Can. J. Math., Vol. XXVI, No. 2, 1974, pp. 473–491

SOME SUBFIELDS OF Q_p AND THEIR NON-STANDARD ANALOGUES

DIANA L. DUBROVSKY

1. Introduction. The desire to study constructive properties of given mathematical structures goes back many years; we can perhaps mention L. Kronecker and B. L. van der Waerden, two pioneers in this field. With the development of recursion theory it was possible to make precise the notion of "effectively carrying out" the operations in a given algebraic structure. Thus, A. Frölich and J. C. Shepherdson [7] and M. O. Rabin [13] studied computable algebraic structures, i.e. structures whose operations can be viewed as recursive number theoretic relations. A. Robinson [18] and E. W. Madison [11] used the concepts of computable and arithmetically definable structures in order to establish the existence of what can be called non-standard analogues (in a sense that will be specified later) of certain subfields of **R** and **C**, the standard models for the theories of real closed and algebraically closed fields respectively.

In this paper we are interested in $\mathbf{Q}_p$, the completion of the rationals with respect to the p-adic valuation. We define recursive p-adic numbers and show that they form a p-valued subfield of $\mathbf{Q}_p$, call it $\mathbf{Q}_p^{(R)}$, which satisfies Hensel's Lemma and is therefore a p-adically closed field. Every computable valued subfield of $\mathbf{Q}_p$ is a proper subfield of $\mathbf{Q}_p^{(R)}$, in fact $\mathbf{Q}_p^{(R)}$ cannot even be a computable field. In contrast to this, we show that there exist computable subfields of $\mathbf{Q}_p$ which are not computable p-valued fields. $\mathbf{Q}_p^{(R)}$ is, however, an arithmetically definable field and, *a fortiori* an arithmetically definable valued field.

We use the concept of computable and arithmetically definable structures in order to establish the existence of a non-standard analogue for $\mathbf{Q}_H$, the henselization of **Q** inside $\mathbf{Q}_p$, in the following sense: Let K_0 be the set of axioms for a p-adically closed field, let $\mathcal{N}(x)$ be a new unary predicate, let K_1 be the set of all true statements of arithmetic relativized to $\mathcal{N}(x)$ and let $K = K_0 \cup K_1 \cup A$, where $A = (x)[\mathcal{N}(x) \Rightarrow F(x)]$ and $F(x)$ means x is a field element.

A model for K consists of a p-adically closed field F in which we have distinguished a set $N \subset F$ which satisfies exactly the same first order statements as the natural numbers. We will denote these models by pairs $(F, \mathcal{N})$.

It is easy to see that K is not a complete theory. One "natural" (or standard)

Received November 15, 1972 and in revised form, July 12, 1973. Parts of this paper were submitted as a Ph.D. thesis to UCLA in 1971. The author wishes to thank Professor Abraham Robinson for his encouragement and advice.

model for K is $(\mathbf{Q}_H, \mathcal{N})$, where $\mathcal{N}$ stands for the standard natural numbers. If $\mathcal{N}^*$ is an arbitrary strong non-standard model of arithmetic, we show that there exists a p-adically closed field $\mathbf{Q}_H^*$ such that

$$(\mathbf{Q}_H^*, \mathcal{N}^*) \equiv (\mathbf{Q}_H, \mathcal{N}).$$

Moreover, this $\mathbf{Q}_H^*$ is essentially unique in the sense that if H^* is another p-adically closed field containing $\mathcal{N}^*$ and such that $(H^*, \mathcal{N}^*)$ and $(\mathbf{Q}_H^*, \mathcal{N}^*)$ are elementarily equivalent with respect to the field of quotients of $\mathcal{N}^*$ (a non-standard version of $\mathbf{Q}$ which is contained in both H^* and $\mathbf{Q}_H^*$), then they are in fact isomorphic. Furthermore, this isomorphism reduces to the identity if we assume that $(\mathbf{Q}_H^*, \mathcal{N}^*)$ is an elementary substructure of $(H^*, \mathcal{N}^*)$.

In the last section, we generalize the uniqueness result to all arithmetically definable p-valued subfields of $\mathbf{Q}_p$.

We will work within a convenient formulation of the Lower Predicate Calculus in which the concept of a valued field can be formalized, say as in [**15**], in terms of the relations $F(x)$, $G(x)$, $E(x, y)$, $S(x, y, z)$, $P(x, y, z)$, $\Sigma(x, y, z)$, $L(x, y)$, $V(x, y)$. These denote, in turn, the property of belonging to the field, the property of belonging to the group, The relation of equality, the relations of addition and multiplication in the field, the relations of addition and order in the group and the relation of valuation respectively.

It will simplify our arguments to assume that all models considered are normal, i.e. that the relation of equality coincides with the identity.

2. Recursive p-adic numbers. Let F be a field valued in an abelian group G. The set $I = \{x \in F : v(x) \geqq 0\}$ is called the valuation ring; the set $M = \{x \in F : v(x) > 0\}$ is a maximal ideal in I. The field $\bar{F} = I/M$ is called the residue class field. If $x \in I$, we denote by $\bar{x}$ the image of x under the canonical map $I \to I/M = \bar{F}$.

A valuation v of a field F of characteristic zero is a p-valuation if $v(p)$ is the smallest positive element of the valuation group, and the residue class field $F = \mathbf{F}_p$, the field with p elements. A field F is called formally p-adic if it admits a p-valuation; it is p-adically closed if it is formally p-adic and has no proper algebraic extensions which are formally p-adic.

