ON A THEOREM OF MAZUR AND ROBERTS.

By J. S. Milne.

The purpose of this paper is to give a short proof of a local flat duality theorem of Mazur and Roberts [3; 9.3], [2; 1.6], and to make some related remarks.

Let $R$ be a complete discrete valuation ring with finite residue field. If $N$ is a flat finite commutative group scheme over $R$ and $K$ is the field of fractions of $R$, then the flat (f.p.q.f.) cohomology group $H^1(R, N)$ may be regarded as a subgroup of $H^1(K, N \otimes_R K)$ [5; p. 293]. Let $\hat{N}$ be the Cartier dual of $N$. Then the theorem states:

**THEOREM.** If $K$ has characteristic zero, then $H^1(R, N)$ is the exact annihilator of $H^1(R, \hat{N})$ in the non-degenerate cup-product pairing [7; II Theorem 2]

$$H^1(K, N \otimes_R K) \times H^1(K, \hat{N} \otimes_R K) \rightarrow H^2(K, G_m) \simeq Q/Z.$$

We first prove a duality result for $p$-divisible groups. The definitions and results in [10; § 2] will be freely used.

Let $K$ be as in the theorem and let $\Gamma$ be the Galois group over $K$ of the algebraic closure $\bar{K}$ of $K$. If $G$ is a $p$-divisible group over $R$, we define $M_G = \bigcup G(R_L)$ where $L$ runs over all finite Galois extensions of $K$ contained in $\bar{K}$ and $R_L$ is the integral closure of $R$ in $L$. $M_G$ becomes a discrete $\Gamma$-module under the obvious action. Multiplication by $p^r$ is surjective on $M_G$ by [10; 2.4 Cor. 1] and has kernel $G_p(\bar{K})$ because the torsion subgroup of $G(R_L)$ may be identified with $G(L)$.

If $G$ is étale then $G(R_L)^r = G(R)$ because in this case, $G(R_L)$ can be identified with $G(L)$; if $G$ is connected then the same equality holds because $G(R_L)$ can be identified with the group of points on the formal group associated to $G$; the equality for a general $G$ now follows from [10; Prop. 4], and from this it follows that $(M_G)^r = G(R)$.

We shall use $A^*$ to denote the Pontryagin dual of a locally compact abelian group $A$, and if $\phi: A \rightarrow B$ is a homomorphism of abelian groups we write $A_\phi$ and $B^{(\phi)}$ for the kernel and cokernel respectively of $\phi$.

Received April 21, 1971.
**Lemma.** $G(R)$ is canonically isomorphic to $H^1(\Gamma, M_\delta)^*$, where $G(R)$ is given the topology induced by that of $R$ and $H^1(\Gamma, M_\delta)$ is given the discrete topology, provided that the torsion subgroups of $G(R)$ and $\hat{G}(R)$ are finite.

(The reader will check easily that the torsion subgroup of $G(R)$ is infinite if and only if $G^{st}$ contains $\mathbb{Q}_p/Z_p$ as a subgroup, and that the lemma is false for $G = \mathbb{Q}_p/Z_p$.)

**Proof.** From the cohomology sequence of

\[(*) \quad 0 \rightarrow G_\nu(\hat{K}) \rightarrow M_G \xrightarrow{p^\nu} M_G \rightarrow 0\]

we get an exact sequence

\[(***) \quad 0 \rightarrow G(R)^{\langle p \rangle} \rightarrow H^1(\Gamma, G_\nu(\hat{K})) \rightarrow H^1(\Gamma, M_G)_{p^\nu} \rightarrow 0.\]

$G(R)^{\langle p \rangle}$ maps into the subgroup $H^1(R, G_\nu)$ of

\[H^1(\Gamma, G_\nu(\hat{K})) = H^1(\hat{K}, G_\nu \otimes_R K)\]

because $(**)$ is compatible with the cohomology sequence over $R$ coming from

\[0 \rightarrow G_\nu \rightarrow G \xrightarrow{p^\nu} G \rightarrow 0.\]

