BULL. AUSTRAL. MATH. SOC. 12F99
VOL. 14 (1976), 193-198. (20H20)

An embedding theorem for fields

J.W.S. Cassels

It is shown that every finitely generated field K of characteristic 0 may be embedded in infinitely many p-adic fields in such a way that the images of any given finite set C of non-zero elements of K are p-adic units. The result is suggested by Lech's proof of his generalization of Mahler's theorem on recurrent sequences. It also provides a simple proof of Selberg's theorem about torsion-free normal subgroups of matrix groups.

THEOREM I. *Let K be a finitely generated extension of the rational field $\mathbb{Q}$ and let C be a finite set of non-zero elements of K. Then there exist infinitely many primes p such that there is an embedding*

$$\alpha : K \to \mathbb{Q}_p$$

of K into the p-adic numbers $\mathbb{Q}_p$ for which

$$|\alpha c| = 1 \quad (\text{all } c \in C).$$

Here $|\ |$ denotes the p-adic valuation.

This theorem does not appear to have been stated explicitly before. The paper of Lech [3] contains implicitly a weaker form in which $\mathbb{Q}_p$ is replaced by some algebraic extension of a p-adic field.

Lech uses his result to generalize Mahler's theorem [4] about the values taken by recurrent sequences to any field of characteristic 0. Indeed Mahler's proof works in a p-adic field and so the generalization is an immediate consequence of the original theorem and the embedding.

Received 21 November 1975.

Another application is:

THEOREM II (Selberg [6]; see also Borel [1]). *Let* G *be a finitely generated group of matrices in a field* k *of characteristic* 0 . *Then* G *contains a normal torsion-free subgroup of finite index.*

Proof. We can take for C the set of non-zero elements of A, A^{-1} , where A runs through a set of generators of G , and for K the subfield of k generated by C . We can also suppose that $p \neq 2$. If α is as given by Theorem I, the elements of the matrices in αG are all in the p-adic integers Z_p . The subgroup of αG consisting of the matrices of the type $I + pB$, where B has elements in Z_p , is clearly normal and is torsion-free. [For we have to show that $(I+pB)^n \neq I$ whenever $B \neq 0$ and it is enough to show this when n is a prime. But then $(I+pB)^n = I + npB + \ldots + p^nB^n$ and the largest element of npB is p-adically greater than the elements of the subsequent terms. The condition $p \neq 2$ is needed when $n = p$.]

The proof given below of Theorem I follows Lech's argument quite closely. There is an additional twist, but that is also familiar from other contexts. We require three simple lemmas.

LEMMA 1. *Let*

$$f_j(X_1, \ldots, X_n) \in \mathsf{Z}[X_1, \ldots, X_n] \quad (1 \leq j \leq J)$$
$$\neq 0$$

be a finite set of non-zero polynomials in the indeterminates $X_1, \ldots, X_n$ *with rational integral coefficients. Then there are rational integers* $a_1, \ldots, a_n$ *such that*

$$f_j(a_1, \ldots, a_n) \neq 0 \quad (1 \leq j \leq J) .$$

Proof. If $n = 1$ pick a_1 distinct from the finitely many roots of the f_j . If $n > 1$ use induction to pick $a_2, \ldots, a_n$ so that $f_j(X_1, a_2, \ldots, a_n) \neq 0$ and then pick a_1 .

LEMMA 2. *Let* $g(X) \in \mathsf{Z}[X]$ *be a non-constant polynomial in the single indeterminate* X *with rational integral coefficients. Then there*

https://doi.org/10.1017/S000497270002503X Published online by Cambridge University Press

are infinitely many primes p *for which there is a solution* $b \in Z$ *of the congruence*

$$g(b) \equiv 0 \pmod{p} .$$

Proof. Let β be a root of $g(\beta) = 0$. Then it is enough to show that there are infinitely many first-degree primes in $Q(\beta)$; and this follows from elementary analytic number-theory. (See, for example, Borevich and Shafarevich [2], Chapter V, §3.1.)

LEMMA 3. Q_p *has infinite transcendence degree over* Q .

Proof. For Q_p is uncountable but the algebraic closure of any extension of Q of finite transcendence degree is countable.

Proof of Theorem I. We note first that, by taking a larger set for C if necessary, we may suppose that $c^{-1} \in C$ whenever $c \in C$. It will thus be enough to find primes p and embeddings α for which

(1) $$|\alpha c| \leq 1 \quad (\text{all } c \in C).$$

Let $x_1, \ldots, x_m$ $(m \geq 0)$ be a transcendence base of K over Q. Then $x_1, \ldots, x_m$ are independent transcendentals and

$$K = Q(y, x_1, \ldots, x_m)$$

for some $y \in K$ which is algebraic over $Q(x_1, \ldots, x_m)$. We can thus put each $c \in C$ into the shape

$$c = U_c(y, x_1, \ldots, x_m) / V_c(x_1, \ldots, x_m)$$

where

(2) $$\begin{cases} U_c(Y, X_1, \ldots, X_m) \in Z[Y, X_1, \ldots, X_m] , \\ \text{and} \\ \quad V_c(X_1, \ldots, X_m) \in Z[X_1, \ldots, X_m] \\ \qquad\qquad \neq 0 \end{cases}$$

Here Z denotes the rational integers and $Y, X_1, \ldots, X_m$ are indeterminates.

