ACTA ARITHMETICA
LXXXVII.3 (1999)

The Hasse Principle modulo nth powers

by

Victor Scharaschkin (Ann Arbor, Mich.)

1. Introduction. Let L/K be a finite Galois extension of global fields with Galois group G. The Hasse Norm Principle states that if G is cyclic then an element of K is in the image of the global norm map iff it is in the image of all the local norm maps. Suppose $\mathrm{char}(K) \neq 2$ and let WK denote the Witt ring of quadratic forms over K. In [13] Leep and Wadsworth showed that a local-global principle holds for the transfer ideal $\mathcal{T}_{L/K}$ of WK iff the Hasse Norm Principle holds modulo squares (see below for a precise definition). Subsequently [14] they examined the validity of this modified Hasse Principle, especially for $\mathrm{Gal}(L/K) = (\mathbb{Z}/2)^d$ and $\mathbb{Z}/2 \times \mathbb{Z}/2^s$ with $s \geq 2$. They showed that in the first case the Hasse Principle mod squares always holds, even though the usual Hasse Principle may fail [13, Theorem 4.5], and that in the second case the Hasse Principle and the Hasse Principle mod squares are equivalent [14, Theorem 1].

In this paper we give a cohomological characterization of the Hasse Principle modulo nth powers. Our main result is Theorem 1.1 below, which is proved in Section 3. The characterization is comparable to the cohomological description of the usual Hasse Principle (see Theorem 2.2 below), and the proof is analogous, but requires the use of hypercohomology. The statement is as follows.

Theorem 1.1. *Let G act trivially on $\mathbb{Z}/n$. The following are equivalent*:

(a) *The Hasse Principle mod nth powers.*
(b) *The restriction map $H^2(G, \mathbb{Z}/n) \to \prod_v H^2(G^v, \mathbb{Z}/n)$ is injective.*
(c) *The corestriction map $\bigoplus_v H_2(G^v, \mathbb{Z}/n) \to H_2(G, \mathbb{Z}/n)$ is surjective.*

Using this theorem we examine in Section 4 the relationship between the standard Hasse Principle and the Hasse Principle mod n. Leep and Wadsworth showed [14, Corollary 2.4] that in the abelian case the Hasse

1991 *Mathematics Subject Classification*: Primary 11R37.

Principle implies the Hasse Principle mod nth powers, but in general an extra condition is needed for this implication to hold. See Example 4.2 and Proposition 4.1.

Finally we specialize to the case of squares, which is particularly interesting in light of its application to the theory of quadratic forms. In Section 6 we prove the following.

THEOREM 1.2. *The Hasse Principle mod squares holds for G iff the ring $H^*(G, \mathbb{Z}/2)$ contains no nilpotent elements of degree 2.*

This enables us to give many more examples where the Hasse Principle mod squares holds.

We now define the terms above. Let L/K be any finite extension of global fields. Let $\mathrm{Nm}_{L/K} : L^\times \to K^\times$ be the norm map, and for every prime v of K and w of L dividing v let $\mathrm{Nm}_{L_w/K_v} : L_w^\times \to K_v^\times$ be the local norm map. An element of $K^\times$ is a *local norm* if it is in the image of every local norm map, and a *global norm* if it is in the image of the global norm map. Every global norm is a local norm. The *Hasse* (*Norm*) *Principle* holds for L/K if every local norm is a global norm.

An element x of $K^\times$ is said to be a *local norm mod nth powers* if it lies in $\mathrm{Nm}_{L_w/K_v}(L_w^\times) \cdot K_v^{\times n}$ for every prime v and every w dividing v. It is a *global norm mod nth powers* if it lies in $\mathrm{Nm}_{L/K}(L^\times) \cdot K^{\times n}$. The *Hasse Norm Principle mod nth powers* (abbreviated to the *Hasse Principle mod* n) holds for L/K if every local norm mod nth powers is a global norm mod nth powers.

Throughout the rest of the paper L/K will be a finite Galois extension of global fields with Galois group G.

2. The Hasse Principle. Let L/K be as described. For each v fix w dividing v. Write L^v for L_w, and G^v for the decomposition group of w, $\mathrm{Gal}(L^v/K_v)$. We omit the subscripts on the various norm maps. All cohomology groups will be Tate groups. We write G^{ab} for the abelianization of G, G/G'. Restating the definitions we have the following.

PROPOSITION 2.1. (a) *The Hasse Principle holds iff the natural map*

$$\frac{K^\times}{\mathrm{Nm}(L^\times)} \to \bigoplus_v \frac{K_v^\times}{\mathrm{Nm}(L^{v\times})}$$

is injective.

(b) *The Hasse Principle mod n holds iff the natural map*

$$\frac{K^\times}{\mathrm{Nm}(L^\times) \cdot K^{\times n}} \to \bigoplus_v \frac{K_v^\times}{\mathrm{Nm}(L^{v\times}) \cdot K_v^{\times n}}$$

is injective.

The sum is taken over all the primes v of K. ∎

Theorem 1.1 is motivated by the following result in [8, VII.11.4].

THEOREM 2.2. *The following are equivalent*:

(a) *The Hasse Principle.*
(b) *The restriction map* $H^2(G, \mathbb{Q}/\mathbb{Z}) \to \prod_v H^2(G^v, \mathbb{Q}/\mathbb{Z})$ *is injective.*
(c) *The corestriction map* $\bigoplus_v H_2(G^v, \mathbb{Z}) \to H_2(G, \mathbb{Z})$ *is surjective.*

COROLLARY 2.3. *The Hasse Principle holds if either of the following are true.*

(a) $G = G^v$ *for some prime* v.
(b) $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$.

For example, the second condition of the corollary is satisfied if G is cyclic, since then by periodicity $H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H^0(G, \mathbb{Q}/\mathbb{Z}) = 0$. The group $H^2(G, \mathbb{Q}/\mathbb{Z})$ (or its dual) is called the *Schur multiplier.* It may sometimes be calculated using the following result.

THEOREM 2.4 [Schur, 1907]. *Let* $G = F/R$ *be a presentation of* G, *where* F *is free. Then*

$$H^2(G, \mathbb{Q}/\mathbb{Z}) \cong \frac{[F, F] \cap R}{[F, R]}.$$

If F *has rank* n *and* R *contains* r *relations, then* $r \geq n + s$ *where* s *is the minimum number of generators of* $H^2(G, \mathbb{Q}/\mathbb{Z})$. *In particular, if* $r = n$ *then* $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$.