A commutative group G is called a Z-group if it is totally ordered, has a minimum positive element, and G/nG has n elements for each integer n.

Next we list two ways of stating that property of some valued fields known as Hensel's Lemma. For a p-valued field they are equivalent (see [**14**]).

HENSEL'S LEMMA. *Let* $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $a_i \in I$. *Assume that there is an* $\alpha \in I$ *such that* $f(\alpha) \equiv 0 \pmod{M}$, $f'(\alpha) \not\equiv 0 \pmod{M}$, *where* M *is the maximal ideal of* I *and* $f'(x)$ *is the formal derivative of* $f(x)$. *Then there exists a unique* $\alpha^* \in I$ *such that* $f(\alpha^*) = 0$ *and* $\alpha \equiv \alpha^* \pmod{M}$.

HENSEL-RYCHLIK PROPERTY. *Let* $f(x) \in I[x]$ *be monic and let* $\mathscr{D}f$ *denote the discriminant of* f. *If there exists an* $\alpha \in I$ *such that* $v(f(\alpha)) > v(\mathscr{D}f)$, *then there exists an* $\alpha^* \in I$ *such that* $f(\alpha^*) = 0$.

The following theorem can now be interpreted as a set of first order axioms for the concept of a p-adically closed field (see [**2**; **3**]).

THEOREM 2.1. *A p-valued field F is p-adically closed if*
(i) *F satisfies Hensel's Lemma, and*
(ii) *the valuation group $v(F^0)$ is a Z-group, where $F^0 = F - \{0\}$.*

THEOREM 2.2. *The elementary theory of p-adically closed fields is complete and axiomatizable, hence decidable* (see [**2**; **3**; **4**; **6**]).

Notice that the p-adic valuation on $\mathbf{Q}$ is a p-valuation and that the completion, $\mathbf{Q}_p$, is a p-adically closed field. We will denote the p-adic valuation on $\mathbf{Q}_p$ as well as its restriction to different subfields of $\mathbf{Q}_p$ by the letter v. Clearly, given a rational number $r \neq 0$, we can effectively find $v(r) \in \mathbf{Z}$.

The results that follow parallel in quite a remarkable way those obtained by Madison and Lachlan for the case of the real numbers. (See [**10**].)

Let $\varphi: \mathbf{Q} \to \mathbf{N}$ be an effective enumeration of the rationals; i.e., φ is a 1-1 function from the rational numbers onto the natural numbers with the property that there exist two algorithms, one for finding $\varphi(r) \in \mathbf{N}$ for each $r \in \mathbf{Q}$ and the other for finding $\varphi^{-1}(n) \in \mathbf{Q}$ for each $n \in \mathbf{N}$.

Thus, we can regard a rational number as "given," if the corresponding natural number is given. We say that a sequence of rational numbers is recursively enumerable (r.e.) if the corresponding sequence of natural numbers is the sequence of values $f(0), f(1), f(2), \ldots$ of a recursive function f.

Definition 2.3. A recursively enumerable sequence of rational numbers $\{r_n\}$ is said to be p-adically recursively convergent if there exists a recursive function $g(x)$ such that, for each $N > 0$, $v(r_{n+1} - r_n) > N$ for $n > g(N)$. $g(x)$ is called a convergence function for the sequence.

A p-adic number is recursive if it is the limit of an r.e., p-adically recursively convergent sequence of rationals.

Note. From now on, whenever we speak of convergence we will always mean convergence in the p-adic valuation.

It is easy to see that if $\{r_n\}$ is an r.e., recursively convergent sequence of rationals with convergence function $g(x)$ and with a as its limit, then $v(a - r_n) > N$ if $n > g(N)$. Conversely, if $\{r_n\}$ is an r.e. sequence of rationals and a is a p-adic number such that $v(r_n - a) > N$ if $n > g(N)$ for some recursive g, then $\{r_n\}$ is recursively convergent since

$$v(r_{n+1} - r_n) \geqq \min\{v(r_{n+1} - a), v(a - r_n)\} > N \quad \text{if } n > g(N),$$

and hence a is a recursive p-adic number.

Thus, this notion of a recursive p-adic number coincides with our "intuitive" idea of a "computable number", as one for which we can effectively produce as close a rational approximation as we want.

Recall that a p-adic number a has a unique canonical expansion in powers of p,

$$a = \sum_{i=-n}^{\infty} a_i p^i$$

where, for each i, $0 \leqq a_i < p$. Thus, the next definition is also natural.

Definition 2.4. A p-adic number $a = \sum_{i=-n}^{\infty} a_i p^i$, $0 \leqq a_i < p$, is called recursive if there exists a recursive function $f(x)$ such that $f(0) = a_0$, $f(2i) = a_i$, $f(2i - 1) = a_{-i}$. $f(x)$ is called an expanding function for a.

It is easy to show that the two definitions given for a recursive p-adic number are equivalent.

Our next aim is to show that the recursive p-adic numbers form a field and to investigate some of its properties.

LEMMA 2.5. *Let $\{r_n\}$ be an r.e. sequence of rationals recursively converging to $a \neq 0$, with recursive convergence function $g(x)$. Then there exists k such that $v(r_n) = k$ for all $n > g(\max\{k, 0\})$. $k = v(a)$ can be effectively found.*

Proof. Since $a \neq 0$, it has finite valuation. Let $k = v(a)$. We know that $v(r_n - a) > k$ for all $n > g(\max\{k, 0\})$. If for some $n > g(\max\{k, 0\})$, $v(r_n) \neq k$, then $v(r_n - a) \leqq v(a) = k$, a contradiction. Hence, for all $n > g(\max\{k, 0\})$ we must have $v(r_n) = k = v(a)$.

