DUALITY THEOREMS IN GALOIS COHOMOLOGY OVER NUMBER FIELDS

By JOHN TATE

1. Notation and terminology

Let X be a Dedekind ring with field of fractions k and let C be a commutative group scheme over X. Except in the special case $X=\mathbf{R}$ or $\mathbf{C}$ (real or complex field) we put, for all $r\in\mathbf{Z}$,

$$H^r(X,C)=\varinjlim_{K} H^r(G_{K/k},{}_{\cdot}C_Y),$$

the direct limit taken over all finite Galois extensions K of k in which the integral closure Y of X is unramified over X, where $G_{K/k}$ denotes the Galois group of such an extension, and where C_Y denotes the group of points of C with coordinates in Y. For example, if $X=k$, our notation coincides with that of [10]. For any X, the group $H^r(X,C)$ is the r-th cohomology group of the profinite group $G_X=\varprojlim_{K} G_{K/k}$ (fundamental group of Spec X) with coefficients in the G_X-module $\varinjlim C_Y$ of points of C with coordinates in the maximal unramified extension of X; a general discussion of the cohomology theory of profinite groups can be found in [5]. In the special case $X\approx\mathbf{R}$ or $\mathbf{C}$ we put

$$H^r(\mathbf{R},C)=\hat{H}^r(G_{\mathbf{C}/\mathbf{R}},C)\quad\text{and}\quad H^r(\mathbf{C},C)=\hat{H}^r(G_{\mathbf{C}/\mathbf{C}},C)=0,$$

where $\hat{H}$ denotes the complete cohomology sequence of the finite group G, in general non trivial in negative dimensions ([2], Ch. 12).

In our applications, X will be a ring associated with an algebraic number field, or with an algebraic function field in one variable over a finite constant field, and the group scheme C will be one of two special types, which we will denote by M and A, respectively. By M we shall always understand (the group scheme of relative dimension zero over X associated with) a finite G_X-module whose order, $|M|=\text{card } M$, is prime to the characteristics of the residue class fields of X. By A we shall denote an abelian scheme over X (i.e., an abelian variety defined over k having "non-degenerate reduction" at every prime of X).

Underlying our whole theory is the cohomology of the multiplicative group, $\mathbf{G}_m$, as determined by class field theory. For any M, we put $M'=\text{Hom}\,(M,\mathbf{G}_m)$. By our assumption that $|M|$ is invertible in X, we see that M' is a group scheme of the same type as M, namely the one associated with the G_X-module $M'=\text{Hom}(M,\mu)$ where μ denotes the group of roots of unity. Moreover we have $|M|=|M'|$, and $M\approx(M')'$. For any A we put $A'=\text{Ext}(A,\mathbf{G}_m)$, the dual abelian variety; then $A\approx(A')'$ by "biduality". Our aim is to discuss dualities between the cohomology of C and C' in both cases, $C=M$ and $C=A$. Notice that $\text{Ext}(M,\mathbf{G}_m)=0$ and $\text{Hom}(A,\mathbf{G}_m)=0$, so that in each case, C' denotes the only non-vanishing group in the sequence $\text{Ext}^r(C,\mathbf{G}_m)$. Thus our results are presumably special cases of a vastly more

general hyperduality theorem for commutative algebraic groups envisaged by Grothendieck, involving all the $\mathrm{Ext}^r(C, \mathbf{G}_m)$ simultaneously.

Finally, for any locally compact abelian group H, we let H^* denote its Pontrjagin character group.

2. Local results

Let k be either $\mathbf{R}$ or $\mathbf{C}$ (archimedean cases), or be complete with respect to a discrete valuation with finite residue class field (non-archimedean case). By local class field theory we have a canonical injection $H^2(k, \mathbf{G}_m) \to \mathbf{Q}/\mathbf{Z}$ which associates with each element of the Brauer group of k its "invariant" which is a rational number (mod. 1). Hence the cup product with respect to the canonical pairing $M \times M' \to \mathbf{G}_m$ gives pairings $H^r(k, M) \times H^{2-r}(k, M') \to \mathbf{Q}/\mathbf{Z}$.