P r o o f. See [11, II.4.6, II.4.7, pp. 50–52]. ∎

In general the Hasse Principle depends both on the group G and the collection of decomposition groups G^v which occur for L/K. Let us say that the Hasse Principle holds for the group G (rather than the extension L/K) if for every Galois extension L/K of global fields with $\mathrm{Gal}(L/K) = G$ the Hasse Principle holds for L/K. At every unramified prime v the groups G^v are cyclic, and hence the only contribution to the sums in Theorem 2.2(c) comes from ramified primes. However, Fröhlich [9, Corollary 1] showed that for any finite G there are infinitely many unramified Galois extensions L/K of number fields with $\mathrm{Gal}(L/K) = G$. Thus we have the following characterization.

PROPOSITION 2.5. *Let* G *be a finite group. Then the Hasse Principle holds for* G *iff* $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. ∎

Gurak [10, Corollary 3.2] states that the Hasse Principle holds for G iff all the p-Sylow subgroups of G, $\mathrm{Syl}_p(G)$, are cyclic. However, while the injectivity of the restriction map $H^r(G, \mathbb{Q}/\mathbb{Z}) \to H^r(\mathrm{Syl}_p(G), \mathbb{Q}/\mathbb{Z})$ shows that this is sufficient, it is not necessary. For example using Theorem 2.4 we find that $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$ for $G = Q_8$ the quaternion group. (In fact G has

periodic cohomology iff all its p-Sylow subgroups are cyclic or generalized quaternion ([5, VI.9.5, p. 157]), and then ([5, Ex. 4, p. 159]) $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$.)

Let $F \subseteq K \subseteq L$ be a tower of fields. It is not true in general that if the Hasse Principle holds for K/F and for L/K then it holds for L/F. A well known example is the extension $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{13})$. The Hasse Principle holds for L/K and K/F, since each is cyclic. But $\mathrm{Gal}(L/F) = G = \mathbb{Z}/2 \times \mathbb{Z}/2$ and one can show that the G^v all have order at most two (only the ramified primes need to be checked), and hence all the $H^2(G^v, \mathbb{Q}/\mathbb{Z})$ are zero. However, $H^2(G, \mathbb{Q}/\mathbb{Z}) = \mathbb{Z}/2$ ([11, II.2.12, p. 37]), so the Hasse Principle fails.

Under an additional condition, however, transitivity of the Hasse Principle does hold.

PROPOSITION 2.6. *Let L/F be a finite Galois extension of number fields, with $\mathrm{Gal}(L/F) = G$. Suppose G has a normal subgroup H with $H^2(H, \mathbb{Q}/\mathbb{Z}) = H^2(G/H, \mathbb{Q}/\mathbb{Z}) = 0$ and suppose that the orders of $(G/H)^{\mathrm{ab}}$ and H^{ab} are relatively prime. Then the Hasse Principle holds for G. That is, $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$.*

Proof. Let $K = L^H$. Then L/K and K/F are Galois, with $\mathrm{Gal}(L/K) = H$ and $\mathrm{Gal}(K/F) = G/H$. Thus the hypotheses imply that the Hasse Principle holds for L/K and K/F.

The Hochschild–Serre spectral sequence gives

$$H^2(G/H, \mathbb{Q}/\mathbb{Z}) \to \ker R \to H^1(G/H, H^1(H, \mathbb{Q}/\mathbb{Z}))$$

where $R = \mathrm{res} : H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(H, \mathbb{Q}/\mathbb{Z})$. Applying the hypotheses we have

$$\begin{aligned} \ker R &= H^2(G, \mathbb{Q}/\mathbb{Z}) \\ &\subseteq H^1(G/H, H^1(H, \mathbb{Q}/\mathbb{Z})) \\ &= \mathrm{Hom}((G/H)^{\mathrm{ab}}, \mathrm{Hom}(H^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})) \\ &\cong \mathrm{Hom}((G/H)^{\mathrm{ab}} \otimes H^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \\ &\cong (G/H)^{\mathrm{ab}} \otimes H^{\mathrm{ab}} \end{aligned}$$

and thus $H^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. ∎

THEOREM 2.7. *Let S_i be the simple factors of a composition series for G and suppose for all i that S_i is non-abelian and $H^2(S_i, \mathbb{Q}/\mathbb{Z}) = 0$. Then the Hasse Principle holds for G.*

Proof. Apply the previous proposition iteratively. If $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ and $S_i = G_i/G_{i-1}$ then $H^2(G_0, \mathbb{Q}/\mathbb{Z}) = 0$, $H^2(G_1/G_0, \mathbb{Q}/\mathbb{Z}) = H^2(S_1, \mathbb{Q}/\mathbb{Z}) = 0$ and $(G_1/G_0)^{\mathrm{ab}} = S^{\mathrm{ab}} = 0$, so the previous proposition applies and $H^2(G_1, \mathbb{Q}/\mathbb{Z}) = 0$. Eventually $H^2(G_n, \mathbb{Q}/\mathbb{Z}) = 0$. ∎

A complete table of $H^2(G, \mathbb{Q}/\mathbb{Z})$ for simple G is given in [11, Chapter 8, pp. 283–284].

3. Hypercohomology. In this section we prove our main result, Theorem 1.1, by suitably altering the proof of Theorem 2.2. We consider modified hypercohomology groups $\mathbb{H}^r(G, M^\bullet)$ where $M^\bullet$ is a complex of G-modules. We require $M^\bullet$ to be *bounded*, that is, to have only finitely many non-zero entries, beginning with the 0th position and extending right. In fact we shall only need complexes of the form $M^0 \to M^1$.

Let $M^\bullet$ be a cochain complex of G-modules. The *hypercohomology groups* $\mathbb{H}^r(G, M^\bullet)$ are the hyper-derived functors $\mathbb{R}^r(-^G)(M^\bullet)$. That is, if $I^\bullet$ is a complex of injective G-modules, $M^\bullet \to I^\bullet$, and $H^n(M^\bullet) \cong H^n(I^\bullet)$ for all n, then $\mathbb{H}^r(G, M^\bullet)$ is defined to be $H^r(I^{\bullet\,G})$. If $M^\bullet$ has only a single non-zero entry $M = M^0$, then the hypercohomology groups coincide with the cohomology groups $H^r(G, M)$. We can similarly obtain the Tate modified hypercohomology groups including negative indices, in analogy with the Tate cohomology groups. See [12].