All we have to do now is to effectively determine $v(a)$. But we can effectively determine the valuation of any rational in the sequence $\{r_n\}$. We also know, since $a \neq 0$, that for some i, the coefficient of p^i, in the canonical expansion of a, is non-zero. Hence, for that same i, the coefficient of p^i in the canonical expansion of the r_n's must be non-zero from some n on.

Now, $v(r_{g(n)+1} - r_{g(n)+2}) > n$ for all n, i.e., the coefficients in the canonical expansions of these two terms of the sequence coincide up to and including the coefficient of p^n, and are the same as in the expansion of a since $v(r_{g(n)+1} - a) > n$ for all n. Therefore, in order to compute the valuation of a, all we have to do is to compute the coefficients of the canonical expansion of $r_{g(n)+1}$ up to and including the coefficient of p^n, for each n, until we find one which is $\neq 0$. (It will exist since $a \neq 0$.) Notice that if $v(a) < 0$, then $v(a) = v(r_{g(0)+1})$.

THEOREM 2.6. *The recursive p-adic numbers form a field.*

Proof. Let $a, b, c \neq 0$ be recursive p-adic numbers, given by r.e. recursively convergent sequences of rationals $\{a_i\}$, $\{b_i\}$, $\{c_i\}$ with recursive convergence functions g_1, g_2, g_3 respectively. Then obviously $\{a_i + b_i\}$, $\{a_i \cdot b_i\}$, $\{-a_i\}$ and $\{1/c_i\}$ are r.e. sequences of rationals converging to $a + b$, $a \cdot b$, $-a$ and $1/c$ respectively and it is easy, using the previous lemma, to give recursive convergence functions for each of them.

The field of recursive p-adic numbers will be denoted by $\mathbf{Q}_p^{(R)}$. It is a subfield of $\mathbf{Q}_p$, so we can consider it as a valued field by restricting the p-adic valuation of $\mathbf{Q}_p$ to $\mathbf{Q}_p^{(R)}$. This restriction of the p-adic valuation is again a p-valuation and thus $\mathbf{Q}_p^{(R)}$ is a formally p-adic field with valuation group $\mathbf{Z}$ and residue class field $\mathbf{F}_p$. The analogues of the next two definitions as well as of the proposition that follows were first considered by Rice [**15**] for the real numbers.

Definition 2.7 A sequence of recursive p-adic numbers $\{a_n\}$ is an r.e. sequence if there exist recursive functions $f(x, y)$ and $g(x, y)$ such that $f(i, y)$ enumerates a recursively convergent sequence of rationals $a_{i,0}, a_{i,1}, \ldots$ with a_i as limit and $g(i, y)$ as convergence function.

Definition 2.8. An r.e. sequence of recursive p-adic numbers is recursively convergent if there exists a recursive function $h(x)$ such that, for each N, $v(a_{n+1} - a_n) > N$ if $n > h(N)$.

PROPOSITION 2.9. *If $\{a_n\} \subset \mathbf{Q}_p^{(R)}$ is an r.e. sequence recursively converging to a, then $a \in \mathbf{Q}_p^{(R)}$. Thus, we may say that $\mathbf{Q}_p^{(R)}$ is recursively complete.*

THEOREM 2.10. *$\mathbf{Q}_p^{(R)}$ satisfies Hensel's Lemma.*

Proof. We will show that the following form of Hensel's Lemma holds in $\mathbf{Q}_p^{(R)}$. Let

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \quad a_i \in I, I = \{x \in \mathbf{Q}_p^{(R)} : v(x) \geqq 0\}.$$

Assume that $\alpha \in I$ and $f(\alpha) \equiv 0 \bmod p^{2r+1}$, $f'(\alpha) \not\equiv 0 \bmod p^{r+1}$ where $r \geqq 0$ and $f'(x)$ is the formal derivative of $f(x)$. Then there exists a unique $\alpha^* \in I$ such that $f(\alpha^*) = 0$ and $\alpha \equiv \alpha^* \bmod p^{r+1}$.

We will use the classical proof for $\mathbf{Q}_p$ (see [**4**]), and then show that the sequence constructed therein is an r.e., recursively convergent sequence of p-adic numbers.

Recall that the sequence, say α_n, is defined by

$$\alpha_1 = \alpha, \quad \alpha_{n+1} = \alpha_n - f(\alpha_n)/f'(\alpha_n).$$

It is then shown by induction that $\alpha_{n+1} \equiv \alpha_n \bmod p^{r+n}$ and $f(\alpha_n) \equiv 0 \bmod p^{2r+n}$.

The sequence $\{\alpha_n\}$ converges to an element of $\mathbf{Q}_p$, call it α^*, with the properties required in the conclusion of Hensel's Lemma. In order to show that $\alpha^* \in \mathbf{Q}_p^{(R)}$ all we must show is that $\{\alpha_n\}$ is an r.e. sequence in $\mathbf{Q}_p^{(R)}$. The convergence function given by $v(\alpha_{n+1} - \alpha_n) \geqq r + n$ is clearly recursive.

