TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 313, Number 2, June 1989

CYCLIC EXTENSIONS OF $K(\sqrt{-1})/K$

JÓN KR. ARASON, BURTON FEIN, MURRAY SCHACHER AND JACK SONN

ABSTRACT. In this paper the height $\mathrm{ht}(L/K)$ of a cyclic 2-extension of a field K of characteristic $\neq 2$ is studied. Here $\mathrm{ht}(L/K) \geq n$ means that there is a cyclic extension E of K, $E \supset L$, with $[E : L] = 2^n$. Necessary and sufficient conditions are given for $\mathrm{ht}(L/K) \geq n$ provided $K(\sqrt{-1})$ contains a primitive 2^nth root of unity. Primary emphasis is placed on the case $L = K(\sqrt{-1})$. Suppose $\mathrm{ht}(K(\sqrt{-1})/K) \geq 1$. It is shown that $\mathrm{ht}(K(\sqrt{-1})/K) \geq 2$ and if K is a number field then $\mathrm{ht}(K(\sqrt{-1})/K) \geq n$ for all n. For each $n \geq 2$ an example is given of a field K such that $\mathrm{ht}(K(\sqrt{-1})/K) \geq n$ but $\mathrm{ht}(K(\sqrt{-1})/K) \not\geq n+1$.

1. INTRODUCTION

Let K be a field of characteristic 0, $\sqrt{-1} \notin K$. In this paper we are primarily concerned with the following embedding question: for which n does there exist a cyclic extension E of K, $E \supset K(\sqrt{-1})$, with $[E : K(\sqrt{-1})] = 2^n$? In considering this question we shall distinguish among several possibilities suggested by the Ulm theory applied to the character group of K. We briefly review this theory below.

Let E_{ab} denote the maximal abelian extension of a field E. The character group, $X(E)$, of E is defined to be the group of continuous homomorphisms from the profinite Galois group, $\mathrm{Gal}(E_{ab}/E)$, of E_{ab} over E to the discrete group Q/Z. $X(E)$ is a discrete abelian torsion group. Let p be a fixed prime. We denote the p-primary component of $X(E)$ by $X(E)_p$. The Ulm subgroups are defined inductively for any ordinal λ by

$$X(E)_p(0) = X(E)_p, \quad X(E)_p(\lambda + 1) = pX(E)_p(\lambda),$$

and for λ a limit ordinal, $X(E)_p(\lambda) = \bigcap_{\beta<\lambda} X(E)_p(\beta)$. The intersection of all $X(E)_p(\lambda)$ is the maximal divisible subgroup $DX(E)_p$ of $X(E)_p$. The elements of $X(E)_p$ of order p^n correspond by duality to cyclic extensions of E of degree p^n; this correspondence associates the cyclic p-extension L/E with the finitely many characters τ such that L is the fixed field of τ. Clearly, if τ_1

Received by the editors February 16, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12F10, 12G05; Secondary 11R20.
The research of the second author was supported by NSF grant DMS-8500883. The research of the third author was supported by NSF grant DMS-8500929.

and τ_2 are characters corresponding to L/E, then $\tau_1 \in X(E)_p(\lambda)$ if and only if $\tau_2 \in X(E)_p(\lambda)$. This leads to the notion of the height of L/E.

Definition. Let L/E be a cyclic p-extension and let $\tau \in X(E)_p$ correspond to L/E. If $\tau \notin DX(E)_p$ we define the height $\mathrm{ht}(L/E)$ of L/E to be λ where $\tau \in X(E)_p(\lambda)$, $\tau \notin X(E)_p(\lambda+1)$. If $\tau \notin DX(E)_p$ and $\mathrm{ht}(L/E) \geq \omega$, the first infinite ordinal, we say that L/E is reduced of infinite height. If $\tau \in DX(E)_p$ we define $\mathrm{ht}(L/E)$ to be ∞; here $\infty > \lambda$ for all ordinals λ. If $\mathrm{ht}(L/E) = \infty$ we say that L/E is divisible.

It is clear that if L is a cyclic p-extension of E then $\mathrm{ht}(L/E) \geq n$ if and only if there exists a cyclic p-extension F of E, $F \supset L$, with $[F : L] = p^n$. The statement that L/E is divisible is equivalent to the existence of a Galois extension F of E, $F \supset L$, with $\mathrm{Gal}(F/E)$ topologically isomorphic to the additive group, Z_p, of p-adic integers.