The hypercohomology groups we shall need can be computed explicitly, at least for non-negative indices. Let $M^\bullet = M^0 \xrightarrow{\alpha} M^1$. For $i = 0, 1$ let $C^{r,i} = \{f : G^r \to M^i\}$ be the set of inhomogeneous r-cochains. Let d be the boundary map $C^{r,i} \to C^{r+1,i}$, and let $T^\bullet$ be the total complex associated with the double complex

$$\begin{array}{ccccc} C^{r-1,0} & \xrightarrow{d} & C^{r,0} & \xrightarrow{d} & C^{r+1,0} \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} \\ C^{r-1,1} & \xrightarrow{-d} & C^{r,1} & \xrightarrow{-d} & C^{r+1,1} \end{array}$$

The boundary map on $T^\bullet$ is $\alpha \pm d$, and we have

$$\mathbb{H}^r(G, M^0 \xrightarrow{\alpha} M^1) = \frac{\{(f, g) \mid df = 0,\ \alpha f = dg\}}{\{(df', \alpha f' - dg')\}}$$

where $f \in C^{r,0}$, $g \in C^{r-1,1}$, $f' \in C^{r-1,0}$ and $g' \in C^{r-2,1}$. Note also that $\mathbb{H}^r(G, M^0 \to 0) = H^r(G, M^0)$ and $\mathbb{H}^r(G, 0 \to M^1) = H^{r-1}(G, M^1)$.

Consider the short exact sequence of complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & A & = & A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & B & = & B & \longrightarrow & 0 & & \end{array}$$

where the entries of each complex are written vertically, and are zero except where indicated. This gives rise to a long exact sequence

$$\mathbb{H}^{r-1}(G, A \to 0) \to \mathbb{H}^r(G, 0 \to B) \to \mathbb{H}^r(G, A \to B) \to \mathbb{H}^r(G, A \to 0),$$

that is,

$$H^{r-1}(G,A) \to H^{r-1}(G,B) \to \mathbb{H}^r(G, A \to B) \to H^r(G,A). \tag{1}$$

Explicitly the map $H^{r-1}(G,B) \to \mathbb{H}^r(G, A \to B)$ is just $g \mapsto (0,g)$ and the map $\mathbb{H}^r(G, A \to B) \to H^r(G,A)$ is $(f,g) \mapsto f$.

We apply this to the complex $L^\times \xrightarrow{n} L^\times$ with $r = 1$. By Hilbert's Theorem 90, $H^1(G, L^\times) = 0$ and so we have

$$H^0(G,L^\times) \xrightarrow{n} H^0(G,L^\times) \to \mathbb{H}^1(G, L^\times \xrightarrow{n} L^\times) \to 0$$

and hence

$$\mathbb{H}^1(G, L^\times \xrightarrow{n} L^\times) \cong \frac{K^\times}{\mathrm{Nm}(L^\times) \cdot K^{\times n}}. \tag{2}$$

Proceeding analogously to the proof of Theorem 2.2, we form the sequence of complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathbf{C_L} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathbf{C_L} & \longrightarrow & 0 \end{array}$$

where $\mathbb{I}_L$ is the group of idèles, and $\mathbf{C_L}$ is the idèle class group $\mathbb{I}_L / L^\times$. We hence obtain

$$\begin{aligned} \mathbb{H}^0(G, \mathbb{I}_L \xrightarrow{n} \mathbb{I}_L) &\xrightarrow{\theta} \mathbb{H}^0(G, \mathbf{C_L} \xrightarrow{n} \mathbf{C_L}) \\ &\longrightarrow \mathbb{H}^1(G, L^\times \xrightarrow{n} L^\times) \xrightarrow{\psi} \mathbb{H}^1(G, \mathbb{I}_L \xrightarrow{n} \mathbb{I}_L). \end{aligned} \tag{3}$$

Proposition 3.1. *The hypercohomology of the idèles is given by*

$$\mathbb{H}^r(G, \mathbb{I}_L \xrightarrow{n} \mathbb{I}_L) \cong \bigoplus_v \mathbb{H}^r(G^v, L^{v\times} \xrightarrow{n} L^{v\times})$$

for all integers r.

Proof. For each v we have maps $G^v \to G$ and $\mathbb{I}_L \to L^{v\times}$, so we have an induced map from $\mathbb{H}^r(G, \mathbb{I}_L \xrightarrow{n} \mathbb{I}_L)$ into $\mathbb{H}^r(G^v, L^{v\times} \xrightarrow{n} L^{v\times})$ and hence into $\prod_v \mathbb{H}^r(G^v, L^{v\times} \xrightarrow{n} L^{v\times})$. We first show that it actually maps into the direct sum.

Since $H^r(G, \mathbb{I}_L) = \bigoplus_v H^r(G^v, L^{v\times})$ [8, VII.7.3] we have by (1) the following diagram, where the left and right vertical arrows are inclusions:

$$\begin{array}{ccccc} \bigoplus_v H^{r-1}(G^v, L^{v\times}) & \xrightarrow{f} & \mathbb{H}^r(G, \mathbb{I}_L \xrightarrow{n} \mathbb{I}_L) & \xrightarrow{g} & \bigoplus_v H^r(G^v, L^{v\times}) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_v H^{r-1}(G^v, L^{v\times}) & \longrightarrow & \prod_v \mathbb{H}^r(G^v, L^{v\times} \xrightarrow{n} L^{v\times}) & \xrightarrow{h} & \prod_v H^r(G^v, L^{v\times}) \end{array}$$

Abbreviate $\mathbb{H}^r(G, \mathbb{I}_L \xrightarrow{n} \mathbb{I}_L)$ by $\mathbb{H}$, $\bigoplus_v \mathbb{H}^r(G^v, L^{v\times} \xrightarrow{n} L^{v\times})$ by Σ, and write $\mathbb{H}'$ for the subgroup of $\mathbb{H}$ which maps into Σ.

Let $\phi \in \mathbb{H}$ map to (ϕ_v) in the product. The image of (ϕ_v) under h must be almost always zero by commutativity of the right square. Thus there is a $(\phi'_v) \in \Sigma$ with $(\phi_v - \phi'_v)$ in the kernel of h. Below we show that $\mathbb{H}'$ is isomorphic to Σ. Thus we may take $\phi' \in \mathbb{H}'$ to be the preimage of (ϕ'_v). Then $\phi - \phi'$ lies in $\ker g$, that is, in the image of f, hence in $\mathbb{H}'$. But this implies that $\phi \in \mathbb{H}'$, so $\mathbb{H} = \mathbb{H}'$.

