ACTA ARITHMETICA
XXV (1973)

On the representation of cyclotomic polynomials as sums of squares

by

J. S. Hsia* (Columbus, Ohio)

Dedicated to Professor Hans J. Zassenhaus' 60th Birthday

1. In a recent paper by Pourchet [4], he showed that every positive definite polynomial in $Q[X]$ is a sum of at most five squares of polynomials. Since the polynomial $f(X) = X^2+7$ needs no fewer than five squares to represent it, Pourchet's bound for $Q(X)$ is the best possible. This result drastically improves an earlier result due to Landau [3] (which asserted that *zeight* squares would serve as an upper bound). We have in [2] extended Pourchet's work by explicitly determining the best possible bound for the representation in sums of squares for definite functions in one variable over an algebraic number field. The application to the class of cyclotomic polynomials over the rationals was dealt with in [4] (see Théorème 3). This note extends the investigation to algebraic number fields.

If K is an algebraic number field, let $\mathfrak{D}_K$ denote the (finite) set of dyadic spots (i.e. those primes containing 2) on K, and $s_K = \mathrm{Max}\, s(K_\mathfrak{p})$ where $s(K_\mathfrak{p})$ is the Stufe of $K_\mathfrak{p}$ and $\mathfrak{p}$ running through the set of all *non-archimedean* spots on K. Thus, if K is totally imaginary, then s_K is just the Stufe of K. It is well known that s_K is either 1, 2, or 4 (Siegel's theorem, [5]). As in [2], we call the *reduced height* of a field F—denoted by $m(F)$—the minimal positive integer (or infinity) such that every sum of squares in F is already a sum of $m(F)$ number of squares. The next two statements can be found in [2]:

1.1. *The reduced height of a formally real algebraic number field K is always 3 or 4. It is 4 if and only if $s_K = 4$.*

1.2. *If K is a formally non-real algebraic number field, then $m(K(X)) = s_K+1$.*

---

* I would like to thank Roger Peterson for useful conversations regarding Lemma 1.4. This research is partially supported by the National Science Foundation under contract Grant GP-23656.

Denote by $\varphi_n(X)$ the nth cyclotomic polynomial, and ζ_n a fixed primitive nth root of unity. For $n > 2$, $\varphi_n(X)$ is positive definite (a rational function $f(X) \in K(X)$ is called *positive definite* if $a \in K$ and $f(a)$ is defined, then $f(a) \geqslant 0$ for all orderings on K). Since $\varphi_n(X)$ is a separable polynomial, it is never a square. From [4] we know that if $4|n$, then $\varphi_n(X)$ is a sum of two squares in $\boldsymbol{Q}[X]$, and so *a fortiori* a sum of two squares in $K[X]$ for any extension field K of $\boldsymbol{Q}$. On the other hand, for any positive odd integer $r > 1$, $\varphi_{2r}(X) = \varphi_r(-X)$. Therefore, in the remaining of this article we may assume the following: *n is an odd integer greater than* 1. We shall be needing the following lemmas:

1.3. Lemma. *Let K be a number field with $s_K = 4$. Then $\varphi_n(X)$ is never a sum of three squares in $K[X]$.*

Proof. If $\varphi_n(X)$ were a sum of three squares in $K[X]$, then for every scalar $b \in K$, we would have $\varphi_n(b)$ a sum of three squares in K. Since $s_K = 4$ here, there is a dyadic prime $\mathfrak{p} \in \mathfrak{D}_K$ for which the Stufe $s(K_\mathfrak{p})$ of $K_\mathfrak{p}$ equals 4. But, in $\boldsymbol{Q}$ we have $\varphi_n(2) \equiv -1 \pmod 8$ which means $\varphi_n(2)$ belongs to the *same* square class as -1 inside $\boldsymbol{Q}_2$ = the field of 2-adic numbers, and so *a fortiori* inside also $K_\mathfrak{p}$. A contradiction.

1.4. Lemma. *If G is a direct product of t components of cyclic groups each of which has even order, then there exist exactly $2^t - 1$ number of subgroups of index* 2.

Proof. Writing $G = A \times B$, where A is a group of odd order and B a direct product of t components of cyclic groups each of which has for its order a 2-power. If H is a subgroup of index 2 in G, it is then clear that A is contained in H. Thus, we have: $H = A \times (B \cap H)$ so that the problem is reduced to one where G is itself elementary 2-abelian, say: $G = \boldsymbol{Z}_{2^{a_1}} \times \ldots \times \boldsymbol{Z}_{2^{a_t}}$, $a_i \geqslant 1$. The Frattini subgroup $\mathfrak{f}(G)$ of G is: $\boldsymbol{Z}_{2^{a_1-1}} \times \times \boldsymbol{Z}_{2^{a_t-1}}$ so that reduction modulo $\mathfrak{f}(G)$ further reduces to the case where G is a direct product of t copies of $\boldsymbol{Z}_2$; i.e. G is just a t-dimensional vector space over $\boldsymbol{Z}_2$, which is known to have $2^t - 1$ distinct copies of hyperplanes.

