 (1961), 284-293.

2. Gross, B. H. and Rohrlich, D. E. Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. Inv. Math. 44 (1978), 201-224.

3. Mazur, B. and Roberts, L. Local Euler characteristics. Inv. Math. 9 (1970), 201-234.

4. Roberts, L. On the flat cohomology of finite group schemes. Thesis. Harvard (1968).

26. Bibliography.

1. Arthaud, N. On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication II. Preprint.

2. Berwick, W. E. H. Modular invariants expressible in terms of quadratic and cubic irrationalities. Proc. London Math. Soc. (2) 28 (1927), 53-69.

3. Birch, B. J. Diophantive analysis and modular functions. Proc. Bombay Colloquium on Algebraic Geometry (1968), 35-42.

4. Brumer, A. and Kramer, K. The rank of elliptic curves. Duke Math. J. (4) 44, (1977), 715-743.

5. Chowla, S. and Selberg, A. On Epstein's zeta-function. Crelle J. 227 (1967), 86-110.

6. Deligne, P. Courbes elliptiques: formulaire. Modular functions of one variable (Antwerp IV). Lecture Notes in Math. 476 (1975), 53-73.

7. Deligne, P. Valeurs de fonctions L et périodes d'intégrales. Proc. Symp. in Pure Math 33 (1979), part 2, 313-346.

8. Deuring, M. Die zetafunktion einer algebraischen Kurve von Geschlechte Eins. I - IV. Gott. Nach. (1953, 1955-1957).

9. Gross, B. and Koblitz, N. Gauss sums and the p-adic Γ-function. Annals Math. 109 (1979), 569-581.

10. Gross, B. $\mathbb{Q}$-curves and p-adic L-functions. In preparation.

11. Lang, S. Cyclotomic fields. Springer-Verlag (1978).

12. Lang, S. Elliptic functions. Addison-Wesley (1973).

13. Ligozat, G. Courbes modulaires de niveau 11. Modular functions of one variable (Bonn V). Lecture Notes in Math. 601 (1977), 149-239.

14. Mazur, B. Modular curves and the Eisenstein ideal. Publ. Math. IHES 47 (1978), 33-186.

15. Oort, F. and Tate J. Group schemes of prime order. Ann. Sci. ENS, 4^e série (1970), 1-21.

16. Ribet, K. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. Inv. Math. 34 (1976), 151-162.

17. Robert, G. Nombres de Hurwitz et unités elliptiques. Thèse. Orsay (1977).

18. Roberts, L. On the flat cohomology of finite group schemes. Thesis. Harvard (1968).

19. Serre, J.-P. Abelian ℓ-adic representations and elliptic curves. Benjamin (1968).

20. Serre, J.-P. Linear representations of finite groups. Springer-Verlag (1977).

21. Serre, J.-P. and Tate, J. Good reduction of abelian varieties. Annals Math. 88 (1968), 492-517.

22. Shimura, G. Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan 11 (1971).

23. Shimura, G. On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. Nagoya Math. J. 43 (1971), 199-208.

24. Shimura, G. On the factors of the Jacobian variety of a modular function field. Jour. Math. Soc. Japan 25 (1973), 523-544.

25. Shimura, G. On the zeta-function of an abelian variety with complex multiplication. Annals Math. 94 (1971), 504-533.

26. Shimura, G. On the periods of modular forms. Math. Ann. 229 (1977), 211-221.

27. Swinnerton-Dyer, H. P. F. The conjecture of Birch and Swinnerton-Dyer, and of Tate. Proc. Driebergen Conference on local fields. Springer (1967), 132-157.

28. Tate, J. Algorithm for determining the type of a singular fibre in an elliptic pencil. Modular forms of one variable (Antwerp IV). Lecture Notes in Math. 476 (1975), 33-52.

29. Tate, J. The arithmetic of elliptic curves. Inv. Math 23 (1974), 179-206.

30. Tate, J. Endomorphisms of abelian varieties over finite fields. Inv. Math. 2, (1966), 134-144.

31. Tate, J. Local constants. Proc. Symposium on algebraic number fields. Academic Press (1977), 89-133.

32. Weil, A. Adèles and algebraic groups. Princeton: Institute for Advanced Study (1961).

33. Weil, A. Elliptic functions according to Eisenstein and Kronecker. Springer-Verlag (1976).

34. Weil, A. Über die Bestimmung Dirichletscher Reihen durch Funktional gleichungen. Math. Ann. 168 (1967), 149-156.

27. Index.