***Theorem*** 1 (Lech's embedding theorem). Let $L$ be any field which is finitely generated over $\mathbb{Q}$, and $S$ be a finite subset of $L$. Then for infinitely many primes $p$, there exists a field embedding $\imath\colon L \to \mathbb{Q}_p$ such that $\imath(S) \subset \mathbb{Z}_p$.

*Proof.* We begin with the following lemma.

***Lemma*** 1. For any non-constant polynomial $g \in \mathbb{Q}[x]$ there exists infinitely many primes $p$ such that $g$ admits a solution modulo $p$ (in the sense that there exists an integer $b \in \mathbb{N}$ such that $|g(b)|_p < 1$).

Granting this lemma we proceed with the proof of the theorem.

Let $d$ be the degree of transcendance of $L$ over $\mathbb{Q}$. Then $L$ is a finite extension of the field $F = \mathbb{Q}(t_1, \cdots, t_d)$. By the primitive element theorem, we may find $\theta$ such that $L = F[\theta]$. Denote by $f(x) = x^d + c_1(t)x^{d-1} + \cdots + c_d(t)$ the minimal polynomial of $\theta$ over $F$. This is an irreducible polynomial, which has only simple roots. In particular its discriminant $\Delta(f)$ is a non-zero constant in $F$.

We may (and shall) suppose that $\theta$ and all $c_i$'s belong to $S$.

Note that any element of $L$ is a polynomial in $\theta$ with coefficients in $F$, hence we may find $P \in \mathbb{Z}[t]$ such that $P \cdot s \in \mathbb{Z}[t, \theta]$ for all $s \in S$.

***Lemma*** 2. For any non-zero element $\Phi \in F$ there exist infinitely many $a \in \mathbb{N}^d$ such that $\Phi(a_1, \cdots, a_d) \neq 0$.

Apply the previous lemma to $\Phi := \Delta(f) \times P$, and fix $a \in \mathbb{N}^d$ such that $\Phi(a) \neq 0$. Now pick a prime $p$ such that the following conditions hold:

(1) $|f_a(b)|_p < 1$ for some $b \in \mathbb{N}$;
(2) $|\Delta(f_a)|_p = 1$;
(3) $|P(a)|_p = 1$.

Observe that conditions (2) and (3) are satisfied for all but finitely many primes since $\Phi(a) \in \mathbb{Q}^*$. And condition (1) is satisfied for infinitely many primes by Lemma 1. In the remaining of the proof $p$, $b$ and $a$ are fixed.

We first build the field embedding on $F$. As $\mathbb{Q}_p$ is uncountable, we may find $\epsilon_1, \cdots, \epsilon_d \in \mathbb{Q}_p$ which are algebraically independent over $\mathbb{Q}$. Dividing them by a suitable power of $p$, we may suppose that $|\epsilon_i| =$ for all $i$. We set $\imath(t_i) := a_i + p\epsilon_i$. Note that $a_1 + p\epsilon_1, \cdots, a_d + p\epsilon_d \in \mathbb{Q}_p$ are algebraically independent over $\mathbb{Q}$, hence $\imath$ extends to a field embedding $\imath\colon F \to \mathbb{Q}_p$. Our aim is now to extend $\imath$ to $L$.

Recall that by construction $P(t) \in \mathbb{Z}(t)$ and $P(t) \cdot c_i(t) \in \mathbb{Z}[t]$. Consider the polynomial $f_{a+p\epsilon}(x) = x^d + c_1(a+p\epsilon)x^{d-1} + \cdots + c_d(a+p\epsilon) \in \mathbb{Z}_p[x]$. By (3), we have $|P(a+p\epsilon) - P(a)|_p \leq 1/p < 1$, and $|c_i(a+p\epsilon) - c_i(a)|_p \leq 1/p < 1$, so that

$$|f_{a+p\epsilon}(b)|_p = |f_{a+p\epsilon}(b) - f_a(b)|_p \leq \max_i\{|c_i(a+p\epsilon) - c_i(a)|_p\} < 1$$

Since $|\Delta(f_a)|_p = 1$, we obtain $\Delta(\tilde{f}_a) = \widetilde{\Delta(f_a)} \neq 0$ hence $\tilde{f}_a \in \mathbb{F}_p[x]$ has only simple roots.