Since $H^1(R, G_\nu)$ and $H^1(R, \hat{G}_\nu)$ annihilate each other in the pairing of the theorem ([4; p. 279] or [2; p. 347]) it follows that $G(R)^{\langle p \rangle}$ and $\hat{G}(R)^{\langle p \rangle}$ annihilate each other in the same pairing. Thus the cup-product isomorphisms $H^1(\Gamma, G_\nu(\hat{K})) \rightarrow H^1(\Gamma, \hat{G}_\nu(\hat{K}))^*$ induce injections $G(R)^{\langle p \rangle} \rightarrow H^1(\Gamma, M_\delta)_{p^\nu}^*$ which in the limit give an injection

\[G(R) = \lim_{\rightarrow} G(R)^{\langle p \rangle} \rightarrow (\lim_{\rightarrow} H^1(\Gamma, M_\delta)_{p^\nu})^* = H^1(\Gamma, M_\delta)^*.\]

To prove that this map is surjective it suffices to prove that $[G(R)^{\langle p \rangle}] = [H^1(\Gamma, M_\delta)]$ (where $[S]$ denotes the number of elements in a set $S$). By [7; II Thm. 5], the Euler-Poincaré characteristic of $\hat{G}_1(\hat{K})$, $\chi(\hat{G}_1(\hat{K})) = (R: pR)^{-h}$ where $h$ is the height of $\hat{G}$ (or $G$). From the cohomology sequence of $(*)$ (with $\nu = 1$) we get that

\[\chi(\hat{G}_1(\hat{K}) = \frac{[\hat{G}(R)_{p}][H^2(\Gamma, \hat{G}_1(\hat{K}))]}{[\hat{G}(R)^{\langle p \rangle}][H^1(\Gamma, M_\delta)]}.\]

The required equality now follows from: (i) $[H^2(\Gamma, \hat{G}_1(\hat{K}))] = [G(R)_{p}]$ (see [7; II Thm. 2]); (ii) $[G(R)^{\langle p \rangle}]/[G(R)_{p}] = (R: pR)$ where $d$ is the dimension of $G$ (the theory of the logarithm [10; 2.4] shows that $G(R)$ is isomorphic to $R^d$ apart from finite groups); (iii) same statement for $\hat{G}$; (iv) $d + \hat{d} = h$ [10; Prop. 3].
Proof of the Theorem. In order to be able to apply the lemma, we use Oort's theorem [6] to embed $N$ in an exact sequence

$$
0 \to N \to G \overset{\phi}{\to} H \to 0
$$

in which $G$ and $H$ are $p$-divisible groups over $R$. (***) induces an exact sequence $0 \to N(R) \to M_g \to M_H \to 0$. $G$ (and so $H$) satisfy the condition of the lemma because, in Oort's construction, $G \otimes_R k = A(p)$ for some abelian variety $A$ over $k$.

Since $H^1(R, N)$ and $H^1(R, \hat{N})$ annihilate each other in the pairing of the theorem, we have

$$
[H^1(R, N)] [H^1(R, \hat{N})] \leq [H^1(K, N \otimes_R K)] = [H(R)^{(\phi)}] [H^1(\Gamma, M_G)^{\phi}]
$$

(where $\phi$ has also been used to denote the maps induced on the cohomology groups). From the cohomology sequences over $R$ of (***) and its dual, we get that

$$
[H^1(R, N)] = [H(R)^{(\phi)}][H^1(R, G)^{\phi}] \supseteq [H(R)^{(\phi)}]
$$

$$
[H^1(R, \hat{N})] = [\hat{G}(R)^{(\hat{\phi})}][H^1(R, \hat{H})^{\hat{\phi}}] \supseteq [\hat{G}(R)^{(\hat{\phi})}].
$$

From the lemma, $\hat{H}(R) \overset{\phi}{\longrightarrow} \hat{G}(R)$ is dual to the map $H^1(\Gamma, M_G) \overset{\phi}{\longrightarrow} H^1(\Gamma, M_H)$, and so $[\hat{G}(R)^{(\hat{\phi})}] = [H^1(\Gamma, M_G)^{\phi}]$. It follows now that all these inequalities must actually be equalities, and this proves the theorem.