We begin our discussion by proving, in §2, a sufficient condition for a cyclic 2-extension L/E to have height $\geq n$. In §3 and §4 we consider the special case $K(\sqrt{-1})/K$. We show in §3 that if K is a number field and $\mathrm{ht}(K(\sqrt{-1})/K) \neq 0$, then $K(\sqrt{-1})/K$ is either divisible or reduced of infinite height; moreover, each of these possibilities occurs infinitely often with K an imaginary quadratic field. The case when K is an arbitrary field is considered in §4. While $\mathrm{ht}(K(\sqrt{-1})/K)$ can be 0, the results of §2 imply that $\mathrm{ht}(K(\sqrt{-1})/K)$ is never 1. We show, however, that for each natural number $n > 1$ there exists a field K such that $\mathrm{ht}(K(\sqrt{-1})/K) = n$.

We conclude this section by establishing some notation that will be maintained throughout the paper. We let $\mu(m)$ denote the group of mth roots of unity over a field of characteristic not dividing m. If E is a finite extension of K we let $\mathcal{N}(E/K)$ denote the image in K^* of the norm map $\mathcal{N}_{E/K}$ from E^* to K^*. The completion of K under a valuation π is denoted K_π. Finally, we let $\widetilde{K}$ denote the separable closure of K.

2. The height of a cyclic 2-extension

Let p be a prime, K a field of characteristic $\neq p$, and L a cyclic p-extension of K, $K \neq L$. We are interested in obtaining conditions that imply that $\mathrm{ht}(L/K) \geq n$.

Let $\mathcal{G} = \mathrm{Gal}(\widetilde{K}/K)$, $\mathcal{H} = \mathrm{Gal}(\widetilde{K}/L)$. Let $[L : K] = p^k$ and let λ be a generator for $\mathrm{Gal}(L/K)$. The choice of λ is equivalent to the choice of a homomorphism $f\colon \mathcal{G} \to Z/p^kZ$ with kernel $\mathcal{H}$. Then $\mathrm{ht}(L/K) \geq n$ if and only if f factors through the natural epimorphism from $Z/p^{k+n}Z$ to Z/p^kZ. Let $\mathcal{G}$ act trivially on Z/rZ and denote $H^i(\mathcal{G}, Z/rZ)$ by $H^i(K, r)$. Since $H^1(K, p^k) = \mathrm{Hom}(\mathcal{G}, Z/p^kZ)$, we see that $\mathrm{ht}(L/K) \geq n$ if and only if f is in the image of the map $H^1(K, p^{k+n}) \to H^1(K, p^k)$. Using the long exact sequence of cohomology groups corresponding to the short exact sequence: $0 \to Z/p^nZ \to Z/p^{k+n}Z \to Z/p^kZ \to 0$, it follows that $\mathrm{ht}(L/K) \geq n$ if and only if $\delta(f) = 0$ where $\delta\colon H^1(K, p^k) \to H^2(K, p^n)$ is the connecting homomorphism. Moreover, if $f(\sigma) = i + p^k Z$ and $f(\tau) = j + p^k Z$, then $\delta(f)$ is represented by the cocycle which maps (σ, τ) to $0 + p^n Z$ if $i + j < p^k$ and to $1 + p^n Z$ if $i + j \geq p^k$.

Now assume that $\mu(p^n) \subset K$ and let ζ be a generator for $\mu(p^n)$. The map $i + p^n Z \to \zeta^i$ is a $\mathscr{G}$-module isomorphism between $Z/p^n Z$ and $\mu(p^n)$ and so $H^2(K, p^n)$ is isomorphic to $H^2(\mathscr{G}, \mu(p^n))$. The p^n-power map on $\widetilde{K}^*$ induces an exact sequence of $\mathscr{G}$-modules: $1 \to \mu(p^n) \to \widetilde{K}^* \to \widetilde{K}^* \to 1$. This short exact sequence gives rise to a long exact sequence of Galois cohomology groups:

$$\cdots \to H^1(\mathscr{G}, \widetilde{K}^*) \to H^2(\mathscr{G}, \mu(p^n)) \to H^2(\mathscr{G}, \widetilde{K}^*) \to H^2(\mathscr{G}, \widetilde{K}^*) \to \cdots .$$

Since $H^1(\mathscr{G}, \widetilde{K}^*) = 0$ by Hilbert's Theorem 90, we see that $H^2(K, p^n)$ is isomorphic to the kernel ${}_{p^n}B(K)$ of the p^n-power map on $H^2(\mathscr{G}, \widetilde{K}^*) \cong B(K)$, the Brauer group of K. Under this isomorphism $\delta(f)$ goes to the class of the cyclic algebra $(L/K, \lambda, \zeta)$. Thus $\delta(f) = 0$ if and only if $\zeta \in \mathscr{N}(L/K)$ [7, Theorem 30.4]. This yields the following basic result of Albert [1, Theorem 11, p. 207].