To show that $\{\alpha_n\}$ is an r.e. sequence, we must show that there exist two recursive functions $\varphi(x, y)$ and $\psi(x, y)$ such that $\varphi(i, y)$ enumerates a sequence of rationals converging to α_i with convergence function $\psi(i, y)$.

Since the coefficients of f are in $\mathbf{Q}_p^{(R)}$, let $\{a_{i,j}\}_{j=1,2,\ldots}$ be the r.e. sequence of rationals converging to a_i, with recursive convergence function g_i:

Let

$$f_j(x) = a_{0,j}x^n + a_{1,j}x^{n-1} + \ldots + a_{n,j}$$
$$f_j'(x) = na_{0,j}x^{n-1} + (n-1)a_{j,1}x^{n-2} + \ldots + a_{1,j}.$$

Let $\chi(x)$ enumerate the r.e. sequence of rationals converging to $\alpha_1 = \alpha$ with recursive convergence function g.

Now define $\varphi(i, y)$ as follows:

$$\varphi(1, y) = \chi(y), \quad \varphi(i+1, y) = \varphi(i, y) - f_y(\varphi(i, y))/f_y'(\varphi(i, y)).$$

Since the $\{a_{i,j}\}_{j=1,2,\ldots}$ $0 \leqq i \leqq n$, are r.e. sequences of rationals, it is clear that $\varphi(i, y)$ is recursive and that the sequence it enumerates converges to α_i. We must find a recursive function $\psi(i, y)$ such that

$$v(\varphi(i, y+1) - \varphi(i, y)) > N, \quad \text{if } y > \psi(i, N).$$

ψ will be defined by induction on i. Clearly $\psi(1, y) = g(y)$. To define $\psi(i, y)$ we notice that, for each i,

$$\varphi(i, y) = \varphi(1, y) + \sum_{j=1}^{i-1} (-1)^j \frac{f_y(\varphi(j, y))}{f_y'(\varphi(j, y))}.$$

Thus

$$v[\varphi(i, y+1) - \varphi(i, y)] \geqslant \min_{1 \leqslant j \leqslant i-1} \left\{ v(\varphi(1, y+1) - \varphi(1, y)), \right.$$
$$\left. v\left(\frac{f_{y+1}(\varphi(j, y+1))}{f_{y+1}'(\varphi(j, y+1))} - \frac{f_y(\varphi(j, y))}{f_y'(\varphi(j, y))} \right) \right\}.$$

Now, $v(\varphi(1, y+1) - \varphi(1, y)) = v(\chi(y+1) - \chi(y)) > N$ if $y > g(N) = \psi(1, N)$.

We must now examine

$$v\left(\frac{f_{y+1}(\varphi(j, y+1))}{f_{y+1}'(\varphi(j, y+1))} - \frac{f_y(\varphi(j, y))}{f_y'(\varphi(j, y))} \right).$$

Clearly the denominator $f_{y+1}'(\varphi(j, y+1))f_y'(\varphi(j, y))$ has a finite fixed valuation from some point on since it converges to $[f'(\alpha_j)]^2$ which is not congruent to zero mod p. This finite valuation can be effectively found.

It can be shown by induction on the degree of the polynomial f that the numerator $f_{y+1}(\varphi(j, y+1))f_y'(\varphi(j, y)) - f_y(\varphi(j, y))f_{y+1}'(\varphi(j, y+1))$ will factor and regroup appropriately so that $\psi(i, y)$ is seen to be recursive.

Let us consider the special case in which the polynomial f is of degree 3. Then

$$
\begin{aligned}
&f_{y+1}(\varphi(j, y+1))f_y'(\varphi(j, y)) - f_y(\varphi(j, y))f_{y+1}'(\varphi(j, y+1)) = \\
&\quad (a_{0,y+1}\varphi(j, y+1)^3 + a_{1,y+1}\varphi(j, y+1)^2 + a_{2,y+1}\varphi(j, y+1) + a_{3,y+1}) \\
&\quad \times (3a_{0,y}\varphi(j, y)^2 + 2a_{1,y}\varphi(j, y) + a_{2,y}) \\
&\quad - (a_{0,y}\varphi(j, y)^3 + a_{1,y}\varphi(j, y)^2 + a_{2,y}\varphi(j, y) + a_{3,y}) \\
&\quad \times (3a_{0,y+1}\varphi(j, y+1)^2 + 2a_{1,y+1}\varphi(j, y+1) + a_{2,y+1}) \\
&\quad = 3a_{0,y+1}a_{0,y}\varphi(j, y+1)^2\varphi(j, y)^2[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + 2a_{1,y+1}a_{1,y}\varphi(j, y+1)\varphi(j, y)[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + a_{2,y+1}a_{2,y}[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + 2a_{0,y+1}a_{1,y}\varphi(j, y+1)^2\varphi(j, y)[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + 2a_{1,y+1}a_{0,y}\varphi(j, y+1)\varphi(j, y)^2[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + \varphi(j, y+1)^2\varphi(j, y)^2[a_{1,y+1}a_{0,y} - a_{0,y+1}a_{1,y}] \\
&\quad + a_{0,y+1}a_{2,y}\varphi(j, y+1)^2[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + a_{2,y+1}a_{0,y}\varphi(j, y)^2[\varphi(j, y+1) - \varphi(j, y)] \\
&\quad + 2\varphi(j, y+1)\varphi(j, y)[a_{2,y+1}a_{0,y}\varphi(j, y) - a_{0,y+1}a_{2,y}\varphi(j, y+1)] \\
&\quad + [a_{3,y+1}a_{2,y} - a_{2,y+1}a_{3,y}] \\
&\quad + 3[a_{3,y+1}a_{0,y}\varphi(j, y)^2 - a_{3,y}a_{0,y+1}\varphi(j, y+1)^2] \\
&\quad + 2[a_{3,y+1}a_{1,y}\varphi(j, y) - a_{3,y}a_{1,y+1}\varphi(j, y+1)].
\end{aligned}
$$

The valuation of the bracketed factor in each term can be made bigger than M provided y is greater than a "recursive combination" of $\psi(j, M)$ with $j < i$ and the $g_k(M)$, $k = 0, 1, 2, 3$.