To show that $\mathbb{H}' \cong \Sigma$, replace $\mathbb{H}$ with $\mathbb{H}'$ in the diagram above. This is valid since the image of $\bigoplus_v H^r(G^v, L^{v\times})$ is contained in $\mathbb{H}'$. Now we can replace the bottom row product with sums, and apply the Five Lemma to the resulting (suitably extended) diagram. ∎

Applying (2) and Proposition 3.1 to (3) we have

$$\frac{K^\times}{\mathrm{Nm}(L^\times)\cdot K^{\times n}} \xrightarrow{\psi} \bigoplus_v \frac{K_v^\times}{\mathrm{Nm}(L^{v\times})\cdot K_v^{\times n}}$$

so that the Hasse Principle mod n holds iff ψ is injective, that is, iff θ is surjective.

We now eliminate the hypercohomology by introducing a variant of Tate's cup product isomorphism.

PROPOSITION 3.2. *Let G be a finite group and $A^\bullet$ and $B^\bullet$ be bounded complexes of G-modules. Then for every pair (r, s) of integers there exists a cup product homomorphism*

$$\mathbb{H}^r(G, A^\bullet) \otimes \mathbb{H}^s(G, B^\bullet) \to \mathbb{H}^{r+s}(G, A^\bullet \otimes B^\bullet)$$

denoted by $\cup$.

Moreover, the cup product commutes (up to sign) with connecting homomorphisms in the following sense: if $B^\bullet = B_0 = B$ and we have short exact sequences

$$0 \to A^\bullet \to A'^\bullet \to A''^\bullet \to 0$$

and

$$0 \to A^\bullet \otimes B \to A'^\bullet \otimes B \to A''^\bullet \otimes B \to 0$$

then for $\alpha'' \in \mathbb{H}^r(G, A^\bullet)$ and $\beta \in \mathbb{H}^s(G, B)$,

$$(\delta(\alpha'')) \cup \beta = \delta(\alpha'' \cup \beta)$$

where δ is the connecting homomorphism. A similar statement is true for $A \otimes B^\bullet$.

Proof. This can be proved in the generality stated. Compare [12, Theorem 1.6] or [7, XII.4.1]. However, we only need the case $A^\bullet = A^0 \to A^1$ and $B^\bullet = B^0 = B$ a single G-module, and we can give an explicit formula in this case, at least for $r, s \geq 0$. Namely, if $(f, g) \in \mathbb{H}^r(G, A^\bullet)$ and

$h \in \mathbb{H}^s(G, B^\bullet) = H^s(G, B)$ then define

$$(f, g) \cup h = (f \cup h, g \cup h).$$

One can check on the level of cocycles that this gives the required map. ∎

THEOREM 3.3. *Let G be a finite group and let $M^\bullet$ be a bounded complex of G-modules whose entries are finitely generated free abelian groups. Let C be a G-module, v an element of $H^2(G, C)$, and suppose that for all subgroups H of G the following two conditions hold*:

(a) $H^1(H, C) = 0$.

(b) $H^2(H, C)$ *is cyclic of order* $|H|$, *generated by* $\mathrm{res}_{G/H}(v)$.

Then cup product with v defines an isomorphism

$$\_\_ \cup v : \mathbb{H}^{r-2}(G, M^\bullet) \xrightarrow{\cong} \mathbb{H}^r(G, M^\bullet \otimes C).$$

P r o o f. Define the *length* of a complex to be the number of non-zero entries it has. If $M^\bullet$ has length 1 the result is true by Tate's Theorem [19, IX.8.14, p. 149]. Assume inductively that the result holds for complexes of length $\leq k$. For the inductive step assume without loss of generality that $M^\bullet$ has the form

$$M^\bullet = M^0 \to M^1 \to \ldots \to M^k.$$

Let $M^{<k}$ be the complex

$$M^{<k} = M^0 \to M^1 \to \ldots \to M^{k-1}$$

and let T be the truncation map which drops the kth entry of a complex, so that the following sequence of complexes is exact:

$$0 \to M^k[-k] \to M^\bullet \xrightarrow{T} M^{<k} \to 0.$$

(Here $M^k[-k]$ is the complex consisting of the single entry M^k at position k.) Every entry of M is flat, so we may tensor with C to obtain

$$0 \to M_k[-k] \otimes C \to M^\bullet \otimes C \to M^{<k} \otimes C \to 0.$$

Applying the inductive hypothesis to the resulting hypercohomology sequence yields for all r the following diagram:

$$\begin{array}{ccccc}
\mathbb{H}^{r-2}(G, M^k[-k]) & \longrightarrow & \mathbb{H}^{r-2}(G, M^\bullet) & \longrightarrow & \mathbb{H}^{r-2}(G, M^{<k}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{H}^r(G, M^k[-k] \otimes C) & \longrightarrow & \mathbb{H}^r(G, M^\bullet \otimes C) & \longrightarrow & \mathbb{H}^r(G, M^{<k} \otimes C)
\end{array}$$

The diagram commutes by Proposition 3.2. By the inductive hypothesis, the vertical maps except the middle one are known to be isomorphisms. Since we have such a diagram for all r, applying the Five Lemma completes the induction. ∎

Let G act trivially on the complex $M^\bullet = \mathbb{Z} \xrightarrow{n} \mathbb{Z}$ and let $C = L^{v\times}$ or $C = \mathbf{C_L}$. Then the hypotheses of Theorem 3.3 hold by Class Field Theory. Thus from (3) (introducing the modified hypercohomology groups) we get

$$\begin{array}{ccccc} \mathbb{H}^0(G, \mathbb{I}_L \to \mathbb{I}_L) & \xrightarrow{\cong} & \bigoplus_v \mathbb{H}^0(G^v, L^{v\times} \xrightarrow{n} L^{v\times}) & \xrightarrow{\theta} & \mathbb{H}^0(G, \mathbf{C_L} \to \mathbf{C_L}) \\ & & \cong\downarrow & & \cong\downarrow \\ & & \bigoplus_v \mathbb{H}^{-2}(G^v, \mathbb{Z} \xrightarrow{n} \mathbb{Z}) & \xrightarrow{\Sigma \operatorname{cor}} & \mathbb{H}^{-2}(G, \mathbb{Z} \xrightarrow{n} \mathbb{Z}) \end{array}$$

The discussion above Proposition 3.2 shows that the Hasse Principle mod n holds iff θ is surjective, and hence iff $\Sigma\,\mathrm{cor}$ is surjective. Finally, from the sequence of complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & = & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle n} & & \downarrow & & \\ & & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n & & \end{array}$$

using the fact that $\mathbb{H}^r(G, A = A) = 0$ for any A, we have

$$\mathbb{H}^r(G, \mathbb{Z} \xrightarrow{n} \mathbb{Z}) \cong H^{r-1}(G, \mathbb{Z}/n).$$

We have now shown the equivalence of (a) and (c) of Theorem 1.1, since $H^{-3}(G, \mathbb{Z}/n) = H_2(G, \mathbb{Z}/n)$. In addition, parts (b) and (c) of the theorem are equivalent, by duality [5, VI.7.1]. This concludes the proof of Theorem 1.1.