Remarks. 1. The above lemma is closely related to a duality theorem of Tate [8] and, in fact, our proof of the lemma mimics a proof of Tate's of the theorem (cf. [9]).

If $X$ is an abelian scheme over $R$ and $G = X(p)$, then $G(R) = X(K) \otimes \mathbb{Z}_p$ and $H^1(\Gamma, M_G) = H^1(\Gamma, X(K)) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and so Tate's theorem for $X$ is equivalent to the lemma for $X(p)$ (all $p$).

2. The lemma can be used to prove that $H^2(\Gamma, M_G) = 0$ if $\hat{G}(R)^{\text{tors}}$ is finite. ($H^i(\Gamma, M_G) = 0$ for $i \geq 2$ because $\Gamma$ has strict cohomological dimension 2). The cohomology sequence of (*) (with $\nu = 1$) gives an exact sequence

$$
0 \to H^1(\Gamma, M_G)^{(\phi)} \to H^2(\Gamma, G_1(K)) \to H^2(\Gamma, M_G)_p \to 0.
$$

If $G(R)^{\text{tors}}$ also is finite, then the lemma implies that $[H^1(\Gamma, M_G)^{(\phi)}] = [\hat{G}(R)_p]$ and [7; II Thm. 2] implies that $[\hat{G}(R)_p] = [H^2(\Gamma, G_1(K))]$. Thus $H^2(\Gamma, M_G)_p = 0$ and this implies that $H^2(\Gamma, M_G) = 0$ because it is a $p$-torsion group (multiplication by $l \neq p$ is an automorphism of $M_G$).
If \( G = \mathbb{Q}_p/\mathbb{Z}_p \) then \( H^2(\Gamma, M_G) \) is dual to \( \lim \downarrow \mathcal{U}_p^\nu(R) \) (loc. cit.) which is zero.

If \( G = \mathcal{G}_m(p) = \mathbb{Q}_p/\mathbb{Z}_p \) then \( H^2(\Gamma, M_G) = Br(K)(p) = \mathbb{Q}_p/\mathbb{Z}_p \neq 0 \).

3. To complete the proof of all statements of \( [2; 1.6] \) one should show that \( H^i(R, N) = 0 \) for all \( i \geq 2 \). Probably the most elementary proof of this part of the theorem is that given in \( [2] \). However, it is quite easy to prove that, for any complete noetherian local ring \( R \) with finite residue field \( k \), \( H^i(R, N) = 0 \) for all \( i \geq 2 \).

Indeed, \( N \) may be embedded in an exact sequence \( 0 \to N \to G_0 \to G_1 \to 0 \) in which \( G_0 \) and \( G_1 \) are smooth group schemes of finite type over \( R \) \([3; 5.1(i)]\), and \([1; 11.7(2)]\) shows that \( H^i(R, G) \to H^i(k, G \otimes_R k) \) for \( i > 0 \) and \( G = G_0 \) or \( G_1 \). \( H^i(k, G \otimes_R k) = 0 \) for \( i \geq 2 \) \([7]\) which shows that \( H^i(R, N) = 0 \) for \( i \geq 3 \). If \( k \) is the algebraic closure of \( k \), then \( 0 \to N(k) \to G_0(k) \to G_1(k) \to 0 \) is exact and \( H^2(k, N(k)) = 0 \) which shows that \( H^1(k, G_0 \otimes k) \to H^1(k, G_1 \otimes k) \) is surjective. Hence \( H^1(R, G_0) \to H^1(R, G_1) \) is surjective, and \( H^2(R, N) = 0 \).

4. The argument in the last paragraph of the theorem shows that \( H(R)^{(\phi)} \to H^1(R, N) \) and \( H^1(R, G)_\phi = 0 \). In particular, if \( \phi \) is multiplication by \( p^\nu \) on \( G \) then (a) \( G(R)^{(p^\nu)} \to H^1(R, G_\nu) \) and (b) \( H^1(R, G)_p^{p^\nu} = 0 \).