1.5. Corollary. *Let n be an odd integer > 1, and $n = p_1^{a_1} \ldots p_t^{a_t}$. The cyclotomic field $\boldsymbol{Q}(\zeta_n)$ has $2^t - 1$ distinct quadratic subfields each of the type:*

$$\boldsymbol{Q}(\sqrt{\varepsilon_{i_1} \ldots \varepsilon_{i_r} p_{i_1} \ldots p_{i_r}}),$$

where $\varepsilon_{i_j} = +1$ or -1 according to $p_{i_j} \equiv 1$ or $-1 \pmod 4$ respectively, and $1 \leqslant i_1 < \ldots < i_r \leqslant t$.

Proof. The cyclotomic extension $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$ has for its Galois group $G \cong \mathrm{Gal}\big(\boldsymbol{Q}(\zeta_{p_1^{a_1}})/\boldsymbol{Q}\big) \times \ldots \times \mathrm{Gal}\big(\boldsymbol{Q}(\zeta_{p_t^{a_t}})/\boldsymbol{Q}\big)$ each component of which is cyclic of order $\varphi(p_i^{a_i})$. Therefore, $\boldsymbol{Q}(\zeta_{p_i^{a_i}})$ contains a *unique* quadratic subfield $L_i = \boldsymbol{Q}(\sqrt{\varepsilon_i p_i})$. Clearly, the composita $L_{i_1} \ldots L_{i_r}$ for $1 \leqslant i_1 < \ldots < i_r \leqslant t$ are all distinct quadratic subfields of $\boldsymbol{Q}(\zeta_n)$, each of which corresponds, by Galois theory, to a distinct subgroup of index 2 in G. Lemma 1.4 says these are then all the quadratic subfields of $\boldsymbol{Q}(\zeta_n)$.

1.6. (i) *$\varphi_n(X)$ is a sum of two squares in $K[X]$ if and only if $\sqrt{-1} \in K(\zeta_n)$.* (ii) *$\varphi_n(X)$ is a sum of four squares in $K[X]$ if and only if the Stufe $s\big(K(\zeta_n)\big)$ is less or equal to two.*

Proof. See Propositions 7 and 8, [2].

2. Quadratic extensions. Let $K = \boldsymbol{Q}(\sqrt{d})$ with d square-free, $d = (\pm)p_1 \ldots p_r$. Denote by $N(d)$ the number of prime factors of d which are congruent to 3 (mod 4). Let us dispose with the non-real case first.

2.1. Theorem. (1) *When $s_K = 1$, every $\varphi_n(X)$ is a sum of two squares;*

(2) *when $s_K = 2$, $\varphi_n(X)$ is always a sum of three squares; however, it is a sum of two squares if and only if:* (i) *$d|n$ and* (ii) *$N(d)$ is an even integer;*

(3) *when $s_K = 4$, $\varphi_n(X)$ is never a sum of three squares — hence also never a sum of two squares (recall the basic assumption that n is odd); $\varphi_n(X)$ is always a sum of five squares; $\varphi_n(X)$ is a sum of four squares if and only if the order of* 2 (mod n) *is even (this occurs if and only if there is a prime factor p of n for which the order of* 2 (mod p) *is even).*

Proof. Statement (1) follows from 1.2, and so does the first part of statement (2). The second part follows from Corollary 1.5 and 1.6 (i). Statement (3) consists of three parts; the first is a consequence of Lemma 1.3, the second of 1.2. Thus, only the last part of (3) needs to be checked. From 1.6(ii), we need to determine the Stufe $s\big(K(\zeta_n)\big)$. This value is two or less if and only if the local degrees of $K(\zeta_n)$ at all the primes in $\mathfrak{D}_{K(\zeta_n)}$ are even, see [1]. On the other hand, $s_K = 4$ here implies the rational prime $2\boldsymbol{Z}$ splits completely in K. Since n is an odd integer, $2\boldsymbol{Z}$ is unramified in $\boldsymbol{Q}(\zeta_n)$. Therefore, $2\boldsymbol{Z}$ is unramified in $K(\zeta_n)$ and the local degrees of $K(\zeta_n)$ at all the primes in $\mathfrak{D}_{K(\zeta_n)}$ have the same value and is, in fact, the same value as the local degree of $\boldsymbol{Q}(\zeta_n)$ at a prime in $\mathfrak{D}_{\boldsymbol{Q}(\zeta_n)}$ — and this is well known to be simply the order of 2 (mod n). Finally, if $n = p_1^{a_1} \ldots p_m^{a_m}$, then the order of 2 (mod n) is the least upper bound of the order of 2 (mod $p_i^{a_i}$), each of which is the product of the order of 2 (mod p_i) times a power of p_i. This completes the proof.