Proposition 1 (A. A. Albert). *Let the context be as above and assume that $\mu(p^n) \subset K$. Then $\mathrm{ht}(L/K) \geq n$ if and only if $\mu(p^n) \subset \mathscr{N}(L/K)$.*

We now turn our attention to the case when $\mu(p^n) \not\subset \mathscr{N}(L/K)$. For p odd, necessary and sufficient conditions for $\mathrm{ht}(L/K) \geq n$ are obtained in [3, Théorème 1]. We consider the case $p = 2$ and determine a sufficient condition for $\mathrm{ht}(L/K) \geq n$ when $\mu(2^n) \not\subset K$. We begin with a preliminary result.

Lemma 2. *Let K be a field of characteristic $\neq 2$ such that $\mu(2^n) \subset K(\sqrt{-1})$. Suppose $\varphi \in H^2(K, 2^n)$ vanishes under both the natural map $H^2(K, 2^n) \to H^2(K(\sqrt{-1}), 2^n)$ induced by restriction and the natural map $H^2(K, 2^n) \to H^2(K, 2)$ induced by the surjection $Z/2^n Z \to Z/2Z$. Then $\varphi = 0$.*

Proof. We may clearly assume that $K(\sqrt{-1}) \neq K$. Let $K' = K(\sqrt{-1})$. We proceed by induction on n. Since the assertion is trivial for $n = 1$ we assume $n > 1$. The short exact sequence $0 \to Z/2^{n-1}Z \to Z/2^n Z \to Z/2Z \to 0$ gives rise to the long exact sequences of cohomology groups:

$$(*) \qquad \cdots \to H^1(K, 2) \xrightarrow{\delta} H^2(K, 2^{n-1}) \to H^2(K, 2^n) \to H^2(K, 2) \to \cdots ,$$

$$(**) \qquad \cdots \to H^1(K', 2^n) \to H^1(K', 2) \to H^2(K', 2^{n-1}) \to H^2(K', 2^n) \to \cdots .$$

Since φ vanishes in $H^2(K, 2)$ it comes from an element χ in $H^2(K, 2^{n-1})$. We consider the image of χ in $H^2(K', 2^{n-1})$ and also in $H^2(K, 2)$. Let $\mathscr{G} = \mathrm{Gal}(\widetilde{K}/K)$, $\mathscr{H} = \mathrm{Gal}(\widetilde{K}/K')$. Since $\mu(2^n) \subset K'$, the map $H^1(K', 2^n) \to H^1(K', 2)$ in $(**)$ is surjective and so the map $H^2(K', 2^{n-1}) \to H^2(K', 2^n)$ in $(**)$ is injective. Since φ vanishes in $H^2(K', 2^n)$ by assumption, χ vanishes in $H^2(K', 2^{n-1})$. Next, consider the map $H^2(K, 2^{n-1}) \to H^2(K, 2)$ induced by the natural epimorphism $Z/2^{n-1}Z \to Z/2Z$. Let ψ denote the image of χ in $H^2(K, 2)$. Since χ vanishes in $H^2(K', 2^{n-1})$, χ vanishes in $H^2(K', 2)$ and so ψ vanishes in $H^2(K', 2)$. Since $\psi \in H^2(K, 2) \cong {}_2B(K)$ is split by K', it follows that $\psi = [(K'/K, \sigma, d)]$ for some $d \in K^*$. But the image of $(-1) \smile (d)$ in the cup product pairing $H^1(\mathcal{G}, \mu(2)) \times H^1(\mathcal{G}, \mu(2)) \to H^2(\mathcal{G}, \mu(2) \otimes \mu(2)) \cong H^2(\mathcal{G}, \mu(2)) \cong {}_2B(K)$ is the class $[(K'/K, \sigma, d)]$ and so $\psi = (-1) \smile (d)$. A routine computation shows that $(d) \smile (d) = (-1) \smile (d)$ is the image of $(d) \in H^1(K, 2)$ under the composition of δ in $(*)$ and the map $H^2(K, 2^{n-1}) \to H^2(K, 2)$. Thus $\chi - \delta((d))$ vanishes in $H^2(K, 2)$. Since $\delta((d))$ vanishes in $H^2(K, 2^n)$, $\delta((d))$ vanishes in $H^2(K', 2^n)$. Since $H^2(K', 2^{n-1})$ injects into $H^2(K', 2^n)$, $\delta((d))$ vanishes in $H^2(K', 2^{n-1})$. Thus $\chi - \delta((d))$ vanishes in both $H^2(K', 2^{n-1})$ and $H^2(K, 2)$. By induction, $\chi - \delta((d)) = 0$. Since φ is the image of $\chi - \delta((d))$, $\varphi = 0$, proving the lemma.

