Then the conditions on $|x| < 1$ require that $f^{1,2}$ should be a solution of (1). If $\det(I - ia) \neq 0$ we can find a solution while if $\det(I - ia) = 0$ there exists no solution.

References


Carnegie Institute of Technology

A REMARK ON AN ARITHMETIC THEOREM OF CHEVALLEY

H. Bass

1. Let $k$ be an algebraic number field with ring of integers $\mathcal{O}$, and let $E$ be a finitely generated subgroup of the multiplicative group, $k^*$. All but finitely many primes $\mathfrak{p}$ are "prime to $E,"$ i.e., the units of $\mathcal{O}_{\mathfrak{p}}$ contain $E$. An ideal $a$ is called "prime to $E"$ if its prime divisors are. In this case we have a natural homomorphism

$$E \rightarrow (\mathcal{O}/a)^*$$

whose kernel, the congruence subgroup $\{a \in E | a \equiv 1 \mod a\}$, is evidently of finite index. We denote the group of all (complex) roots of unity by $\mathbb{Q}/\mathbb{Z}$.

**Theorem.** Let $\chi : E \rightarrow \mathbb{Q}/\mathbb{Z}$ be a character of $E$. Then there are infinitely many prime ideals $\mathfrak{p}$ of $k$, prime to $E$, such that $\chi$ factors through a character of $(\mathcal{O}/\mathfrak{p})^*$, i.e., such that $\ker(E \rightarrow (\mathcal{O}/\mathfrak{p})^*) \subset \ker \chi$.

It follows immediately that if $U$ is a subgroup of finite index in $E$ then $\ker(E \rightarrow (\mathcal{O}/a)^*) \subset U$ for a suitable $a$, which we may take to be square free. This is the form of the theorem proved by Chevalley in [2]. That $a$ may be taken square free is implicit in his proof. The following corollary paraphrases Chevalley's theorem.

**Corollary 1 (Chevalley).** If we embed $E$ in $\prod_{\mathfrak{p} \text{ prime to } E} (\mathcal{O}/\mathfrak{p})^*$,
its closure is naturally identical with the completion, \( \hat{E} \), of \( E \) in the topology defined by all subgroups of finite index.

I was led to these matters after proving the following corollary. I am indebted to J.-P. Serre for referring me to Chevalley's paper.

**Corollary 2.** The algebraic closure of a finite field is generated, as a field, by roots of unity of prime order. The same is (therefore) true of the maximal unramified extension of a \( p \)-adic field.

**Proof.** Let \( \overline{F}_p \) be the algebraic closure of \( F_p = \mathbb{Z}/p\mathbb{Z} \), and let \( H \) be the subgroup of \( \overline{F}_p^* \) generated by roots of unity of prime order. Let \( L = F_p(H) \) and let \( G = G(F_p/F_p) \), the Galois group. To show that \( L = F_p \) it suffices, by Galois theory, to show that the restriction map, \( G \to \text{Aut}(H) \), is a monomorphism, since \( L \) is the fixed field of its kernel.

Now \( G \) is topologically isomorphic to \( \mathbb{Z} \), with generator \( \Phi = \text{Frobenius (pth power)} \). \( H \) is isomorphic to the additive group \( \mathbb{Q}^p \mathbb{F}_q \), so \( \text{Aut}(H) = \prod_{q \neq p} \mathbb{F}_q^* \). Under this identification, \( G \to \prod_{q \neq p} \mathbb{F}_q^* \) sends \( f \) to the element with all coordinates equal to \( p \). With \( E \) the subgroup of \( \mathbb{Q}^* \) generated by \( p \), our assertion now follows from Corollary 1.

Q.E.D.

In case \( k = \mathbb{Q} \) the theorem above was proved by Mills in [3] in a slightly more precise form. Mills' argument is essentially the same as Chevalley's (of which Mills was presumably unaware). This consists of reducing the theorem to a computation of \( (F^*)^m \cap k^* \), \( F \) being the field over \( k \) generated by a primitive \( m \)th root of unity. This reduction is repeated, for the reader's convenience, in the next section.

The preciseness of the final theorem is then a direct reflection of the precision with which \( (F^*)^m \cap k^* \) is computed.

2. We show here (following Chevalley) how to deduce the Theorem from the next proposition, whose proof will be given in part 3.

**Proposition.** Given \( N > 0 \), then there is an \( m > 0 \) such that, if \( F \) is the field generated over \( k \) by a primitive \( m \)th root of unity, we have

\[
(F^*)^m \cap k^* \subseteq (k^*)^N.
\]