In the remainder of this section, assume $K = \boldsymbol{Q}(\sqrt{d})$ with $d > 0$ and square-free, $d = p_1 \ldots p_r$. This time we observe that $\sqrt{-1}$ belongs to $K(\zeta_n)$ if and only if: (i) $d|n$ and (ii) $N(d)$ is odd. Hence, if $d \equiv 1 \pmod 4$ $\varphi_n(X)$ can never be a sum of two squares in $K[X]$. So, let $d \equiv 2$ or $3 \pmod 4$. But, n is odd and $d|n$; $\sqrt{-1} \in K(\zeta_n)$ implies $d \equiv 3 \pmod 4$. Summarizing, we get:

2.2. THEOREM. *Let $K = Q(\sqrt{d})$ with $d > 0$ and square-free. $\varphi_n(X)$ is a sum of two squares in $K[X]$ if and only if*: (i) $d|n$ *and* (ii) $d \equiv 3 \pmod 4$.

If $K = Q(\sqrt{d})$ with $d \equiv 1 \pmod 8$, then $2Z$ splits completely in K so that $s_K = 4$, and according to Lemma 1.3, $\varphi_n(X)$ can never be a sum of three squares in $K[X]$. We know from [2] that $m(K(X)) = 5$. But, here we have $N(d)$ is even (zero is considered also even), so that K is linearly disjoint from $Q(\zeta_n)$ if and only if $d \nmid n$. If $d|n$ then K is already contained in $Q(\zeta_n)$ so that $s(Q(\zeta_n))$ is even if and only if the order of $2 \pmod n$ is even. If $d \nmid n$, the Galois group of $K(\zeta_n)$ is isomorphic to $\mathrm{Gal}(K/Q) \times \mathrm{Gal}(Q(\zeta_n)/Q)$ and one sees that $s(K(\zeta_n)) = 2$ if and only if $s(Q(\zeta_n)) = 2$. Thus, we obtain:

2.3. THEOREM. *Let $K = Q(\sqrt{d})$ with $d > 0$ and square-free, and $d \equiv 1 \pmod 8$. Then, $\varphi_n(X)$ is never a sum of three squares in $K[X]$. $\varphi_n(X)$ is always a sum of five squares; it is, however, a sum of four squares if and only if the order of $2 \pmod n$ is even.*

2.4. COROLLARY. *Let $K = Q(\sqrt{d})$ with $d > 0$ and square-free. Then, $\varphi_n(X)$ is always a sum of four squares in $K[X]$ except when $d \equiv 1 \pmod 8$ and the order of $2 \pmod n$ is odd. In the exceptional case $\varphi_n(X)$ is a sum of five squares.*

Proof. From the results thus far, we need only to deal with the cases: $d \equiv 2 \pmod 4$ and $d \equiv 5 \pmod 8$. In the first case, $2Z$ ramifies in K, and in the second case $2Z$ extends to a prime in K so that by virtue of the multiplicative behaviour of local degrees with respect to field extensions, we see the Stufe $s(K(\zeta_n))$ of $K(\zeta_n)$ will be less than or equal to two in both cases. Hence, 1.6(ii) finishes the proof.

3. Odd extensions. In this section K is a (formally real) algebraic number field with absolute field degree $[K : Q] = d$ an odd integer. It follows from a result in [2] that the reduced height $m(K(X))$ for $K(X)$ is five. Since s_K equals four here, Lemma 1.3 implies that no $\varphi_n(X)$ — n is still odd of course — can be a sum of three squares in $K[X]$. Therefore, the only issue at hand is to characterize those $\varphi_n(X)$ that are sums of exactly four squares. In order to accommodate the other (possibly non-real) number fields, we prove the following:

3.1. PROPOSITION. *Let K be an algebraic number field such that $s_K = 4$. Then, $\varphi_n(X)$ is a sum of five squares in $K[X]$; it is a sum of exactly four squares if and only if for every prime $\mathfrak{p} \in \mathfrak{D}_K$ at which the local degree*

$$n(\mathfrak{p}|2) = [K_\mathfrak{p} : Q_2]$$

of K at $\mathfrak{p}$ is odd, the order of $2^{f(\mathfrak{p}|2)} \pmod n$ is even — here, $f(\mathfrak{p}|2)$ denotes the residue class degree of K at $\mathfrak{p}$.