Theorem 3. *Let K be a field of characteristic $\neq 2$ and let L be a cyclic 2-extension of K. Assume that $\mu(2^n) \subset K(\sqrt{-1})$. Then $\mathrm{ht}(L/K) \geq n$ if and only if $-1 \in \mathcal{N}(L/K)$ and $\mu(2^n) \subset \mathcal{N}(L(\sqrt{-1})/K(\sqrt{-1}))$.*

Proof. Let $\mathcal{G} = \mathrm{Gal}(\widetilde{K}/K)$, $\mathcal{H} = \mathrm{Gal}(\widetilde{K}/L)$, and let $[L : K] = 2^k$. Let $f: \mathcal{G} \to Z/2^kZ$ have kernel $\mathcal{H}$ and let λ be the corresponding generator for $\mathrm{Gal}(L/K)$. Then $\mathrm{ht}(L/K) \geq n$ if and only if $\delta(f) = 0$, where $\delta(f) \in H^2(K, 2^n)$ is as defined in the remarks preceding the lemma. By our description of $\delta(f)$ it is clear that the image of $\delta(f)$ in $H^2(K, 2)$ is the class of the cyclic algebra $(L/K, \lambda, -1)$, while the image of $\delta(f)$ in $H^2(K(\sqrt{-1}), 2^n)$ is the class of $(L(\sqrt{-1})/K(\sqrt{-1}), \sigma, \zeta)$ where ζ generates $\mu(2^n)$. The theorem is now an immediate consequence of the lemma and [7, Theorem 30.4].

Corollary 4. *Let K be a field of characteristic 0 with $\mu(2^n) \subset K(\sqrt{-1})$, $n \geq 2$. If $\mathrm{ht}(K(\sqrt{-1})/K) > 0$, then $\mathrm{ht}(K(\sqrt{-1})/K) \geq n$. In particular, $\mathrm{ht}(K(\sqrt{-1})/K)$ is never 1.*

Proof. Immediate from Theorem 3.

Corollary 4 holds, of course, also for fields K of characteristic $\neq 2$. The result, however, is uninteresting in that generality since $K(\sqrt{-1})/K$ is divisible if K has characteristic $\neq 0$.

It is worth pointing out that $\mathrm{ht}(K(\sqrt{-1})/K) = 0$ if and only if -1 is not a sum of two squares in K; this follows directly from Albert's criterion. Since $\mathrm{ht}(K(\sqrt{-1})/K)$ is never 1, the question arises as to what the possible heights of $K(\sqrt{-1})/K$ are. In the next section we consider this question when K is a number field.

3. The number field case

Throughout this section K will be an algebraic number field not containing $\sqrt{-1}$.

Theorem 5. *Let K be an algebraic number field not containing $\sqrt{-1}$ and suppose $\operatorname{ht}(K(\sqrt{-1})/K) > 0$. Then $K(\sqrt{-1})/K$ is either divisible or reduced of infinite height.*

Proof. Fix $n > 0$. We must show that there exists a cyclic extension E of K, $E \supset K(\sqrt{-1})$, with $[E : K(\sqrt{-1})] = 2^n$. By [2, Chapter 10, Theorem 6] such an E exists if and only if for each prime π of K and for each extension γ of π to $K(\sqrt{-1})$, $\zeta \in \mathscr{N}(\sqrt{-1})_\gamma/K_\pi)$ for every 2^nth root of unity $\zeta \in K_\pi$. (The condition of [2, Chapter 10, Theorem 6] that $c_{2^n} \in \mathscr{N}(K(\sqrt{-1})_\gamma/K_\pi)$ in the special case is easily seen to hold since, in the notation of that chapter, α_0 is a square in K.) Fix a prime π of K, γ a prime of $K(\sqrt{-1})$ extending π, and ζ a 2^nth root of unity in K_π. Since $\zeta \in \mathscr{N}(K(\sqrt{-1})_\gamma/K_\pi)$ if $\zeta = 1$ or if $\sqrt{-1} \in K_\pi$, we may assume that $\zeta = -1$. But $-1 \in K^2 + K^2$ since $\operatorname{ht}(K(\sqrt{-1})/K) > 0$ and so $-1 \in \mathscr{N}(K(\sqrt{-1})_\gamma/K_\pi)$. Thus $K(\sqrt{-1})/K$ must be either divisible or reduced of infinite height. Q.E.D.