THEOREM 2.1. *For all M and r the group $H^r(k, M)$ is finite and the pairing just discussed yields an isomorphism $H^r(k, M) \approx H^{2-r}(k, M')^*$.*

In particular we have $H^r(k, M) = 0$ for $r > 2$ when k is non-archimedean. In fact, even more is true in that case, namely the group G_k has strict cohomological dimension 2 in the sense of [5]. This fact, together with the theorem, can be proved easily using results of Nakayama [11], by writing $M = F/R$, where F is a $\mathbf{Z}$-free G_k-module.

THEOREM 2.2. *If k is archimedean, then $H^r(k, M)$ is an elementary abelian 2-group whose order is independent of r. If k is non-archimedean and $\mathfrak{o}$ is the valuation ring in k, then the "Euler-characteristic" of M has the value*

$$\chi(k, M) = \frac{|H^0(k, M)|\,|H^2(k, M)|}{|H^1(k, M)|} = \frac{1}{(\mathfrak{o} : |M|\mathfrak{o})}.$$

The archimedean case is trivial. In the non-archimedean case one uses the multiplicativity of χ to reduce to various special types of simple M's, only one of which is difficult. In that one the determination of χ is essentially equivalent to a result of Iwasawa [7] on the structure of $K^*/(K^*)^p$ as $G_{K/k}$-module, for a certain type of extension K/k.

In case of an abelian variety A defined over k the relationship $A' = \mathrm{Ext}(A, \mathbf{G}_m)$ leads to a "derived cup product" pairing:

$$H^r(k, A) \times H^{1-r}(k, A') \to \mathbf{Q}/\mathbf{Z},$$

as explained in [16]. The group $H^0(k, A)$, which is the group of rational points of A in k (modulo its connected component in case $k = \mathbf{R}$ or $\mathbf{C}$) is compact and totally disconnected because A is complete and k locally compact. On the other hand, we view $H^1(k, A)$ as discrete and have then

THEOREM 2.3. *For all A and r, the pairing just mentioned yields an isomorphism $H^r(k, A) \approx H^{1-r}(k, A')^*$ (possibly provided we ignore the p-primary components of the groups in case k is of characteristic $p > 0$).*

In the archimedean case this theorem is due to Witt [17]. For k non-archimedean of characteristic 0, the case $r = 0$ and 1 is proved in [16]. One

can simplify that proof and at the same time extend the result to all r (i.e., show $H^2(k,A)=0$ in the non-archimedean case), by applying theorems 2.1 and 2.2 to the kernel, M, of the isogeny $A \xrightarrow{m} A$. The same method works for k of positive characteristic, with the proviso in the theorem. Although that proviso is probably unnecessary, new methods will be required to remove it, possibly those of Shatz [15], where the analog of theorem 2.1 is proved for arbitrary finite commutative group schemes M over k.

Suppose now that k is non-archimedean with valuation ring $\mathfrak{o}$. Let M be a finite $G_{\mathfrak{o}}$-module such that $|M|$ is invertible in $\mathfrak{o}$.

THEOREM 2.4. *We have* $|H^0(\mathfrak{o},M)| = |H^1(\mathfrak{o},M)|$ *and* $H^r(\mathfrak{o},M)=0$ for $r>1$. *In the duality of Theorem* 2.1 *between* $H^1(k,M)$ *and* $H^1(k,M')$, *the subgroups* $H^1(\mathfrak{o},M)$ *and* $H^1(\mathfrak{o},M')$ *are the exact annihilators of each other.*

The first statements follow from the fact that $G_{\mathfrak{o}}$ is a free profinite group on one generator. The annihilation results from $H^2(\mathfrak{o},\mathfrak{G}_m)=0$. The *exact* annihilation now follows by counting, using theorems 2.1 and 2.2.

THEOREM 2.5. *If A is an abelian scheme over $\mathfrak{o}$, we have* $H^1(\mathfrak{o},A)=0$.