Therefore, $\psi(i, y)$ will be defined in terms of a recursive combination of $\psi(j, y)$, $j < i$, and $g_k(y)$ and individual valuations which can be effectively found. Hence $\psi(i, y)$ is recursive.

The computations for the general inductive step are straightforward but messy.

Thus we have shown that $\mathbf{Q}_p^{(R)}$ is a p-adically closed field.

Notice that if we define an arithmetical p-adic number as the limit of an arithmetical sequence of rationals for which there exists an arithmetical convergence function, or as one which is given by an arithmetical expanding function, we can show that these two definitions are equivalent and then proceed as in the case of recursive p-adic numbers and show that they too form a field, call it $\mathbf{Q}_p^{(A)}$, which is "arithmetically complete" in the sense of proposition 2.9, and, finally that $\mathbf{Q}_p^{(A)}$ is also a p-adically closed field.

3. Computable and arithmetically definable valued fields.

Definition 3.1. A field F valued in an ordered group G is said to be a computable valued field if there exists a 1-1 map φ from the disjoint union of F and G (denoted $F \cup G$) into $\mathbf{N}$ such that

(i) $\varphi[F]$ and $\varphi[G]$ are recursive subsets of $\mathbf{N}$,

(ii) $\varphi[F] \cap \varphi[G] = \phi$, and

(iii) φ takes the relations $S(x, y, z)$ and $P(x, y, z)$ of the field F, $\Sigma(x, y, z)$ and $L(x, y)$ of the group G and the valuation $V(x, y)$ onto recursive number theoretic relations.

The map φ is called an admissible indexing for the valued field F.

Notice that if φ is an admissible indexing for an algebraic structure S, then $\psi: S \to \mathbf{N}$ defined by $\psi(x) = q^{\varphi(x)}$ for each $x \in S$, where q is a fixed prime, is also an admissible indexing for S.

Several examples of computable valued fields have been known for some time, e.g., the field of rational numbers $\mathbf{Q}$ considered as a valued field with the p-adic valuation is a computable valued field. Another far more interesting example of a computable valued field is the henselization of $\mathbf{Q}$ in $\mathbf{Q}_p$, which we will denote by $\mathbf{Q}_H$.

Our next aim is to investigate the relationship between computable valued subfields of $\mathbf{Q}_p$ and the field of recursive p-adic numbers, $\mathbf{Q}_p^{(R)}$.

LEMMA 3.2. *Let F be a computable p-valued subfield of $\mathbf{Q}_p$ and let φ be an admissible indexing for F. Then φ is effective on* $\mathbf{Q}$ (i.e., given any $r \in \mathbf{Q}$ we can effectively find its image under φ) *and also on the value group* $\mathbf{Z}$.

THEOREM 3.3. *Every computable p-valued subfield of $\mathbf{Q}_p$ is a subfield of $\mathbf{Q}_p^{(R)}$.*

Proof. Let F be a computable p-valued subfield of $\mathbf{Q}_p$, and let $\varphi: F \cup \mathbf{Z} \to \mathbf{N}$ be an admissible indexing. Let $0'$ be the image under φ of $0 \in F$.

Let $n \in \varphi[F]$, $n \neq 0'$. We will show that the expanding function of $\varphi^{-1}(n)$ is recursive.

Since $n \neq 0'$, $\exists y V'(n, y)$. Let $y_0 = \mu y V'(n, y)$. y_0 is the image under φ of the valuation of $\varphi^{-1}(n)$.

Let $j = \mu i V'(\varphi(p^i), y_0)$. Since $\exists i V'(\varphi(p^i), y_0)$, we can effectively find j. The first non-zero coefficient in the canonical expansion of $\varphi^{-1}(n)$ will be the coefficient of p^j. To find out what this coefficient is, notice first that $D'(x, y, z) \equiv S'(y, z, x)$ is a recursive number theoretic relation which holds if and only if $\varphi^{-1}(x) - \varphi^{-1}(y) = \varphi^{-1}(z)$.

The first non-zero coefficient in the canonical expansion of $\varphi^{-1}(n)$ is x if and only if

$$0 \leqq x \leqq p - 1 \ \& m_0 = \mu m D(n, \varphi(xp^j), m) \ \& \\ \& y_1 = \mu y V'(m_0, y) \ \& L'(y_0, y_1)$$

where $L'(x, y)$ is the recursive number theoretic relation corresponding to the order relation $L(x, y)$[or $x < y$] in $\mathbf{Z}$.

To find the next non-zero coefficient in the canonical expansion of $\varphi^{-1}(n)$, we consider $\varphi^{-1}(m_0)$ and proceed in the same way as before.