We next show that each of the possibilities

$$K(\sqrt{-1})/K \text{ divisible} \quad \text{or} \quad K(\sqrt{-1})/K \text{ reduced}$$

of infinite height occurs infinitely often with K an imaginary quadratic field.

Theorem 6. *Let p and q be prime with $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$. Then:*

(1) *$Q(\sqrt{-2p}, \sqrt{-1})/Q(\sqrt{-2p})$ is divisible, and*

(2) *$Q(\sqrt{-2pq}, \sqrt{-1})/Q(\sqrt{-2pq})$ is reduced of infinite height.*

Proof. Let K be either $Q(\sqrt{-2p})$ or $Q(\sqrt{-2pq})$. Since K is totally imaginary and the rational prime (2) ramifies in K, $-1 \in K^2 + K^2$ [6, Theorem 1]. By Theorem 5, $K(\sqrt{-1})/K$ is either divisible or reduced of infinite height.

Let M be the composite of all Z_2-extensions of K. Then M is the composite of unique Z_2-extensions K_1 and K_2 where K_1 is the cyclotomic Z_2-extension of K, K_2/Q is normal, and $K_1 \cap K_2 = K$ [5, Theorem 3 and Remark (ii), p. 159]. Let $K_2 \supset E$ where $[E : K] = 2$. Since $K_1 \supset K(\sqrt{2})$, it follows that $K(\sqrt{-1})/K$ is divisible if and only if $K(\sqrt{-1})$ is contained in $E(\sqrt{2})$, the composite of all quadratic subextensions of M/K.

Being contained in a Z_2-extension of K, E must be unramified outside of (2). The results of [4, §3] imply that E must be either $K(\sqrt{-1})$ or $K(\sqrt{-2})$ if $K = Q(\sqrt{-2p})$. In particular, $Q(\sqrt{-2p}, \sqrt{-1})/Q(\sqrt{-2p})$ is divisible.

Suppose that $K = Q(\sqrt{-2pq})$ but $K(\sqrt{-1})/K$ is divisible. Then $K(\sqrt{-1})$ is contained in $E(\sqrt{2})$. The rational primes (p) and (q) ramify in K so there are unique primes π and γ of K extending, respectively, (p) and (q). By [5, Theorem 11] π and γ split completely in E. Since $p \equiv 1 \pmod 4$, (p) splits in $Q(\sqrt{-1})$ so π splits in $K(\sqrt{-1})$. Suppose $E \neq K(\sqrt{-1})$. Since π splits in both E and $K(\sqrt{-1})$, π splits in $K(\sqrt{2})$. But $p \equiv 5 \pmod 8$ so (p) is inertial in $Q(\sqrt{2})$, a contradiction. Thus $E = K(\sqrt{-1})$. But then q must split in $Q(\sqrt{-1})$, contradicting $q \equiv 3 \pmod 4$. Thus $Q(\sqrt{-2pq}, \sqrt{-1})/Q(\sqrt{-2pq})$ is reduced of infinite height. Q.E.D.

4. The arbitrary field case

We have seen that if K is a number field and $\mathrm{ht}(K(\sqrt{-1})/K) = n < \omega$, then $n = 0$. This raises the question of whether $\mathrm{ht}(K(\sqrt{-1})/K)$ is always either 0 or $\geq \omega$. Suppose F is a field with $\mathrm{ht}(F(\sqrt{-1})/F) = 0$. By Albert's theorem (Proposition 1), $-1 \notin F^2 + F^2$. Let E be a field containing F and let $K = F(x, y)$ where x is transcendental over F and $x^2 + y^2 = -1$. Then $\mathrm{ht}(E(\sqrt{-1})/E) \neq 0$ if and only if $-1 \in E^2 + E^2$. This is the case if and only if there is a specialization from K into E. It is easy to show that if $\mathrm{ht}(K(\sqrt{-1})/K) \geq n$, then $\mathrm{ht}(E(\sqrt{-1})/E) \geq n$ for every field $E \supset F$ with $\mathrm{ht}(E(\sqrt{-1})/E) \neq 0$. (This will also follow from the main result of this section.) For this reason it is natural to focus attention on the height of $K(\sqrt{-1})/K$. We shall show that for every $n > 1$ there is a field F such that $\mathrm{ht}(K(\sqrt{-1})/K) = n$ for K as above. (By Corollary 4, there are no fields E with $\mathrm{ht}(E(\sqrt{-1})/E) = 1$.) We begin with a preliminary result.