To prove this one has only to combine results of Lang [8] and Greenberg [6].

3. Global results

Let k be a finite extension of $\mathbb{Q}$ (case (N)), or a function field in one variable over a finite field (case (F)). Let S be a non-empty (possibly infinite) set of prime divisors of k, including the archimedean ones in case (N), and let k_S denote the ring of elements in k which are integers at all primes P *not* in S. For example, if S is the set of all prime divisors of k, then $k_S=k$. Let M be a finite module for the Galois group of the maximal extension of k unramified outside S, and such that $|M|k_S=k_S$. For each prime P *in* S, let k_P denote the completion of k at P. The localization maps $H^r(k_S,M)\to H^r(k_P,M)$ taken all together yield a map

$$H^r(k_S,M) \xrightarrow{\alpha_r} \coprod_{P\in S} H^r(k_P,M),$$

where the symbol $\coprod$ denotes the (compact) *direct product* for $r=0$, the (locally compact) *restricted direct product relative to the subgroups* $H^1(\mathfrak{o}_p,M)$ for $r=1$, and the (discrete) *direct sum* for $r\geqslant 2$. By Theorems 2.1 and 2.4, our local dualities yield isomorphisms

$$\coprod_{P\in S} H^r(k_P,M) \approx \Big[\coprod_{P\in S} H^{2-r}(k_P,M')\Big]^*.$$

Thus by duality we obtain maps

$$\coprod_{P\in S} H^r(k_P,M) \xrightarrow{\beta_r} H^{2-r}(k_P,M')^*,$$

namely $\beta_r=(\alpha'_{2-r})^*$, where α' is to M' as α is to M.

Let $\mathrm{Ker}^r(k_S,M)$ denote the kernel of α_r, that is, the group of elements in

$H^r(k_S, M)$ which are zero locally at all primes $P \in S$. There is a canonical pairing

$$(*) \qquad \mathrm{Ker}^2(k_S, M) \times \mathrm{Ker}^1(k_S, M') \to \mathbf{Q}/\mathbf{Z}$$

defined as follows: we represent the cohomology classes to be paired by a 2-cocycle f and a 1-cocycle f'. Then for each $P \in S$ we have, over k_P, a 1-cochain g_P and a 0-cochain g'_P such that $f = \delta g_P$ and $f' = \delta g'_P$. Also, since $H^3(k_S, \mathfrak{G}_m)$ has no non-zero elements of order dividing $|M|$, there is, over k_S, a 2-cochain h with coefficients in $\mathfrak{G}_m$, such that $f \cup f' = \delta h$. Then, over k_P, we have $\delta(g_P \cup f') = \delta h = \delta(f \cup g'_P)$ and $\delta(g_P \cup g'_P) = f \cup g'_P - g_P \cup f'$, so that for each P the cochains $(g_P \cup f') - h'_P$ and $(f \cup g'_P) - h$ are cocycles representing the same class, say x_P, in $H^2(k_P, \mathfrak{G}_m)$. We pair our original elements to the sum (over $P \in S$) of the invariants of these x_P; it is easy to see that the result is independent of the choices involved.

THEOREM 3.1. (*a*) *The pairing* (*) *just discussed is a perfect duality of finite groups.*

(*b*) α_0 *is injective,* β_2 *is surjective, and for* $r = 0, 1, 2$ *we have* $\mathrm{Im}\ \alpha_r = \mathrm{Ker}\ \beta_r$.

(*c*) α_r *is bijective for* $r \geqslant 3$.