**Proof of the theorem.** Recall that we have \( E \subseteq k^* \) and \( \chi: E \to \mathbb{Q}/\mathbb{Z} \). We must find \( p \) such that \( \ker(E \to (\mathbb{Q}/p)^*) \subseteq \ker \chi \). Choose \( N > 0 \) so that \( E \cap (k^*)^N \subseteq \ker \chi \). This is possible since \( \chi(E) \) is finite and since \( k^* \) is the product of a free abelian with a finite group. Now choose \( m > 0 \) as in the proposition above. Then \( (F^*)^m \cap E \subseteq \ker \chi \). It follows that \( \chi \) factors via \( E \to F^*/(F^*)^m \); i.e., there is a character \( \chi': F^* \to \mathbb{Q}/\mathbb{Z} \) of order \( m \) such that \( \chi' | E = \chi \). Let \( L = F(E^{1/m}) \), the
(finite) extension generated by $m$th roots of elements of $E$. It follows from Kummer theory (see Artin [1]) that there is an $s \in G(L/F)$ such that $s(a^{1/m}) = a^{1/m} \chi(a)$ for all $a \in E$. By the Chebotarev density theorem there exist infinitely many primes $\mathfrak{P}$ of $F$ such that $s = ((L/F)/\mathfrak{P})$, the Artin symbol in the abelian extension $L/F$ (see Serre [4, p. 34]). Choose such a $\mathfrak{P}$ prime to $m$. Then if $a \in E$ and $a \equiv 1 \mod \mathfrak{P}$, $a$ is an $m$th power in the local field $F_\mathfrak{P}$. Hence the local degrees at $\mathfrak{P}$ of $F(a^{1/m})/F$ are all one. It follows that $s = ((L/F)/\mathfrak{P})$ fixes $a^{1/m}$ and, consequently, $\chi(a) = 1$. Thus, the prime $p$ of $k$ that $\mathfrak{P}$ divides solves our problem, and we have proved the theorem.

3. The proposition will be proved in a sequence of lemmas which give some more specific information.

**Lemma 1.** Let $F/k$ be a finite field extension and $q$ an integer with prime factorization $\prod p_i^{e_i}$.

(a) $\left( F^* \right)^{q} \cap k^* = \prod \left[ \left( F^* \right)^{p_i^{e_i}} \cap k^* \right]$.

(b) If $d = [F : k]$ is prime to $q$, then $\left( F^* \right)^{d} \cap k^* = (k^*)^{q}$.

**Proof.** (a) is obvious. (b): If $x \in \left( F^* \right)^{q} \cap k^*$, take norms to obtain $x^d \in (k^*)^q$. g.c.d. $(d, q) = 1 \Rightarrow x \in (k^*)^q$.

Now we fix some notation: $k_m$ denotes the field over $k$ generated by a primitive $m$th root of unity.

**Lemma 2.** If $p \neq 2$, $(k^*)^a \cap k^* = (k^*)^a$. $(k^*)^a \cap k^* = (k^*)^a \cap k^* \subset (k^*)^{a-1}$, where $a = \min (2, e)$. Hence, if $k_4 \subset k$, $(k_2^*)^a \cap k^* = (k^*)^a$.

**Proof.** See Chevalley [2, pp. 37, 38].

For a prime $p$ we define

$$e(p) = e(p, k)$$

to be the largest integer $e$ such that, for each prime $p$ of $k$ above $p$, the local field at $p$ contains $k_p$. Note that if $e > 0$ and $p \neq 2$ this implies $p$ is ramified; hence $e(p) = 0$ for all but finitely many $p$.

**Lemma 3.** Suppose $n \geq e = e(p)$. Then for any $m > 0$

$$(k_m^*)^m \cap k^* \subset \left( k_p^* \right)^m \cap k^*;$$

unless $p = 2$ and $e = 1$. In this case replace the right side by $(k^*)^{2e-2}$.

**Proof.** Write $m = p^r q$ with $q$ prime to $p$. We apply Lemma 2 to $k_q$ to obtain $(k_q^*)^m \cap k_q^* \subset (k_q^*)^m$, where $h = n$ for $p$ odd, and which we discuss below for $p = 2$. Choose $f$ maximal so that $k_p \subset k_q$. If $F$ is the local field of $k$ at a prime dividing $p$ then $F \subset F_p \subset F_q$. However, the big extension is unramified, and the small one totally rami-
fied. Hence $F = F_p^f$, so, by definition of $e = e(p)$, we have $f \leq e$.

Suppose $y \in k^*_p$ is such that $y^{p^h} \in k^p$. If $s \in G(k_q^p/k_q)$ then $sy = yz$ with $z^{p^h} = 1$. By definition of $f$, therefore, $z^{p^f} = 1$. It follows that $sy^{p^f} = y$, so $y^{p^f} \in k^p$. Writing $y^{p^h} = (y^{p^f})^{p^h-f}$ we have therefore shown that

$$(k^*_p)^{p^h} \cap k^*_p \subseteq (k^*_p)^{p^{h-f}} \subseteq (k^*_p)^{p^{h-f-c}},$$

the second inclusion ensuing from $f \leq e$. We have thus descended the field tower, $k \subseteq k^p \subseteq k_q \subseteq k_m$, and proved our assertion in the case $h = n$. By Lemma 2 this is the case for $p$ odd, and for $p = 2$ provided $k_4 \subseteq k_q$. In the remaining case we must have $p = 2$ and $f = 1$, so $k^p = k$ and we can take $h = n - 1$. The proof then yields $(k^*_p)^{2^{n-1}} \cap k^*_p \subseteq (k^*)_2^{2^{n-2}} = (k^*)_2^{2^{n-2}}$.

Combining Lemmas 1, 2, and 3 we have:

**Corollary.** Let

$$f(p) = \begin{cases} e(p) & \text{for } p \neq 2, \\ e(2) + 2 & \text{for } p = 2. \end{cases}$$

Then if $m$ has prime factorization $\prod_{p \in S} p^\nu(p)$, with $\nu(p) \geq f(p)$, and if $m_0 = \prod_{p \in S} p^\nu(p)$, then

$$(k^*_m)^m \cap k^* \subseteq (k^*)_m^{m_0}.$$  

Since $m_0$ depends only on the prime divisors of $m$, and not their exponents, it is clear that the proposition of §2 follows from the corollary.

**References**