(b) implies that \( H^1(R, G) = 0 \) and remark 3 implies that \( H^i(R, G) = 0 \) for \( i > 1 \).

The theorem implies the existence of an exact sequence,

\[ 0 \to H^1(R, G_\nu) \to H^1(K, G_\nu \otimes_R K) \to H^1(R, G_\nu)^* \to 0 \]

which, after (a), may be identified with,

\[ 0 \to G(R)^{(p^\nu)} \to H^1(K, G_\nu \otimes_R K) \to (G(R)^{(p^\nu)})^* \to 0. \]

After passing to the direct limit with \( \nu \) one obtains Mazur's duality theorem for \( p \)-divisible groups \([2; 3.5]\), viz. that there is an exact sequence

\[ 0 \to G(R) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(K, G \otimes_R K) \to G(R)^* \to 0. \]

(where \( H^1(K, G \otimes_R K) \) is defined to be \( \lim H^1(K, G_\nu \otimes_R K) \)).

5. As is explained in \([2]\), by introducing flat cohomology groups “with compact support” it is possible to give a statement of the theorem which is closer to the usual statements of Poincaré duality.

6. One may ask whether the theorem still holds if \( K \) has non-zero
characteristic $p$. That it does is essentially proved in [4]. We show how the theorem may be deduced from Lemma 5 of that paper. (It has also been proved by M. Artin and B. Mazur, unpublished).

**Step 0.** We may assume that $N$ has order a power of $p$.

**Proof.** If $p$ does not divide the order of $N$ then the theorem reduces to an easy statement about Galois cohomology (cf. [7, II Proposition 19]).

**Step 1.** There exists a finite extension $L/K$ of degree prime to $p$ such that $N \otimes_{R} R_{L}$ has a composition series all of whose quotients are of the form $N_{a,b}$ with $(a, b) = (t^{(p-1)c}, 0), (0, 0), \text{ or } (0, t^{(p-1)c})$. (Notation as in [4].)

**Proof.** This is shown in [4; pp. 278-9] except that we do not check that $L$ can be chosen so that $p \nmid [L : K]$. However, this is easy. (To get a composition series for $N \otimes_{R} L$ whose quotients are only $\mathfrak{q}_{p}, \mathfrak{a}_{p}$, or $\mathbb{Z}/p\mathbb{Z}$ one has to use that a $p$-group acting on an abelian $p$-group always has a fixed element.)

**Step 2.** If $L/K$ is finite of degree prime to $p$, and the theorem is true for $N \otimes_{R} R_{L}$ over $R_{L}$, then it is true for $N$ over $R$.

**Proof.** Since the Galois group of $K$ is solvable, we may reduce to considering a cyclic Galois extension of prime degree $l$. Let $\Gamma_{l} = \text{Gal}(L/K)$ be generated by $\sigma$. $\Gamma_{l}$ acts on $H^{1}(R_{L}, N)$. 

**Lemma.** The restriction map $r: H^{1}(R, N) \to H^{1}(R_{L}, N)$ is injective with image $H^{1}(R_{L}, N)^{\Gamma_{l}}$.

**Proof.** The exact sequence

$$0 = H^{1}(\Gamma_{l}, N(L)) \to H^{1}(K, N) \xrightarrow{r} H^{1}(L, N)^{\Gamma_{l}} \to H^{2}(\Gamma_{l}, N(L)) = 0$$

shows that the corresponding fact for cohomology over the fields is true. Interpret the cohomology groups as Čech cohomology groups and let $x \in H^{1}(R_{L}, N)^{\Gamma_{l}}$ be represented by the 1-cocyle $c$. As $\sigma \cdot c = x$, $c = r(c') + b$ where $c'$ is a 1-cocycle for $N$ over $K$ and $b$ is a 1-coboundary for $N$ over $L$. As $N(R_{L}) = N(L)$, $b$ is also a 1-coboundary for $N$ over $R_{L}$. Then $r(c') = c - b$ is a 1-cocycle for $N$ over $R_{L}$, fixed under $\Gamma_{l}$, and hence $c'$ is a 1-cocycle for $N$ over $R$. Thus $x \in r(H^{1}(R, N))$.

