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

1. T. Carleman, *Sur la résolution de certaines équations intégrales*, Mat. Ark. Astronom. Fys. **16**, no. 26 (1922).

2. N. I. Muskhelishvili, *Singular integral equations*, Noordhoff, Groningen, 1953.

3. N. P. Vekua, *Systems of singular integral equations and some boundary problems*, GITTL, Moscow-Leningrad, 1950.

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 $\mathfrak{O}$, 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 $\mathfrak{O}_\mathfrak{p}$ contain E. An ideal $\mathfrak{a}$ is called "prime to E" if its prime divisors are. In this case we have a natural homomorphism

$$E \to (\mathfrak{O}/\mathfrak{a})^*$$

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

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

It follows immediately that if U is a subgroup of finite index in E then $\ker(E\to(\mathfrak{O}/\mathfrak{a})^*)\subset U$ for a suitable $\mathfrak{a}$, which we may take to be square free. This is the form of the theorem proved by Chevalley in [2]. That $\mathfrak{a}$ 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* $\prod_{\mathfrak{p} \text{ prime to } E} (\mathfrak{O}/\mathfrak{p})^*$,

Received by the editors August 19, 1964 and, in revised form, September 28, 1964.

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

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

In case $k=\boldsymbol{Q}$ 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 mth 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 mth root of unity, we have*

$$(F^*)^m\cap k^*\subset(k^*)^N.$$

PROOF OF THE THEOREM. Recall that we have $E\subset k^*$ and $\chi\colon E\to\boldsymbol{Q}/\boldsymbol{Z}$. We must find $\mathfrak{p}$ such that $\ker(E\to(\mathcal{O}/\mathfrak{p})^*)\subset\ker\chi$. Choose $N>0$ so that $E\cap(k^*)^N\subset\ker\chi$. 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 $(F^*)^m\cap E\subset\ker\chi$. It follows that χ factors via $E\to F^*/(F^*)^m$; i.e., there is a character $\chi'\colon F^*\to\boldsymbol{Q}/\boldsymbol{Z}$ of order m such that $\chi'|E=\chi$. Let $L=F(E^{1/m})$, the (finite) extension generated by mth 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 Čebotarev 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 $a\equiv 1 \bmod \mathfrak{P}$, a is an mth 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 $\mathfrak{p}$ 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 $\prod_i p_i^{n_i}$.*

(a) $(F^*)^q\cap k^*=\bigcap_i [(F^*)^{p_i^{n_i}}\cap k^*]$.

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

PROOF. (a) is obvious. (b): If $x\in(F^*)^q\cap k^*$, 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 mth root of unity.

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

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 $\mathfrak{p}$ of k above p, the local field at $\mathfrak{p}$ contains k_{p^e}. Note that if $e>0$ and $p\neq 2$ this implies $\mathfrak{p}$ is ramified; hence $e(p)=0$ for all but finitely many p.

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

$$(\overset{*}{k}_m)^{pn}\cap k^*\subset(\overset{*}{k}_{p^e})^{pn-e}\cap k^*,$$

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

PROOF. Write $m=p^rq$ with q prime to p. We apply Lemma 2 to k_q to obtain $(k^*_m)^{p^n}\cap k^*_q\subset(k^*_q)^{p^h}$, where $h=n$ for p odd, and which we discuss below for $p=2$. Choose f maximal so that $k_{p^f}\subset k_q$. If F is the local field of k at a prime dividing p then $F\subset F_{p^f}\subset F_q$. However, the big extension is unramified, and the small one totally ramified. Hence $F=F_{p^f}$ so, by definition of $e=e(p)$, we have $f\leqq e$.

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

$$(k_q^*)^{p^h}\cap k_{p^f}^*\subset (k_{p^f}^*)^{p^{h-f}}\subset (k_{p^e}^*)^{p^{h-e}},$$

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

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 $\prod_{p\in S}p^{n(p)}$, with $n(p)\geqq f(p)$, and if $m_0=\prod_{p\in S}p^{f(p)}$, then

$$(k_m^*)^m\cap k^*\subset (k^*)^{m/m_0}.$$

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

1. E. Artin, *Galois theory*, Univ. Notre Dame, Notre Dame, Ind., 1944.

2. C. Chevalley, *Deux théorèmes d'arithmétique*, J. Math. Soc. Japan **3** (1951), 36–44.

3. W. H. Mills, *Characters with preassigned values*, Canad. J. Math. **15** (1963), 169–171.

4. J.-P. Serre, *Corps locaux*, Hermann, Paris 1962.

Columbia University