Clearly this procedure is effective, and it gives us all the coefficients in the canonical expansion of $\varphi^{-1}(n)$ for each $n \in \varphi[F]$. Hence $F \subset \mathbf{Q}_p^{(R)}$.

THEOREM 3.4. *$\mathbf{Q}_p^{(R)}$ is not a computable valued field.*

Proof. Suppose it were and let φ be an admissible indexing. Consider the enumeration of $\mathbf{Q}_p^{(R)}$ given by $\{\varphi^{-1}(n): n \in \varphi[\mathbf{Q}_p^{(R)}]\}$. Since $\varphi[\mathbf{Q}_p^{(R)}]$ is assumed to be a recursive subset of $\mathbf{N}$, we can effectively decide, for each $n \in \mathbf{N}$ whether $n \in \varphi[\mathbf{Q}_p^{(R)}]$ or not.

Let a be the p-adic integer whose canonical expansion is given by the following rule: coefficient of p^n, if $n \in \varphi[\mathbf{Q}_p^{(R)}]$, = coefficient of p^n in the canonical expansion of $\varphi^{-1}(n)$, plus 1, if this latter coefficient is less than $p - 1$. Coefficient of $p^n = 0$ otherwise.

Since we can effectively find any coefficient in the canonical expansion of $\varphi^{-1}(n)$ for $n \in \varphi[\mathbf{Q}_p^{(R)}]$ this procedure is effective and hence $a \in \mathbf{Q}_p^{(R)}$. But by construction $a \neq \varphi^{-1}(n)$ for all $n \in \varphi[\mathbf{Q}_p^{(R)}]$. Therefore, $\mathbf{Q}_p^{(R)}$ is not a computable valued field.

Kochen [9] showed that if K is a p-adically closed field, there exists a unique p-valuation on K and that the ring of integers consists of the elements of the form $\gamma(w)$ for some $w \in K$, where

$$\gamma(w) = \frac{1}{2p}\left[(w^p - w + 1)^{-1} + (w^p - w - 1)^{-1}\right].$$

Since the p-adic valuation on $\mathbf{Q}_p^{(R)}$ is a p-valuation, its ring of integers is characterized as above and thus we have

THEOREM 3.5. *$\mathbf{Q}_p^{(R)}$ is not a computable field.*

Proof. Assume $\mathbf{Q}_p^{(R)}$ is a computable field, and let $\varphi: \mathbf{Q}_p^{(R)} \to \mathbf{N}$ be an admissible indexing. We know that, for each $x \in \mathbf{Q}_p^{(R)}$, $v(x) \geqq 0$ if and only if there exists w such that $[x = (1/2p)((w^p - w + 1)^{-1} + (w^p - w - 1)^{-1})]$. Hence, the image under φ of the ring of integers I of $\mathbf{Q}_p^{(R)}$, call it A, is an r.e. subset of $\mathbf{N}$. Let $g(x)$ be a recursive function enumerating it. We shall describe an effective procedure, for deciding, for each $x \in \mathbf{Q}_p^{(R)}$, whether $v(x) \geqq 0$ or not. This will show that A is a recursive subset of $\mathbf{N}$.

Let $n \in \varphi[\mathbf{Q}_p^{(R)}]$ be fixed. We know that either $v(\varphi^{-1}(n)) \geqq 0$ or $v(1/\varphi^{-1}(n)) \geqq 0$. Hence either n or $\varphi(1/\varphi^{-1}(n))$ will appear first in the range of g. In case $\varphi(1/\varphi^{-1}(n))$ appears first, it is still possible for $\varphi^{-1}(n)$ to be an integer in $\mathbf{Q}_p^{(R)}$ since it can have valuation 0. So we check whether $\varphi(p \cdot \varphi^{-1}(n))$ or $\varphi(1/p\varphi^{-1}(n))$ appears first in the range of g. If $\varphi(1/p\varphi^{-1}(n))$ appears first in the range of g, since

$$v(1/p\varphi^{-1}(n)) \geqq 0 \Rightarrow -1 - v(\varphi^{-1}(n)) \geqq 0 \Rightarrow v(\varphi^{-1}(n)) \leqq -1,$$

we know that $n \notin A$, i.e., $v(\varphi^{-1}(n)) < 0$.

If $\varphi(p\varphi^{-1}(n))$ appears first in the range of g, since

$$v(p\varphi^{-1}(n)) \geqq 0 \Rightarrow 1 + v(\varphi^{-1}(n)) \geqq 0 \Rightarrow v(\varphi^{-1}(n)) \geqq -1,$$

we know that $v(\varphi^{-1}(n)) = 0$ or -1. In this last case, to decide whether $n \in A$ or not, repeat the preceding procedure with $\varphi(1 + \varphi^{-1}(n)^2)$ in place of n. There are 3 possibilities once again.

Notice that $v(1 + \varphi^{-1}(n)^2) \geqq \min\{0,\ 2v(\varphi^{-1}(n))\}$. If $v(x) \geqq 0$, then $v(\varphi^{-1}(n)) \geqq 0$ and $n \in A$. If $v(x) < 0$, then $v(\varphi^{-1}(n)) < 0$ and $n \notin A$. If $v(x) = 0$ or -1, then $v(x)$ must be 0 and hence $v(\varphi^{-1}(n)) = 0$ and $n \in A$.

Thus we have shown that A is a recursive subset of $\mathbf{N}$.