We can select an irreducible equation $G(Y) = 0$ for y over

$Q(x_1, \ldots, x_m)$ of the shape

$$G(Y) = H(Y, x_1, \ldots, x_m)$$

where

$$H(Y, X_1, \ldots, X_m) \in Z[Y, X_1, \ldots, X_m] .$$

If H is of degree s in Y we denote the coefficient of Y^s by $H_0(X_1, \ldots, X_m)$, so

$$H_0(X_1, \ldots, X_m) \in Z[X_1, \ldots, X_m]$$
$$\neq 0 .$$

The discriminant of $G(Y)$ is of the shape $\Delta(x_1, \ldots, x_m)$, where

$$\Delta(X_1, \ldots, X_m) \in Z[X_1, \ldots, X_m]$$
$$\neq 0 .$$

By Lemma 1 we can pick $a_1, \ldots, a_m \in Z$ such that

(3) $$\Delta(a_1, \ldots, a_m) \neq 0 ,$$

(4) $$H_0(a_1, \ldots, a_m) \neq 0 ,$$

(5) $$V_c(a_1, \ldots, a_m) \neq 0 \quad (\text{all } c \in C).$$

By (4) and Lemma 2 there are infinitely many primes $p \neq 2$ for which there is a solution $b \in Z$ of the congruence

(6) $$H(b, a_1, \ldots, a_m) \equiv 0 \pmod{p} .$$

On excluding finitely many of these primes we may also suppose by (3), (4), (5), that

(7) $$\Delta(a_1, \ldots, a_m) \not\equiv 0 \pmod{p} ,$$

(8) $$H_0(a_1, \ldots, a_m) \not\equiv 0 \pmod{p} ,$$

(9) $$V_c(a_1, \ldots, a_m) \not\equiv 0 \pmod{p} \quad (\text{all } c \in C).$$

By Lemma 3 we can select m independent transcendentals $\theta_1, \ldots, \theta_m$ in Q_p. On replacing the θ_j by $p^t\theta_j$ with large positive integral t

if necessary, we may suppose that

$$|\theta_j| < 1 \quad (1 \le j \le m) .$$

Then

$$\xi_j = a_j + \theta_j \quad (1 \le j \le m)$$

is a set of independent transcendentals in $\mathbb{Q}_p$ with

$$|\xi_j - a_j| < 1 . \tag{10}$$

Now by (6), (7), (10) and Hensel's Lemma there is an $\eta \in \mathbb{Q}_p$ with $|\eta - b| < 1$ and

$$H(\eta, \xi_1, \ldots, \xi_m) = 0 .$$

Thus

$$x_j \to \xi_j \quad (1 \le j \le m) ,$$
$$y \to \eta$$

defines an isomorphism α of $K = \mathbb{Q}(y, x_1, \ldots, x_m)$ with $\mathbb{Q}(\eta, \xi_1, \ldots, \xi_m) \subset \mathbb{Q}_p$.

Further,

$$|U_c(\eta, \xi_1, \ldots, \xi_m)| \le 1 , \quad |V_c(\xi_1, \ldots, \xi_m)| \le 1$$

by (2) and since $|\xi_j| \le 1$, $|\eta| \le 1$; and indeed

$$|V_c(\xi_1, \ldots, \xi_m)| = 1$$

by (9) and (10). Hence

$$\begin{aligned} |\alpha c| &= |U_c(\eta, \xi_1, \ldots, \xi_m)| / |V_c(\xi_1, \ldots, \xi_m)| \\ &\le 1 . \end{aligned}$$

This completes the proof.

https://doi.org/10.1017/S000497270002503X Published online by Cambridge University Press

References

[1] Armand Borel, "Compact Clifford-Klein forms of symmetric spaces", *Topology* 2 (1963), 111-122.

[2] Z.I. Borevich and I.R. Shafarevich, *Number theory* (translated by Newcomb Greenleaf for Scripta Technica. Pure and Applied Mathematics, 20. Academic Press, New York and London, 1966).

[3] Christer Lech, "A note on recurring series", *Ark. Mat.* 2 (1954), 417-421.

[4] Kurt Mahler, "Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen", *Proc. K. Nederl. Akad. Wetensch. Amsterdam* 38 (1935), 50-60.

[5] K. Mahler, "On the Taylor coefficients of rational functions", *Proc. Cambridge Philos. Soc.* 52 (1956), 39-48.

[6] Atle Selberg, "On discontinuous groups in higher-dimensional symmetric spaces", *Contributions to function theory*, 147-164 (International Colloquium on Function Theory, Bombay, 1960. Tata Institute of Fundamental Research, Bombay, 1960).

Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge,
Cambridge,
UK.