Note that in the statement of Theorem 1.1 we may replace the product in (b) with the sum over any sufficiently large finite set of primes, since there are only finitely many possible distinct G^v. We shall use the theorem in this form in the remaining sections.

4. The Hasse Principle mod n. Theorem 1.1 will be our main tool in obtaining results about the Hasse Principle mod n. We first investigate the relationship between the usual Hasse Principle and the Hasse Principle mod n. The next two propositions generalize [14, Corollary 2.4] to the non-abelian case. We write G_n for elements killed by n, and G^* for $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Thus $H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) = G^{\mathrm{ab}\,*}$.

PROPOSITION 4.1. *Suppose the Hasse Principle holds for the extension L/K. Then the Hasse Principle mod n holds for L/K iff the natural map*

$$\delta : \bigoplus_v (G^{v\,\mathrm{ab}})_n \to (G^{\mathrm{ab}})_n$$

is surjective. In particular, it holds if $G_n \twoheadrightarrow (G^{\mathrm{ab}})_n$.

P r o o f. From the exact sequence

$$0 \to \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \xrightarrow{n} \mathbb{Q}/\mathbb{Z} \to 0$$

we obtain the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{G^{\mathrm{ab}\,*}}{n(G^{\mathrm{ab}\,*})} & \longrightarrow & H^2(G,\mathbb{Z}/n) & \longrightarrow & H^2(G,\mathbb{Q}/\mathbb{Z})_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & \bigoplus_v \dfrac{G^{v\,\mathrm{ab}\,*}}{n(G^{v\,\mathrm{ab}\,*})} & \longrightarrow & \bigoplus_v H^2(G^v,\mathbb{Z}/n) & \longrightarrow & \bigoplus_v H^2(G^v,\mathbb{Q}/\mathbb{Z})_n & \longrightarrow & 0
\end{array}$$

Here α, β and γ are restriction maps. One subtlety here is that the G^v are defined only up to conjugacy. Nonetheless α is well defined, since it maps into an abelian group. The sum is taken over a sufficiently large finite set, as described in Section 3.

By hypothesis γ is injective so by Theorem 1.1, the Hasse Principle mod n holds iff α is injective. The first statement now follows on taking duals.

The second statement is a consequence of the Chebotarev Density Theorem which implies that a conjugate of every cyclic subgroup of G occurs among the G^v, so that the G^v cover G^{ab}. For a proof of this theorem for arbitrary global fields see [15]. ∎

Example 4.2. *For the quaternion group $G = Q_8$ the Hasse Principle holds, and for every $k \geq 1$ the Hasse Principle mod $4k$ holds. However, the Hasse Principle mod squares may fail.*

P r o o f. From Theorem 2.4, $H^2(G,\mathbb{Q}/\mathbb{Z}) = 0$, so that the Hasse Principle holds for G. Since every element in G has order dividing $4k$, Proposition 4.1 implies that the Hasse Principle mod $4k$ holds. However, $G_2 = \{\pm 1\}$ and $(G^{\mathrm{ab}})_2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, so that δ in Proposition 4.1 is not surjective, and if all the G^v are cyclic then the Hasse Principle mod squares fails.

Proposition 4.3. *Suppose that the Hasse Principle mod m holds for L/K and n divides m. Then the Hasse Principle mod n holds for L/K provided that the natural map $G_n \to (G^{\mathrm{ab}})_n$ is surjective.*

P r o o f. Let $m = nt$. To simplify the calculations we work with homology groups instead of eventually taking duals. Since $H_1(G,\mathbb{Z}) = G^{\mathrm{ab}}$ the sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/t \to 0$ yields

$$0 \to G^{\mathrm{ab}} \xrightarrow{t} G^{\mathrm{ab}} \to H_1(G,\mathbb{Z}/t) \to 0$$

and hence $H_1(G,\mathbb{Z}/t) = G^{\mathrm{ab}}/t(G^{\mathrm{ab}})$. Now from the sequence

$$0 \to \mathbb{Z}/t \xrightarrow{n} \mathbb{Z}/nt \to \mathbb{Z}/n \to 0$$

we obtain

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bigoplus_v \dfrac{H_2(G^v,\mathbb{Z}/nt)}{n(H_2(G^v,\mathbb{Z}/nt))} & \longrightarrow & \bigoplus_v H_2(G^v,\mathbb{Z}/n) & \longrightarrow & \bigoplus_v \widehat{G^v} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \dfrac{H_2(G,\mathbb{Z}/nt)}{n(H_2(G,\mathbb{Z}/nt))} & \longrightarrow & H_2(G,\mathbb{Z}/n) & \longrightarrow & \widehat{G} & \longrightarrow & 0
\end{array}$$

where

$$\widehat{G} = \ker\left[\frac{G^{\mathrm{ab}}}{t(G^{\mathrm{ab}})} \xrightarrow{n} \frac{G^{\mathrm{ab}}}{nt(G^{\mathrm{ab}})}\right] = \frac{(G^{\mathrm{ab}})_n + t(G^{\mathrm{ab}})}{t(G^{\mathrm{ab}})} \cong \frac{(G^{\mathrm{ab}})_n}{[t(G^{\mathrm{ab}})]_n}.$$

The vertical maps are corestriction; the rightmost map is thus the natural map induced by inclusion [20, III.5.3]. From Theorem 1.1(c) we thus see that the Hasse Principle mod n holds iff the map

$$\bigoplus_v \frac{(G^{v\,\mathrm{ab}})_n}{[t(G^{v\,\mathrm{ab}})]_n} \to \frac{(G^{\mathrm{ab}})_n}{[t(G^{\mathrm{ab}})]_n}$$

is surjective, and the result follows as in Proposition 4.1. ∎

Let $\exp(G)$ denote the exponent of the group G.