Now let $\langle , \rangle_{K}$ denote the cup-product pairing

$$H^{1}(K, N) \times H^{1}(K, N) \to H^{2}(K, G_{m}) \approx \mathbb{Q}/\mathbb{Z}$$

and let $\langle , \rangle_{L}$ denote the corresponding pairing over $L$. We will need the formulas,
THEOREM OF MAZUR AND ROBERTS.

(i) \( \langle rx, ry \rangle_L = l \langle x, y \rangle_L \) for \( x, y \in H^1(K, N) \);

(ii) \( \langle sx, sy \rangle_L = \langle x, y \rangle_L \) for \( x, y \in H^1(L, N) \).

Let \( y_0 \in H^1(K, \tilde{N}) \) be such that \( \langle x, y_0 \rangle_K = 0 \) for all \( x \in H^1(R, N) \). For any \( x \in H^1(R_L, \tilde{N}) \), one has \( lx = x_1 + (\sigma - 1)x_2 \) where \( x_1 = \sum_{i=0}^{l-1} \sigma^i x \) and \( x_2 = \sum_{i=1}^{l-1} \iota \sigma^i x \). \( \sigma x_1 = x_1 \), and so it may be written \( x_1 = r(x'_1) \). Thus,

\[
\langle x_1, ry_0 \rangle_L = l \langle x'_1, y_0 \rangle_K = 0,
\]

\[
\langle (\sigma - 1)x_2, ry_0 \rangle_L = \langle x_2, \sigma^{-1}ry_0 \rangle_L - \langle x_2, ry_0 \rangle_L = 0,
\]

and

\[
l \langle x, ry_0 \rangle = \langle x_1, ry_0 \rangle + \langle (\sigma - 1)x_2, ry_0 \rangle = 0.
\]

It follows that \( \langle x, ry_0 \rangle_L = 0 \) for all \( x \in H^1(R_L, N) \), that \( ry_0 \in H^1(R_L, N) \), and that \( y_0 \in H^1(R, N) \).

**Step 3.** \( H^i(R, N) = 0 \) for \( i \geq 2 \).

**Proof.** This is proved in remark 3 above.

To complete the proof, replace \( K \) by an extension field as in Step 1, and prove by induction on the order of \( \tilde{N} \) making use of [4, Lemma 5] and Step 3. This induction argument is written out in [4, p. 283].

7. Once one has remark 4, it is possible to give a proof of the Euler characteristic formula of Mazur and Roberts [3; 8.1] based on the methods of Tate [10; §2].

Indeed, consider the sequence (***) and let \( \Omega \) and \( \Omega' \) be the modules of formal differentials of the formal Lie groups associated to \( G \) and \( H \). Let \( (\omega_i)_{1 \leq i \leq d} \) and \( (\omega'_i)_{1 \leq i \leq d} \) be bases of \( \Omega \) and \( \Omega' \) consisting of translation-invariant differentials, and let \( \theta = \omega_1 \wedge \cdots \wedge \omega_d \) and \( \theta' = \omega'_1 \wedge \cdots \wedge \omega'_d \). If \( d\phi(\theta') = a\theta \) then the same argument as that in the proof of Lemma 1 and Proposition 3 of [10, §2] shows that the discriminant ideal of \( N \) over \( R \) is generated by \( g^2 \) where \( g \) is the rank of \( N \). On the other hand, the theory of the logarithm mapping shows that \( [H(R)^{(\phi)}/[G(R)_{\phi}] = (R : bR) \) where \( b \) is the determinant of \( t(\phi) : t_0(K) \to i_H(K) \) with respect to the dual bases of \( (\omega_i) \) and \( (\omega'_i) \) (cf. the second definition of log, [10; p. 169]). Obviously \( b = a \). Since \( G(R)_{\phi} = H^0(R, N) \) and \( H(R)^{(\phi)} \approx H^1(R, N) \), this proves the formula.

This proof is essentially the first proof in [3] except that there it has been made more elementary.

UNIVERSITY OF MICHIGAN.
REFERENCES.