It follows that $\tilde{f}_a(x) = (x - \tilde{b})Q(x)$ with $Q(\tilde{b}) \neq 0$ and $\tilde{f}'_a(\tilde{b}) \neq 0$, which implies $|f'_{a+p\epsilon}(b)|_p = 1$. We may thus apply Hensel's lemma to the polynomial $f_{a+p\epsilon}$ and the approximate root $b$, and we conclude to the existence of $\beta \in \mathbb{Q}_p$ such that $f_{a+p\epsilon}(\beta) = 0$ and $|\beta - b| < 1$ (hence in particular $|\beta| \leq 1$).

Extend $\imath$ to a ring homomorphism $\imath\colon F[x] \to \mathbb{Q}_p$ by setting $\imath(x) = \beta$. By construction the kernel of $\imath$ contains the polynomial $f$, since

$$\imath(f) = \imath(x^d + c_1(t)x^{d-1} + \cdots + c_d(t)) = \beta^d + c_1(a + p\epsilon)\beta^{d-1} + \cdots + c_d(a + p\epsilon) = 0$$

It follows that $\imath$ factors through $F[x]/(f)$ which is isomorphic to $L$. We obtain in this way a field embedding $\imath\colon L \to \mathbb{Q}_p$ satisfying $\imath(\theta) = \beta$.

Now pick any $s \in S$, and write $P\cdot s = Q(t,\theta)$ with $Q \in \mathbb{Z}[t,x]$. Then $|\imath(s)|_p \times |P(a+p\epsilon)|_p \leq 1$, and since $P \in \mathbb{Z}[t]$, and $|P(a)|_p = 1$ we conclude that $|\imath(s)|_p \leq 1$ as required. □

*Proof of Lemma 2.* We may suppose that $\Phi$ is a polynomial. We prove the theorem by induction on $d$. For $d = 1$, then it follows from the fact that $\mathbb{N}$ is infinite and a non-constant polynomial admits only finitely many zeroes. Write $\Phi(t_0, t_1, \cdots, t_d) = \sum_I \Phi_I(t_0)T^I$ with $T = (t_1, \cdots, t_d)$. By the previous argument there exists an integer $a_0$ such that $\Phi_I(a_0) \neq 0$ for all multi-indices $I$ such that $\Phi_I \neq 0$. To conclude, we apply the induction step to $\Phi(a_0, t_1, \cdots, t_d)$. □

*Proof of Lemma 1.* We may suppose that $f \in \mathbb{Z}[x]$. We proceed by contradiction, and pick a finite set of primes $P := \{p_1, \cdots, p_n\}$ such that all primes factors of $f(b)$ belong to $P$ for all $b \in \mathbb{N}$.

Set $N = p_1 \cdots p_k$ and choose an integer $a \in \mathbb{N}$ such that $f(a) \neq 0$. Since all prime factors of $f(a)$ belongs to $P$, there exists an integer $j \geq 1$ such that $f(a)|\ N^{j-1}$. Observe that for each $n$, we have $f(a + N^j n) = f(a) \mod (N^j)$. Note that

$$|f(a)|_{p_i} \geq |N^{j-1}|_{p_i} = p_i^{1-j} > |N^j|_{p_i}$$

hence $|f(a + N^j n)|_{p_i} = |f(a)|_{p_i}$ for all $i = 1, \cdots, k$.

Since all prime factors of $f(a + N^j n)$ belong to $P$, we infer $f(a + N^j n) = \pm f(a)$. This implies one of the two polynomials $f(a + N^j T) \pm f(a)$ to have infinitely many roots which is absurd. □

CNRS - Centre de Mathématiques Laurent Schwartz, École Polytechnique, 91128 Palaiseau Cedex, France

*Email address*: charles.favre@polytechnique.edu