Lemma 7. *Let K be a field not containing $\sqrt{-1}$ and let L be a cyclic extension of K, $[L:K] = 4$, with $L \supset K' = K(\sqrt{-1})$. Then $\mathrm{ht}(L/K) \geq 1$ if and only if there is a $d \in K'$ such that $L = K'(\sqrt{d})$ and $\mathcal{N}_{K'/K}(d) = -1$.*

Proof. If such a d exists then $\mathcal{N}_{L/K}(\sqrt{d}) = \mathcal{N}_{K'/K}(-d) = \mathcal{N}_{K'/K}(d) = -1$. By Proposition 1 we have $\mathrm{ht}(L/K) \geq 1$. Conversely, if $\mathrm{ht}(L/K) \geq 1$, then by Proposition 1 there is an $a \in L$ such that $\mathcal{N}_{L/K}(a) = -1$. Let $\mathrm{Gal}(L/K) = \langle \lambda \rangle$, $\mathrm{Gal}(L/K') = \langle \mu \rangle$, where $\mu := \lambda^2$. Then $\mathcal{N}_{L/K'}(a\lambda(a)) = \mathcal{N}_{L/K}(a) = -1 = \mathcal{N}_{L/K'}(\sqrt{-1})$. By Hilbert's Theorem 90 there is an $e \in L^*$ such that $\sqrt{-1} = a\lambda(a)\mu(e)e^{-1}$. Let $b = a\lambda(e)e^{-1}$. Then $b\lambda(b) = \sqrt{-1}$ so $\mu(b) = \lambda(\sqrt{-1})\lambda(b^{-1}) = -b$. Let $d = b^2$. Then $\mu(d) = d$ so $d \in K'$ and $b \notin K'$ so $L = K'(\sqrt{d})$. Finally, $\mathcal{N}_{K'/K}(d) = b^2\lambda(b^2) = (b\lambda(b))^2 = -1$. Q.E.D.

Theorem 8. *Let F be a field in which -1 is not a sum of two squares. Let $K = F(x, y)$ where x is transcendental over F and $x^2 + y^2 = -1$ and suppose $\mathrm{ht}(K(\sqrt{-1})/K) \geq n$. Then $\mu(2^n) \subset F(\sqrt{-1})$.*

Proof. We may clearly assume that $n > 2$. Let $F' = F(\sqrt{-1})$ and let $K' = K(\sqrt{-1})$. Let M be a cyclic extension of K containing K' with $[M : K'] = 2^n$. Proceeding by induction, we may assume that F' contains a primitive 2^{n-1}th root of unity, ζ. We will prove that ζ is a square in F'.

Let σ generate $\mathrm{Gal}(K'/K)$ and let $t = x + y\sqrt{-1} \in K'$. Then $\mathcal{N}_{K'/K}(t) = x^2 + y^2 = -1$, so $\sigma(t) = -t^{-1}$. We have $x = (t - t^{-1})/2$, $y = (t + t^{-1})/2\sqrt{-1}$, so $K' = F'(t)$, a rational function field over F'.

Let $f \in F'[t]$ be a polynomial in t of degree m, f not divisible by t. Since $\sigma(t) = -t^{-1}$, $f^\sigma = t^{-m} f^*$ where f^* is a polynomial of degree m which is also not divisible by t. Since $\sigma^2 = \mathrm{id}$, we have $f^{**} = (-1)^m f$. For any two such polynomials f and g we have $(fg)^* = f^* g^*$. It follows that if f is irreducible, then f^* is also irreducible. We also have $(vf)^* = v^\sigma f^*$ for such a polynomial f and any $v \in F'$.

Let L be the unique subfield of M containing K' with $[L:K] = 4$. Since $n \geq 3$, $\mathrm{ht}(L/K) \geq 1$. By the lemma there is a $d \in K'$ such that $L = K'(\sqrt{d})$ and $\mathcal{N}_{K'/K}(d) = -1$. We may multiply d by any nonzero square in K' having norm 1 in K. In particular, we may multiply d by any even power of t and by -1. Since $\mathcal{N}_{K'/K}(d) = \mathcal{N}_{K'/K}(t) = -1$, Hilbert's Theorem 90 implies that there exists an element $e \in K' = F'(t)$ such that $d = te^{\sigma-1}$. Let $e = t^k(a/b)$, a, $b \in F'[t]$, $t \nmid a$, $t \nmid b$, $k \in \mathbf{Z}$. Then $e^{\sigma-1} = (-1)^k t^{-2k}(a/b)^{\sigma-1}$. Replacing d, if necessary, by $\pm t^{2k} d$, we may assume that $k = 0$. Let $m = \deg b$. Since $t(a/b)^{\sigma-1} = t(ab^\sigma)^{\sigma-1} = t(at^{-m}b^*)^{\sigma-1} = t(-1)^m t^{2m}(ab^*)^{\sigma-1}$, replacing d by $\pm t^{-2m} d$, we may assume that $e \in F'[t]$ and $t \nmid e$. If $e = c^2 r$, where $r \in F'[t]$ is square-free, then $d = (c^{\sigma-1})^2 r^{\sigma-1} t$. Since $(c^{\sigma-1})^2$ is an element of K' having norm 1 in K, we may assume that e is square-free.