Notice that these statements imply, and are, in turn, summarized by, the existence of an exact sequence:

$$0 \to H^0(k_S, M \xrightarrow{\alpha_0} \prod_{P \in S} H^0(k'_P, M) \xrightarrow{\beta_0} H^2(k_S, M')^* \to H^1(k_S, M) \searrow^{\alpha_1}$$

$$\prod_{P \in S} H^1(k_P, M) \swarrow_{\beta_1}$$

$$0 \leftarrow H^0(k_S, M')^* \xleftarrow{\beta_2} \prod_{P \in S} H^2(k_P, M) \xleftarrow{\alpha_2} H^2(k_S, M) \leftarrow H^1(k_S, M')^*$$

together with isomorphisms

$$H^r(k_S, M) \simeq \prod_{P \text{ real}} H^r(k_P, M) \quad \text{for} \quad r \geqslant 3,$$

where the unlabeled arrows in the exact sequence require the non-degeneracy of the pairing (*) for their definition.

I understand that a large part of Theorem 3.1 has been obtained independently by Poitou, and I suspect that the theorem is closely related to results of Shafaryevitch on the extension problem to which he alluded in his talk at this Congress.

If $M = \mu_m$, the group of mth roots of unity, then Theorem 3.1 summarizes well-known statements in class field theory. For general M, all statements of the theorem except case $r = 1$ of (*b*) can be proved by considering the pairing $M \times \mathrm{Hom}(M, C) \to C$, where C is the S-idele-class group of the maximal extension of k unramified outside S; denoting by G the Galois group of that extension, one shows that the resulting pairing $H^2(k_S, M) \times \mathrm{Hom}_G(M, C) \to \mathbf{Q}/\mathbf{Z}$ is non-degenerate, except that in case (*N*), there is a kernel on the right-hand side, namely the norm from K to k of $\mathrm{Hom}_{\mathbf{Z}}(M, D_K)$, where D_K is the connected component of the idele class group of a sufficiently large finite extension K of k. For finite S all groups involved are finite and the case $r = 1$ of (*b*) then follows by counting, using Theorem 2.2 and a method

of Ogg [12]. The passage to infinite S is not difficult. As a by-product of the proof one finds that the group G has strict cohomological dimension 2 for all primes l such that $lk_S = k_S$, except of course if $l=2$ and k is not totally imaginary.

Let A be an abelian scheme over k_S and let m be a natural number such that $mk_S = k_S$. For $X = k_S$ or $X = k_P$, we put:

$$H^r(X, A; m) = \varprojlim_n [\mathrm{Coker}\,(H^r(X, A) \xrightarrow{m^n} H^r(X, A))] \quad \text{for} \quad r \leqslant 0,$$

and $$H^r(X, A; m) = \varinjlim_n [\mathrm{Ker}\,(H^r(X, A) \xrightarrow{m^n} H^r(X, A))] \quad \text{for} \quad r \geqslant 1.$$

The localization maps give homorphisms

$$H^r(k_S, A; m) \xrightarrow{\alpha_r} \prod_{P \in S} H^r(k_P, A; m),$$

where now $\prod$ denotes the (compact) *direct product* for $r = 0$, and the (discrete) *direct sum* for $r \geqslant 1$. By Theorem 2.3 we have isomorphisms

$$\prod_{P \in S} H^r(k_P, A; m) \approx \left[\prod_{P \in S} H^{1-r}(k_P, A'; m)\right]^*$$

and consequently by duality we have maps $\beta_r = (\alpha'_{1-r})^*$:

$$\prod_{P \in S} H^r(k_P, A; m) \xrightarrow{\beta_r} H^{1-r}(k_S, A'; m)^*.$$

Let $\mathrm{Ker}^r(k_S, A; m)$ denote the kernel of α_r. For $r \geqslant 1$ and fixed m and A, this group is independent of S, by Theorem 2.5. Hence, $\mathrm{Ker}^1(k_S, A, m)$ is the m-primary component of the group of everywhere locally trivial principal homogeneous spaces for A over k. As is well known (and follows for example from [10], Theorem 5) this group is an extension of a finite group by a divisible group of "finite rank". There is canonical pairing

$$(**) \qquad \mathrm{Ker}^1(k_S, A; m) \times \mathrm{Ker}^1(k_S, A'; m) \to \mathbf{Q}/\mathbf{Z}$$

which can be defined either by a method using finite modules of m-primary division points and quite analogous to the definition of the pairing (*) above, or else by generalizing the method used by Cassels [3] in case dim $A = 1$, the generalization involving the "reciprocity law" of Lang [9].