PROPOSITION 4.4. *Let $e_N = \exp(K^\times/\operatorname{Nm}(L^\times))$, and let $e_G = \exp(G)$. Then the Hasse Principle mod e_N implies the Hasse Principle which implies the Hasse Principle mod e_G.*

Proof. Suppose first that the Hasse Principle mod e_N holds, and let x be a local norm. Then it is certainly a local norm mod e_Nth powers, and hence by hypothesis $x = y \cdot z^{e_N}$, where y is a global norm and $z \in K^\times$. By the definition of e_N, z^{e_N}, and hence x, are global norms. The second implication follows from Proposition 4.1. ∎

When G is abelian the situation is particularly simple. The following result is essentially Corollary 2.4 of [14].

COROLLARY 4.5. *Suppose G is abelian. Then the Hasse Principle mod m implies the Hasse Principle mod n for all $n \mid m$. Moreover, the following are equivalent*:

(a) *The Hasse Principle holds.*
(b) *The Hasse Principle mod n holds for all n.*
(c) *The Hasse Principle holds mod e_N, where $e_N = \exp(K^\times/\operatorname{Nm}(L^\times))$.*

Proof. Proposition 4.3 shows that the Hasse Principle mod m implies the Hasse Principle mod n for all $n \mid m$.

Proposition 4.1 shows that (a) implies (b), while (b) implies (c) trivially, and (c) implies (a) by Proposition 4.4. ∎

If G is abelian and has odd order then $e_N \mid e_G$ by a result of Opolka [16, Proposition 3], so that the conditions in Proposition 4.4 are equivalent. For example, if $G = (\mathbb{Z}/p)^d$ then the Hasse Principle is equivalent to the Hasse Principle mod p. An alternative proof of this is sketched in the next section.

5. The Hasse Principle mod p. In this section we concentrate on the Hasse Principle mod p for odd primes p. The cohomology rings $H^*(G, \mathbb{Z}/p)$ for odd p differ from $H^*(G, \mathbb{Z}/2)$, and so some results for the Hasse Principle mod p for odd p differ from those for the Hasse Principle mod squares, which is discussed in the next section.

We assume in this section that G is a p-group. This is no loss of generality, since for arbitrary G the restriction map $H^2(G, \mathbb{Z}/p) \to H^2(\mathrm{Syl}_p(G), \mathbb{Z}/p)$ is injective for any Sylow p-subgroup $\mathrm{Syl}_p(G)$ of G, so that the condition of Theorem 1.1 depends only on $\mathrm{Syl}_p(G)$. The following result is useful for calculations.

PROPOSITION 5.1. *Let $G = \mathbb{Z}/p^s$. Then the cohomology ring $H^*(G, \mathbb{Z}/p)$ of G is given abstractly as $\mathbb{F}_2[x_1]$ if $p^s = 2$ and $\mathbb{F}_p[x_1, y_2]/\langle x_1^2 \rangle$ otherwise. Here the subscript on the variable denotes its degree.*

Proof. See [3, p. 61]. ∎

The cohomology ring of an abelian group with coefficients in $\mathbb{Z}/p$ can now be calculated using the following Künneth formula [3, p. 62], which holds for any finite groups G_1 and G_2:

$$H^n(G_1 \times G_2, \mathbb{Z}/p) \cong \bigoplus_{r+s=n} H^r(G_1, \mathbb{Z}/p) \otimes H^s(G_2, \mathbb{Z}/p),$$

which gives as rings

$$H^*(G_1 \times G_2, \mathbb{Z}/p) \cong H^*(G_1, \mathbb{Z}/p) \otimes H^*(G_2, \mathbb{Z}/p). \tag{4}$$

For an abelian extension, the Hasse Principle is stronger than the Hasse Principle mod p (Corollary 4.5). However, if G is elementary abelian or has only two factors then the two principles are equivalent.

PROPOSITION 5.2. *Let $G = \mathbb{Z}/p^m \times \mathbb{Z}/p^n$, where $m \geq 2$. Then the following are equivalent*:

(a) *The Hasse Principle.*
(b) *The Hasse Principle mod p.*
(c) *There exists a prime v (necessarily ramified) for which $G^v = G$.*

Proof. In view of Corollary 4.5 and Theorem 2.2, it suffices to show that (b) implies (c). By Proposition 5.1 and (4), or simply by direct cocycle calculation, $x^2 = 0$ for all x in $H^1(G, \mathbb{Z}/p)$. (This is not true for $p = 2$.) Let $H^1(G, \mathbb{Z}/p) = \mathrm{Hom}(G, \mathbb{Z}/p)$ be generated by x and y. We shall show

that xy is in the kernel of the restriction map $H^2(G,\mathbb{Z}/p) \to H^2(H,\mathbb{Z}/p)$ for every maximal subgroup H, so that the map in Theorem 1.1(b) cannot be injective unless $G = G^v$ for some v.

Let H be a maximal subgroup of G, and let $\mathrm{res} = \mathrm{res}_{G/H}$. Let G/H have generator zH, and let $\phi : G \to \mathbb{Z}/p$ be defined by $t \mapsto j$ where $tH = z^jH$ in G/H. Then ϕ is a non-zero element of $H^1(G,\mathbb{Z}/p)$ with kernel H, so that $\mathrm{res}(\phi) = 0$. Now write $\phi = \alpha x + \beta y$, with $\alpha, \beta \in \mathbb{Z}/p$. We know that res is a ring homomorphism and $x^2 = 0$, so $\mathrm{res}(xy) = \mathrm{res}(\beta^{-1}x)\mathrm{res}(\phi) = 0$, provided $\beta \neq 0$. If $\beta = 0$ then $\alpha \neq 0$ and $\mathrm{res}(xy) = \mathrm{res}(\phi)\mathrm{res}(\alpha^{-1}y) = 0$. ∎

PROPOSITION 5.3. *Let G be a non-cyclic elementary abelian p-group (with p odd). Then the Hasse Principle and the Hasse Principle mod p are equivalent.*

P r o o f. We have to show that the Hasse Principle mod p implies the Hasse Principle. Since $pG = 0$, we have a homology diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigoplus_v \bigwedge^2 G^v & \longrightarrow & \bigoplus_v H_2(G^v,\mathbb{Z}/p) & \longrightarrow & \bigoplus_v G^v & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \Sigma} & & \downarrow & & \\ 0 & \longrightarrow & \bigwedge^2 G & \longrightarrow & H_2(G,\mathbb{Z}/p) & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

where σ and Σ are corestriction maps. Here we have used the canonical isomorphism $H_2(G,\mathbb{Z}) = \bigwedge^2 G$ of [5, V.6.4, p. 123], and written G $(= G^{\mathrm{ab}})$ for $H_1(G,\mathbb{Z})$. By hypothesis Σ is surjective, and we need to show that σ is. However this follows for $p \neq 2$ since both rows are canonically split. See [5, Ex. 4, p. 127], where the splitting map is given explicitly, but is defined only if 2 is invertible. ∎

6. The Hasse Principle mod squares. In this section we determine some conditions on $G = \mathrm{Gal}(L/K)$ which ensure that the Hasse Principle mod squares always holds for L/K (that is, so that the Hasse Principle mod squares holds for G). Unless otherwise stated G will be a 2-group. Our goal is to prove Theorem 1.2. We build on the following result, which is proved in [13, Theorem 4.5].