Let $e = vp_1 \cdots p_r$ where the p_i are distinct monic irreducible polynomials in $F'[t]$, $p_i(0) \neq 0$, and $v \in F'$. Denoting the degree of e by k, we have $e^* = t^k e^\sigma = t^k v^\sigma p_1^\sigma \cdots p_r^\sigma = v^\sigma p_1^* \cdots p_r^*$. Now suppose there are i and j, $i \neq j$, such that p_i divides p_j^*. Then, since p_j^* is irreducible, $p_j^* = wp_i$ for some $w \in F'$. Let $l = \deg(p_i) = \deg(p_j^*) = \deg(p_j)$. Then $(-1)^l p_j = p_j^{**} = w^\sigma p_i^*$. It follows that $(wp_ip_j)^\sigma = t^{-2l} w^\sigma p_i^* p_j^* = t^{-2l}(-1)^l p_j w p_i$, i.e., $(wp_ip_j)^{\sigma-1} = t^{-2l}(-1)^l = (\sqrt{-1}/t)^{2l}$. Writing $e = (wp_ip_j)b$ we have $d = te^{\sigma-1} = (\sqrt{-1}/t)^{2l} b^{\sigma-1} t$. It follows, as before, that we may assume that p_i does not divide p_j^* if $i \neq j$.

We have $d = te^{\sigma-1} \equiv e^{\sigma+1} t = ee^* t^{1-k}$ modulo nonzero squares in K'. Suppose first that k is even. Then $L = K'(\sqrt{ee^*t})$. Since $\mathrm{ht}(L/K') \geq n-1$, $\zeta \in \mathcal{N}(L/K')$. Thus there are polynomials f, g, h, $h \neq 0$, which we may assume have no common factor, such that $f^2 - ee^*tg^2 = \zeta h^2$. If t divides h, then t divides f. But t does not divide ee^* so t must also divide g, a contradiction. Thus $h(0) \neq 0$ and so $\zeta = f(0)^2/h(0)^2$. This shows that ζ is a square in F', as was to be shown.

Finally, assume that k is odd. Then $L = K'(\sqrt{ee^*})$. As above, there are polynomials f, g, h, $h \neq 0$, which we may assume have no common factor, such that $f^2 - ee^*g^2 = \zeta h^2$. Since k is odd, one of the factors p_i of e has odd degree. Suppose p_i divides e^*. Since p_i does not divide p_j^* if $i \neq j$ we conclude that p_i divides p_i^*. Thus $p_i^* = wp_i$ where $w \in F'$. Let $l = \deg(p_i)$. Then $(-1)^l p_i = p_i^{**} = w^\sigma p_i^* = w^\sigma w p_i$. Since l is odd, $\mathcal{N}_{F'/F}(w) = w^\sigma w = -1$, contrary to hypothesis. Thus p_i does not divide e^*

so p_i divides ee^* to the first power. It follows, as before, that h is not divisible by p_i and that ζ is a square in $V = F'[t]/(p_i)$. But $[V : F'] = l$ is odd so ζ is a square in F'. Q.E.D.

Corollary 9. *Let $n \geq 2$ and let ζ be a primitive 2^nth root of unity over Q. Let $F = Q(\zeta + \zeta^{-1})$. Let x be a transcendental over F and let $K = F(x, y)$ where $x^2 + y^2 = -1$. Then $\mathrm{ht}(K(\sqrt{-1})/K) = n$. In particular, there exists a cyclic extension E of K, $E \supset K(\sqrt{-1})$, with $[E : K(\sqrt{-1})] = 2^n$ but there does not exist such an E with $[E : K(\sqrt{-1})] = 2^{n+1}$.*

Proof. Immediate from Theorem 8 and Corollary 4.

We would like to thank the referee for pointing out the following interesting consequence of Theorem 8.

Corollary 10. *Let F be a field in which -1 is not a sum of two squares and let $K = F(x, y)$ where x is transcendental over F and $x^2 + y^2 = -1$. Let $F' = F(\sqrt{-1})$ and let $K' = K(\sqrt{-1})$. Assume that $\mathrm{ht}(K'/K) \geq 3$ and let L be a cyclic extension of K, $L \supset K'$, with $[L : K'] = 2$ and $\mathrm{ht}(L/K) \geq 2$. Then $\mathcal{N}(L/K') \cap F' = (F')^2$.*

Proof. This follows from the proof of Theorem 8.