THEOREM 3.2. *The pairing* (**) *annihilates only the divisible part of* $\mathrm{Ker}^1(k, A; m)$, *nothing more.*

In case dim $A = 1$ this theorem is due to Cassels [3], and his methods suffice for the case of general A, once one has Theorem 3.1 at one's disposal. Cassels' proof of skew symmetry in dimension 1 gives in the general case:

THEOREM 3.3. *If E is a divisor on A rational over k, and $\varphi_E : A \to A'$ the corresponding homomorphism, defined by $\varphi_E(a) = Cl(E_a - E)$, then for any $\alpha \in \mathrm{Ker}^1(k_S, A; m)$ the elements α and $\varphi_E(\alpha)$ annihilate each other in the pairing* (**).

There is also a canonical pairing

$$(***) \qquad \mathrm{Ker}^0(k_S, A; m) \times \mathrm{Ker}^2(k_S, A', m) \to \mathbf{Q}/\mathbf{Z}$$

and we have

THEOREM 3.4. *The map α_2 is surjective and its kernel is the divisible part of $H^2(k_S, A; m)$. Moreover, the following statements are equivalent:*

(i) *$\mathrm{Ker}^1(k_S, A; m)$ is finite (i.e. its divisible part is 0).*

(ii) *$Im\ \alpha_0 = \mathrm{Ker}\ \beta_0$, and the pairing (***) gives a perfect duality between the compact group Ker^0 and the discrete group Ker^2.*

Thus *if* these equivalent conditions (i) and (ii) are satisfied, we have an exact sequence

$$0 \to \coprod_{P \text{ real}} H^2(k_P, A'; m)^* \xrightarrow{\alpha_2^*} H^2(k_S, A'; m)^* \to H^0(k_S, A; m) \downarrow \alpha_0$$

$$\coprod_{P \in S} H^1(k_P, A, m) \xleftarrow{\alpha_1} H^1(k_S, A; m) \leftarrow H^1(k_S, A'; m)^* \xleftarrow{\beta_0} \coprod_{P \in S} H^0(k_P, A; m)$$

$$\beta_1 \downarrow$$

$$H^0(k_S, A'; m)^* \to H^2(k_S, A; m) \xrightarrow{\alpha_2} \coprod_{P \text{ real}} H^2(k_P, A; m) \to 0$$

quite analogous to (3.1), but with the appropriate shift of dimensions by 1.

4. Conjectures

In view of Theorem 3.4, one would have to be more pessimistic than I not to make the following

CONJECTURE 4.1. *$\mathrm{Ker}^1(k_S, A; m)$ is finite.*

There is some numerical evidence for this. For example, Selmer [13] has shown $\mathrm{Ker}^1(\mathbf{Q}, A, 3)$ is finite for all but a few elliptic curves A of the form $x^3 + y^3 = cz^3$ with $0 \leqslant c \leqslant 500$. A proof of 4.1 which yielded an a priori estimate for the order of $\mathrm{Ker}^1(k_S, A; m)$ would yield an effective procedure for computing the rank of, and finding generators for, the group of rational points on an abelian variety. In general, conjecture 4.1, is in the nature of an existence theorem for rational points of infinite order on abelian varieties.

Another conjecture in the same direction is that of Birch and Swynnerton-Dyer, discussed by Cassels in his talk at this Congress, to the effect that the rank of the group of rational points on an abelian variety A of dimension 1 is determined by the order of the pole of the zeta-function of A at $s = 1$. In case (F), i.e., if k is a function field over a finite field k_0 with q elements, the two conjectures are conjecturally equivalent. Namely, let Y be the complete non-singular model of k/k_0, and X the unique complete non-singular model of $k(A)/k_0$ which is minimal with respect to the morphism $X \to Y$. Let $\overline{X} = X \times \overline{k}_0$ be the variety obtained by extending the finite ground field to its algebraic closure, and let $\varphi : \overline{X} \to \overline{X}$ be the Frobenius morphism of $\overline{X}$ relative to k_0. Combining the result of Ogg [12] and Shafaryevitch [14] with recent results of M. Artin [1] on the Grothendieck cohomology of algebraic surfaces, one sees that conjecture 4.1 is equivalent in case (F) to