To compute the valuation of $\varphi^{-1}(n)$ for $n \in \varphi[\mathbf{Q}_p^{(R)}]$ we first check whether n is in A or not.

$$\text{If } n \in A,\ v(\varphi^{-1}(n)) = \mu i[\varphi(p^{-i} \cdot \varphi^{-1}(n)) \notin A] \dot{-} 1$$
$$\text{If } n \notin A,\ v(\varphi^{-1}(n)) = \mu i[\varphi(p^{i} \cdot \varphi^{-1}(n)) \in A].$$

Thus if $\mathbf{Q}_p^{(R)}$ were a computable field it would be a computable valued field since we can clearly construct an admissible indexing $\psi: \mathbf{Q}_p^{(R)} \cup \mathbf{Z} \to \mathbf{N}$ which takes the valuation onto a recursive number theoretic relation. This contradicts Theorem 3.4.

Actually, this proof works for any p-radically closed field F so we can state the following more general

THEOREM 3.6. *Let F be a p-adically closed field, G its value group and let $\varphi: F \to \mathbf{N}$ be an admissible indexing for the computability of F. Assume G is a computable group. Then there exists $\psi: F \cup G \to \mathbf{N}$ which is an admissible indexing for the computability of F as a valued field.*

In contrast to this, let us note that, for $\alpha \in \mathbf{Q}_p - \mathbf{Q}_p^{(R)}$, $\mathbf{Q}(\alpha)$ is a computable field [7] but not a computable valued field. In fact, if $K \subseteq \mathbf{Q}_p$ is not contained in $\mathbf{Q}_p^{(R)}$, no formally p-adic extension of K whose valuation extends that of K is a computable valued field.

Remark. If in Definition 3.1 we substitute arithmetical for recursive throughout, we obtain the definition of an arithmetically definable (A.D.) valued field. Recall that $\mathbf{Q}_p^{(A)}$, the field of arithmetical p-adic numbers, is a p-adically closed subfield of $\mathbf{Q}_p$. It is easy to see that the previous proofs carry over to the case of A.D. valued fields; thus we obtain that every A.D. p-valued subfield of $\mathbf{Q}_p$ is a proper subfield of $\mathbf{Q}_p^{(A)}$, furthermore $\mathbf{Q}_p^{(A)}$ is not even an A.D. field.

THEOREM 3.7. *$\mathbf{Q}_p^{(R)}$ is an arithmetically definable field.*

Proof. Recall that for each $a \in \mathbf{Q}_p^{(R)}$ there exists a unique canonical expansion

$$a = \sum_{i=-n}^{\infty} a_i p^i.$$

Hence, to each $a \in \mathbf{Q}_p^{(R)}$ there corresponds a unique recursive function, namely its expanding function.

Let $\{f_i\}$ be Kleene's effective enumeration of all unary partial recursive functions. Let

$$A = \{i : f_i \text{ is the expanding function for some } p\text{-adic number and } (j)[j < i \Rightarrow f_j \neq f_i]\}.$$

Notice that f is the expanding function for some p-adic number if and only if

$$\forall n[f(n) \in \{0, 1, \ldots, p-1\}] \,\&\, (\exists s)(\forall t)[t > s \,\&\, (\exists u)t = 2u + 1 \Rightarrow f(t) = 0].$$

Also, $(\forall n)[f_i(n) = \cup(\mu y T_1(i, n, y))]$.
Hence,

$$i \in A \equiv (n)[\cup(\mu y T_1(i, n, y)) \in \{0, 1, \ldots, p-1\}]$$
$$\,\&\, (\exists s)(t)[(\exists w)[t > s \,\&\, t = 2w + 1] \Rightarrow \cup(\mu y T_1(i, t, y)) = 0]$$
$$\,\&\, (j)[j < i \Rightarrow (m)[\cup(\mu y T_1(j, m, y)) \neq \cup(\mu y T_1(i, m, y))]]$$

and thus, A is an arithmetical set.

Let $\varphi : \mathbf{Q}_p^{(R)} \to \mathbf{N}$ be defined as follows: for $a \in \mathbf{Q}_p^{(R)}$, $\varphi(a) = i \Leftrightarrow i \in A \,\&\, f_i$ is the expanding function for a. Since for each $a \in \mathbf{Q}_p^{(R)}$ there exists exactly one $i \in A$ such that f_i is the expanding function for a, φ is well defined and $\varphi[\mathbf{Q}_p^{(R)}] = A$.

It is now easy to show that φ takes the relations $S(x, y, z)$ and $P(x, y, z)$ (sum and product of $\mathbf{Q}_p^{(R)}$) onto arithmetical number theoretical relations.

COROLLARY 3.8. *$\mathbf{Q}_p^{(R)}$ is an A.D. valued field.*

Proof. We use the same method as in Theorem 3.5 to show that the image under φ of the ring of integers of $\mathbf{Q}_p^{(R)}$ is recursive in S' and P', and hence arithmetical.

4. Existence and uniqueness of $\mathbf{Q}_H$*. In this section we will primarily discuss $\mathbf{Q}_H$, the Henselization of $\mathbf{Q}$ inside $\mathbf{Q}_p$. $\mathbf{Q}_H$ consists of all the elements of $\mathbf{Q}_p$ which are algebraic over $\mathbf{Q}$. It has been proved by Nerode [**12**] that $\mathbf{Q}_H$ is a computable field and hence, since it satisfies Hensel's Lemma, we can use Theorem 3.6 to conclude that it is a computable valued field. (See also [**5**].)