PROPOSITION 6.1. *The Hasse Principle mod squares holds for $(\mathbb{Z}/2)^d$.*

P r o o f. We give an alternative proof, applying Theorem 1.1(b). Let $G = (\mathbb{Z}/2)^d$. The Künneth formula (4) together with Proposition 5.1 gives that $H^*(G,\mathbb{Z}/2) \cong \mathbb{F}_2[x_1,\dots,x_d]$, where the x_i form a basis for $H^1(G,\mathbb{Z}/2) = \mathrm{Hom}(G,\mathbb{Z}/2)$. Suppose $\phi \in H^2(G,\mathbb{Z}/2) \setminus \{0\}$ restricts to zero on every decomposition subgroup. Then it certainly restricts to zero on every cyclic

subgroup. Write

$$\phi = \sum_{1 \le i \le j \le d} \varepsilon_{i,j}\, x_i x_j.$$

By linear algebra for any i and j we can choose a cyclic subgroup H with x_i and x_j non-vanishing on H, but all the other x_h vanishing there. Then $\mathrm{res}_{G/H}(\phi) = \mathrm{res}_{G/H}(x_i) \cdot \mathrm{res}_{G/H}(x_j) \neq 0$. ∎

This proof fails for a non-elementary 2-group or for a p-group for an odd prime because the cohomology ring is no longer an integral domain.

We can give another condition equivalent to Theorem 1.1(b), using a result of Quillen. We first need a lemma.

LEMMA 6.2. *Let $\mathcal{C}$ be the collection of cyclic subgroups of G, $\mathcal{E}$ the collection of elementary abelian 2-subgroups of G, and $\mathcal{T}$ the collection of subgroups of order 2. Then the injectivity of any of the three maps below implies the injectivity of the other two. In particular, the Hasse Principle mod squares holds for G iff some (hence all) of the r_i are injective.*

(a) $r_1 : H^2(G, \mathbb{Z}/2) \xrightarrow{\mathrm{res}} \bigoplus_{T \in \mathcal{T}} H^2(T, \mathbb{Z}/2)$,
(b) $r_2 : H^2(G, \mathbb{Z}/2) \xrightarrow{\mathrm{res}} \bigoplus_{E \in \mathcal{E}} H^2(E, \mathbb{Z}/2)$,
(c) $r_3 : H^2(G, \mathbb{Z}/2) \xrightarrow{\mathrm{res}} \bigoplus_{C \in \mathcal{C}} H^2(C, \mathbb{Z}/2)$.

Proof. If r_1 is injective then obviously so is r_2. If r_2 is injective and $x \in H^2(G, \mathbb{Z}/2)$ is non-zero then there is an $E \in \mathcal{E}$ such that $y = \mathrm{res}_{G/E}(x) \neq 0$. Now by Proposition 6.1 there is a cyclic subgroup C of E with $\mathrm{res}_{E/C}(y) \neq 0$, and hence r_3 is injective. Finally, suppose that r_3 is injective. Let $C \in \mathcal{C}$, and let $T \in \mathcal{T}$ be the subgroup of C of order 2. Then since $H^2(C, \mathbb{Z}/2) \overset{\mathrm{res}}{\cong} H^2(T, \mathbb{Z}/2) \cong \mathbb{Z}/2$, we see that r_1 is injective. ∎

Proof of Theorem 1.2. Suppose $z \in H^2(G, \mathbb{Z}/2) \setminus \{0\}$ is nilpotent. Let $z^m = 0$, and let T be a subgroup of G of order 2. Then $H^*(T, \mathbb{Z}/2) = \mathbb{F}_2[x]$ is reduced, but $0 = \mathrm{res}_{G/T}(z^m) = \mathrm{res}_{G/T}(z)^m$, so necessarily $\mathrm{res}_{G/T}(z) = 0$ for every such T. By Lemma 6.2 we see that the Hasse Principle mod squares fails for G.

Conversely, Quillen showed that the kernel of the map r_2 is nilpotent. An easy proof is given in [17]. Thus if $H^*(G, \mathbb{Z}/2)$ contains no nilpotent elements then r_2 is injective. ∎

We give several corollaries of Theorem 1.2 below.

COROLLARY 6.3. *Let G be an abelian 2-group. The Hasse Principle mod squares holds for G iff G is cyclic or elementary abelian.*

Proof. We need to prove "only if". Write G as a product of cyclic groups and use equation (4) and Proposition 5.1 to calculate the cohomology ring.

If G has more than one cyclic factor then $H^*(G, \mathbb{Z}/2)$ will contain a non-zero nilpotent element unless all the factors of G are of order 2. ∎

COROLLARY 6.4. *Let G and H be 2-groups whose cohomology rings $H^*(G, \mathbb{Z}/2)$ and $H^*(H, \mathbb{Z}/2)$ are reduced. Then $H^*(G \times H, \mathbb{Z}/2)$ is reduced, and thus the Hasse Principle mod squares holds for G, H and $G \times H$.*

Proof. The tensor product of two reduced k-algebras over a perfect field k is reduced [4, V, §15.5, Theorem 3(d), p. AV 125]. ∎

COROLLARY 6.5. *Let G be a group whose Sylow 2-subgroups are of the form $(\mathbb{Z}/2)^d \times D$ where $d \geq 0$ and D is a product of zero or more dihedral groups. Then the Hasse Principle mod squares holds for G.*

Proof. Let D_{2^n} denote the dihedral group with 2^n elements. Then $H^*(D_{2^n}, \mathbb{Z}/2) = \mathbb{F}_2[x_1, y_1, z_2]/\langle x_1 y_1 \rangle$, where the subscript on the variable denotes the degree [1, IV.2.7, p. 130]. This ring is reduced. ∎

Tables of cohomology rings $H^2(G, \mathbb{Z}/2)$ may be found in [18] and [6]. Unless G has large Sylow 2-subgroups we can thus determine immediately if the Hasse Principle mod squares holds for G. For example, there are 51 groups of order 32. Consulting the tables, we see that groups $7, 8, 23, 33, 34, 42, 49$ have reduced cohomology rings, and numbers $1, 27, 46, 47$ have nilpotent elements without any degree 2 nilpotents. Thus the Hasse Principle mod squares holds for these 11 groups.