CONJECTURE 4.2. *The operator $\varphi - q$ annihilates exactly that part of $H^2(\bar{X},\mathbf{Z}_m)$ which is "algebraic" and rational over k_0, and no more.*

Clearly, 4.2 makes sense for any complete non-singular surface X over a finite field, not only for a pencil of elliptic curves. So generalized, conjecture 4.2 is equivalent, modulo Weil's well-known conjectures, to the following function theoretic analog of the conjecture of Birch and Swynnerton-Dyer.

CONJECTURE 4.3. *Let X be a complete non-singular algebraic surface defined over a finite field k_0. Then the order of the pole of the zeta-function of X at the point $s=1$ is equal to the number of algebraically independent divisors on X rational over k_0, i.e., to the k_0-picard number of X.*

Mumford has called my attention to the following interpretation of 4.3 in the special case when X is the product of two curves, one of which is elliptic.

CONJECTURE 4.3'. *Let E and E' be two complete non-singular curves defined over a finite field k_0, and suppose E is of genus 1. Then there exists a non-constant rational map $E' \to E$ defined over k_0 if and only if the zeta-function of E divides that of E'.*

In particular, if E and E' have genus 1, then they are isogenous over k_0 if and only if they have the same zeta-function. This beautiful statement has been proved by Birch and Swynnerton-Dyer and (independently) by Mumford, using results of Deuring [4] on the lifting to characteristic 0 of the Frobenius automorphism.

REFERENCES

[1]. ARTIN, M., *Grothendieck topologies*. Mimeographed notes, Harvard, 1962.

[2]. CARTAN-EILENBERG, *Homological Algebra*. Princeton Univ. Press, 1956.

[3]. CASSELS, J. W. S., Arithmetic on curves of genus 1 (IV). Proof of the Hauptvermutung, *J. reine angew. Math.*, 211 (1962), 95–112.

[4]. DEURING, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14 (1941), 197–272.

[5]. DOUADY, A., Cohomologie des groupes compacts totalement discontinus. *Séminaire Bourbaki*, 12, 1959–60, exposé 189.

[6]. GREENBERG, M., Schemata over local rings, *Ann. Math.*, 73, 1961, 624–648.

[7]. IWASAWA, K., On Galois groups of local fields. *Trans. Amer. Math. Soc.*, 80 (1955), 448–469.

[8]. LANG, S., Algebraic groups over finite fields. *Amer. J. Math.*, 78 (1956), 555–563.

[9]. LANG, S., *Abelian Varieties*. Interscience Publishers, New York, 1959.

[10]. LANG, S. & TATE, J., Principal homogeneous spaces over abelian varieties, *Amer. J. Math.*, 80 (1958), 659–684.

[11]. NAKAYAMA, T., Cohomology of class field theory and tensor products of modules I. *Ann. Math.*, 65 (1957), 255–267.

[12]. OGG, A., Cohomology of Abelian varieties over function fields, *Ann. Math.*, 76 (1962), 185–212.

[13]. SELMER, E. S., The diophantine equation $ax^3+by^3+cz^3=0$. *Acta Math.*, 85 (1951), 203–362.

[14]. SHAFARYEVITCH, I.R., Главные однородные пространства, определенные над полем функций. *Труды Математического института имени В. А. Стеклова*, Том LXIV.

[15]. SHATZ, S., *Cohomology of Artinian group schemes over local fields.* Thesis, Harvard, June, 1962.

[16]. TATE, J., W. C.-groups over P-adic fields, *Séminaire Bourbaki*, 1957–58, exposé 156.

[17]. WITT, E., Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellen Funktionenkörper, *J. reine angew. Math.*, 171 (1934), 4–11.