We conclude with several remarks about the preceding results.

1. Suppose K is a field of characteristic $\neq 2$ with $\sqrt{-1} \notin K$ and $\sqrt{-2} \notin K$. Then $\mathrm{ht}(K(\sqrt{-1})/K) = \mathrm{ht}(K(\sqrt{-2})/K)$. For suppose $\sigma \in X(K)$ corresponds to $K(\sqrt{-1})/K$ and $\tau \in X(K)$ corresponds to $K(\sqrt{-2})/K$. Then $\sigma\tau$ corresponds to $K(\sqrt{2})/K$. Since we may clearly assume that $\sqrt{2} \notin K$, $\mathrm{ht}(K(\sqrt{2})/K) = \infty$ so $\mathrm{ht}(K(\sqrt{-1})/K) = \mathrm{ht}(K(\sqrt{-2})/K)$. Thus Theorems 5 and 6 and Corollaries 4 and 9 are also valid with $K(\sqrt{-1})/K$ replaced by $K(\sqrt{-2})/K$.

2. Suppose p is a rational prime, $p \equiv 5 (\mathrm{mod}\, 8)$. Then $\mathrm{ht}(Q(\sqrt{p})/Q) = 1$. To see this we note that $\mathrm{ht}(Q(\sqrt{p})/Q) \geq 1$ if and only if for every prime q of Q and every extension π of q to $Q(\sqrt{p})$, $-1 \in \mathcal{N}(Q(\sqrt{p})_\pi/Q_q)$. This holds if $q \neq p$ since -1 is a unit and $Q(\sqrt{p})_\pi/Q_q$ is unramified. The condition is also satisfied if $q = p$ since $\sqrt{-1} \in Q_q$. Since $Q(\sqrt{p})$ is tamely ramified over Q at q and $\mu(8) \not\subset Q_q$, $\mathrm{ht}(Q_q(\sqrt{p})/Q_q) = 1$ [8, Lemma 11, p. 74]. It follows that $\mathrm{ht}(Q(\sqrt{p})/Q) = 1$. This shows that the results of §3 and §4 do not hold, in general, for other quadratic extensions of Q.

3. Theorem 6 provides a class of extensions which are reduced of infinite height. These are not, however, the simplest such examples. Perhaps the simplest are the following. Let p be a rational prime, $p \equiv 1 \ (\mathrm{mod}\, 4)$ and let $q > 0$ be a quadratic residue $(\mathrm{mod}\, p)$. Since $Q(\sqrt{pq}, \sqrt{p})/Q(\sqrt{pq})$ is everywhere unramified, it has infinite height by [2, Chapter 10, Theorem 6]. Since the Leopold conjecture holds for $Q(\sqrt{pq})$, the only quadratic extension of $Q(\sqrt{pq})$ which is divisible is $Q(\sqrt{pq}, \sqrt{2})$. Thus $Q(\sqrt{pq}, \sqrt{p})/Q(\sqrt{pq})$ must be reduced of infinite height.

REFERENCES

1. A. A. Albert, *Modern higher algebra*, Univ. of Chicago Press, Chicago, 1937.
2. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1967.
3. F. Bertrandias and J.-J. Payan, *Γ-Extensions et invariants cyclotomiques*, Ann. Sci. École Norm. Sup. (4) **5** (1972), 517–543.
4. J. E. Carroll, *On determining the quadratic subfields of Z_2-extensions of complex quadratic fields*, Compositio Math. **30** (1975), 259–271.
5. J. E. Carroll and H. Kisilevsky, *Initial layers of Z_l-extensions of complex quadratic fields*, Compositio Math. **32** (1976), 157–168.
6. B. Fein, B. Gordon, and J. Smith, *On the representation of* -1 *as a sum of two squares in an algebraic number field*, J. Number Theory **3** (1971), 310–315.
7. I. Reiner, *Maximal orders*, Academic Press, New York, 1975.
8. O. Schilling, *The theory of valuations*, Math. Surveys, no. 4, Amer. Math. Soc., Providence, R.I., 1950.

SCIENCE INSTITUTE, THE UNIVERSITY OF ICELAND, 107 REYKJAVIK, ICELAND

DEPARTMENT OF MATHEMATICS, OREGON STATE UNIVERSITY, CORVALLIS, OREGON 97330

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024

FACULTY OF MATHEMATICS, TECHNION-ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA, 32000 ISRAEL