Proof. Since n is odd, $2Z$ is unramified in $Q(\zeta_n)$. If $\mathfrak{p} \in \mathfrak{D}_K$ has odd local degree, then both the ramification index $e(\mathfrak{p}|2)$ as well as the residue class degree $f(\mathfrak{p}|2)$ of K at $\mathfrak{p}$ are odd. Therefore, $\mathfrak{p}$ is unramified in $K(\zeta_n)$. Write: $\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_{g(\mathfrak{p})}$ with $\mathfrak{P}_i$'s in $\mathfrak{D}_{K(\zeta_n)}$ — since $K(\zeta_n)/K$ is Galois. The local degrees $n(\mathfrak{P}_i|2)$ are even integers if an only if the relative residue class degrees $f(\mathfrak{P}_i|\mathfrak{p})$ are also even. But, these are just the order of $2^{f(\mathfrak{p}|2)} \pmod n$ — see Proposition 3-2-12(iii), [6]. Now, the rest is taken care of by 1.6(ii), and the fact that $s_{K(\zeta_n)} = 2$ if and only if the local degrees of $K(\zeta_n)$ at each of the spots in $\mathfrak{D}_{K(\zeta_n)}$ are even.

4. Some concluding remarks. Let K be an arbitrary number field with absolute field degree an even integer. Suppose K is complex (i.e. totally imaginary), then $m(K(X))$ is always $s_K + 1$ by 1.2. When $s_K = 1$, every $\varphi_n(X)$ is a sum of two squares. When $s_K = 2$, $\varphi_n(X)$ is a sum of three squares, but it is a sum of two squares if and only if $\sqrt{-1} \in K(\zeta_n)$. The case of $s_K = 4$ is treated in Proposition 3.1. If K is formally real, then $m(K(X)) = 4$ or 5 according respectively to $m(K) = 3$ or 4, and precise characterizations are given in [2]. However, $m(K) = 4$ if and only if $s_K = 4$, which case is again handled by Proposition 3.1. For $m(K) = 3$, every $\varphi_n(X)$ is a sum of four squares; it is a sum of two squares if and only if $\sqrt{-1}$ belongs to $K(\zeta_n)$ as before. Note that when K is linearly disjoint from $Q(\zeta_n)$ — this occurs, for example, if the discriminant of K/Q is relatively prime to n — and that K/Q is a galois extension, then the Galois group $\mathrm{Gal}(K(\zeta_n)/Q) \cong \mathrm{Gal}(K/Q) \times \mathrm{Gal}(Q(\zeta_n)/Q)$. In such cases, Lemma 1.4 and Corollary 1.5 may be particularly useful to determine as to whether or not $\sqrt{-1}$ lies inside $K(\zeta_n)$. More specially, if K/Q is a cyclic extension, one needs to look only at the unique quadratic subfield then, say, $Q(\sqrt{d})$. The discussion given in § 2 above provides the answer.

Finally, there remains the touchy question of sums of three squares in $K[X]$. Already in the real quadratic case difficulties abound. Of course, Theorem 2.3 says that if $K = Q(\sqrt{d})$ with $d \equiv 1 \pmod 8$ then there can be no $\varphi_n(X)$ that is a sum of three squares. On the other hand, inside $Q(\sqrt{2})$, for instance, $\varphi_n(X)$ can be a sum of *precisely three* squares (e.g. $\varphi_3(X) = (X + 1/2)^2 + (1/\sqrt{2})^2 + (1/2)^2$ and $\varphi_5(X) = (X^2 + X/2)^2 + (X/2 + 1)^2 + (X/\sqrt{2})^2$, etc.). The general answer of which $\varphi_n(X)$ is exactly a sum of three squares in $K[X]$, for already real quadratic fields K, is not known to me. *One difficulty with the problem of sums of three squares in $K[X]$ is that the local-global principle fails to hold.* Indeed, if $K = Q(\sqrt{d})$ with $d > 0$, square-free, and $d \not\equiv 1 \pmod 8$, then for each finite spot $\mathfrak{p}$, $K_\mathfrak{p}$ has Stufe $\leqslant 2$ so that every polynomial in $K_\mathfrak{p}[X]$ is a sum of three squares, and if $\mathfrak{p}$ is a real spot then every positive definite polynomial in $K_\mathfrak{p}[X]$

is a sum of two squares. Thus, a polynomial such as $f(X) = X^2+3$ is locally everywhere a sum of at most three squares and yet globally it is a sum of four (and no fewer) squares.

References

[1] I. G. Connell, *The Stufe of number fields*, Math. Zeitschr. 124(1972), pp. 20–22.

[2] J. S. Hsia and R. P. Johnson, *On the representation in sums of squares fro definite functions in one variable over an algebraic number field*, to appear in Amer. J. Math.

[3] E. Landau, *Über die Darstellung definiter Funktionen durch Quadrate*, Math. Ann. 62(1906), pp. 272–285.

[4] Y. Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. 19(1971), pp. 89–104.

[5] C. L. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Zeitschr. 11 (1921), pp. 246–275.

[6] E. Weiss, *Algebraic Number Theory*, 1963.

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
Columbus, Ohio

Received on 10. 1. 1973 (366)