Finally, we mention the case where the Hasse Principle mod squares is as far as possible from holding: when the obviously sufficient condition $G = G^v$ for some v is also necessary.

PROPOSITION 6.6. *Let H be a subgroup of G of index 2, and suppose $x \in \mathrm{Hom}(G, \mathbb{Z}/2)$ has kernel H. Then there is a long exact sequence*

$$H^{r-1}(G, \mathbb{Z}/2) \xrightarrow{x\cup} H^r(G, \mathbb{Z}/2) \xrightarrow{\mathrm{res}} H^r(H, \mathbb{Z}/2) \xrightarrow{\mathrm{cor}} H^r(G, \mathbb{Z}/2).$$

Proof. See [2, Satz 4.5]. ∎

The maximal subgroups H of G are exactly the H of index 2, necessarily normal. In the graded ring $H^*(G, \mathbb{Z}/2)$ define the *essential* cohomology of G to be

$$\mathrm{Ess}(G) = \bigcap_H \ker \mathrm{res}_{G/H},$$

where the intersection runs over all the maximal subgroups H of G (or, equivalently, over all proper subgroups of G). Thus $\mathrm{Ess}(G)$ consists exactly of the elements of the cohomology ring which restrict to zero on every proper subgroup. Let $\mathrm{Ess}^2(G)$ be the degree two elements of $\mathrm{Ess}(G)$ (together with

zero). Proposition 6.6 with $r = 2$ gives the formula

$$\text{Ш}^2(G) = \bigcap_{x \in H^1(G,\mathbb{Z}/2)} \langle x \rangle \tag{5}$$

where $\langle x \rangle$ denotes the ideal generated by x in the cohomology ring.

If $\text{Ш}^2(G) \neq 0$ then the Hasse Principle mod squares is clearly equivalent to the existence of a v with $G = G^v$. For example, we have the following generalization of [14, Theorem 1].

PROPOSITION 6.7. *Let $G = \mathbb{Z}/2^m \times \mathbb{Z}/2^n$ with $m \geq 2$. Then the following are equivalent*:

(a) *The Hasse Principle.*
(b) *The Hasse Principle mod squares.*
(c) *There exists a prime v with $G = G^v$.*

Proof. Following Corollaries 4.5 and 2.3, it suffices to show that (b) implies (c). Using the Künneth formula (4) and Proposition 5.1 we see that $H^*(G, \mathbb{Z}/2) = \mathbb{F}_2[x_1, y_2, z_1]/\langle x_1^2 \rangle$ if $n = 1$, and $\mathbb{F}_2[x_1, y_2, z_1, w_2]/\langle x_1^2, z_1^2 \rangle$ otherwise (subscripts denote degree). We now use equation (5). In both cases $\text{Ш}^2(G) = \langle x_1 \rangle \cap \langle z_1 \rangle \cap \langle x_1 + z_1 \rangle$ and $x_1 z_1 = x_1(x_1 + z_1) \in \text{Ш}^2(G)$. ∎

Note however that if G is abelian with more than 2 factors then $\text{Ш}^2(G) = 0$ so that Proposition 6.7 holds only for abelian 2-groups of rank 2. More generally, we can determine $\text{Ш}^2(G)$ from the tables of [18] and [6].

Acknowledgements. The author would like to thank Professor Milne (University of Michigan) for suggesting the use of hypercohomology in this problem, and Professor Wadsworth (University of California at San Diego) for carefully reading an earlier version of this paper and making many very helpful suggestions.

References

[1] A. Adem and R. J. Milgram, *Cohomology of Finite Groups*, Grundlehren Math. Wiss. 309, Springer, 1994.
[2] J. Arason, *Cohomologische Invarianten quadratischer Formen*, J. Algebra 36 (1975), 448–491.
[3] D. J. Benson, *Representations and Cohomology I*, Cambridge Stud. Adv. Math. 30, Cambridge Univ. Press, 1991.
[4] N. Bourbaki, *Algebra II*, English transl., Springer, 1990.
[5] K. S. Brown, *Cohomology of Groups*, Grad. Texts in Math. 87, Springer, 1982.
[6] J. F. Carlson, *The mod-2 cohomology of 2-groups*, http://www.math.uga.edu/~jfc/groups/cohomology.html.
[7] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton Univ. Press, 1956.
[8] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

[9] A. Fröhlich, *On non-ramified extensions with prescribed Galois group*, Mathematika 9 (1962), 133–134.
[10] S. Gurak, *On the Hasse Norm Principle*, J. Reine Angew. Math. 299 (1978), 16–27.
[11] G. Karpilovsky, *The Schur Multiplier*, Oxford Univ. Press, 1987.
[12] Y. Koya, *A generalization of class formation by using hypercohomology*, Invent. Math. 101 (1990), 705–715.
[13] D. B. Leep and A. R. Wadsworth, *The transfer ideal of quadratic forms and a Hasse norm theorem mod squares*, Trans. Amer. Math. Soc. 315 (1989), 415–431.
[14] —, —, *The Hasse theorem mod squares*, J. Number Theory 42 (1992), 337–348.
[15] J. Moshe, *The Cebotarev density theorem for function fields*: *an elementary approach*, Math. Ann. 261 (1982), 467–475.
[16] H. Opolka, *Norm exponents and representation groups*, Proc. Amer. Math. Soc. 111 (1961), 595–597.
[17] D. Quillen and B. B. Venkov, *Cohomology of finite groups and elementary abelian subgroups*, Topology 11 (1972), 317–318.
[18] D. J. Rusin, *The cohomology of the groups of order 32*, Math. Comp. 53 (1989), 359–385.
[19] J. P. Serre, *Local Fields*, English transl., Grad. Texts in Math. 67, Springer, 1979.
[20] E. Weiss, *Cohomology of Groups*, Academic Press, 1969.

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48109
U.S.A.
E-mail: victorvs@math.lsa.umich.edu

Received on 24.2.1998 (3342)