Let K_0 be a set of first order axioms for the concept of a p-adically closed field, e.g., as given by Theorem 2.1. As was mentioned earlier, K_0 is complete and axiomatizable and $\mathbf{Q}_H$ is a model of K_0.

Let $\mathcal{N}(x)$ be a new unary predicate; denote by K_1 the set of all true statements of arithmetic relativized to $\mathcal{N}(x)$, and let A denote the sentence $(x)[\mathcal{N}(x) \Rightarrow F(x)]$.

Let $K = K_0 \cup K_1 \cup A$. A model for K consists of a p-adically closed field F in which we have distinguished a subset $\mathcal{N} \subset F$ which satisfies exactly the same first order sentences as the natural numbers, i.e., $\mathcal{N} \subset F$ constitutes a strong model of arithmetic. We will denote these models by pairs $(F, \mathcal{N})$. If $\mathcal{N}$

is a strong model of arithmetic, and v is a p-valuation on $\mathbf{Q}$, the field of quotients of $\mathcal{N}$, then for F any p-adically closed field containing $\mathbf{Q}$, $(F,\mathcal{N})$ is a model of K. K is not complete, e.g. look at the sentence

$$(x)[F(x) \Rightarrow \exists y(\mathcal{N}(y) \,\&\, v(y) > v(x))].$$

Thus, the existence of non-standard analogues of $\mathbf{Q}_H$ (in the sense of Theorem 4.1) is not a consequence of completeness.

THEOREM 4.1. *Let $\mathcal{N}^*$ be any strong non-standard model of arithmetic. There exists a p-adically closed field $\mathbf{Q}_H^*$ containing $\mathcal{N}^*$ such that*

$$(\mathbf{Q}_H^*,\mathcal{N}^*) \equiv (\mathbf{Q}_H,\mathcal{N}).$$

Proof. The method used here is essentially the same used by A. Robinson and by E. W. Madison to obtain similar results for the case of algebraic and real algebraic numbers respectively.

Since $\mathbf{Q}_H$ is a computable valued field, there exists an admissible indexing $\varphi:\mathbf{Q}_H \cup \mathbf{Z} \to \mathcal{N}$ such that $\varphi[\mathbf{Q}_H] = \mathbf{Q}_H'$ and $\varphi[\mathbf{Z}] = \mathbf{Z}'$ are recursive subsets of $\mathcal{N}$; say they are defined by the recursive predicates $A(x)$ and $B(x)$ respectively. Recall that φ takes the relations $S(x, y, z)$, $P(x, y, z)$, $\Sigma(x, y, z)$, $L(x, y)$ and $V(x, y)$ onto recursive number-theoretic relations S', P', Σ', L' and V'.

The copy of the natural numbers contained in $\mathbf{Q}_H$ is carried by φ onto a subset of $\mathcal{N}$, call it $\mathcal{N}'$. $\mathcal{N}'$ is recursively enumerable since it is the range of the recursive function $\{g(0) = 0'; g(1) = 1'; g(n + 1) = \sigma(g(n), 1')\}$ where $\sigma(x, y)$ is the function defined by the recursive predicate $S'(x, y, z)$, $0' = \varphi(0)$, $1' = \varphi(1)$ for $0, 1 \in \mathbf{Q}_H$.

Let $B(x, y)$ be the arithmetical predicate representing $y = g(x)$. It is clear that $B(x, y)$ satisfies the following properties:

(i) $(x)\,\exists y(z)[B(x, y) \,\&\, B(x, z) \Rightarrow y = z]$

(ii) $(x)(y)(z)[B(x, y) \,\&\, B(z, y) \Rightarrow x = z]$

(iii) $B(x_1, y_1) \,\&\, B(x_2, y_2) \,\&\, B(x_3, y_3) \Rightarrow [S(x_1, x_2, x_3) \Leftrightarrow S'(y_1, y_2, y_3)] \,\&\, [P(x_1, x_2, x_3) \Leftrightarrow P'(y_1, y_2, y_3)]$.

The predicate $\mathcal{N}'(x) \equiv A(x) \,\&\, \exists y B(y, x)$ defines the natural numbers arithmetically and

$$\mathcal{N}' = \{n \in \mathcal{N} : \mathcal{N}'(n) \text{ holds}\}.$$

The pair $(\mathbf{Q}_H',\mathcal{N}')$ together with the number theoretic predicates S', P', Σ', L', V' constitutes a model of K which is isomorphic to $(\mathbf{Q}_H,\mathcal{N})$.

Consider the subsets of $\mathcal{N}^*$ which are defined as follows:

$$\mathbf{Q}_H^* = \{n \in \mathcal{N}^* : A(n) \text{ holds}\},$$
$$\mathbf{Z}'^* = \{n \in \mathcal{N}^* : B(n) \text{ holds}\},$$
$$\mathcal{N}_1^* = \{n \in \mathcal{N}^* : \mathcal{N}'(n) \text{ holds}\}.$$

Since the predicates S', P', Σ', L', V' are all arithmetical, they define relations in $\mathcal{N}^*$ which, considered together with the sets $\mathbf{Q}_H^*$, $\mathbf{Z}'^*$, $\mathcal{N}_1^*$

determine a structure $(\mathbf{Q}_H^*, \mathcal{N}_1^*)$. It is not hard to see that $(\mathbf{Q}_H^*, \mathcal{N}_1^*)$ is a model of K which is elementarily equivalent to $(\mathbf{Q}_H, \mathcal{N})$. Furthermore, $\mathcal{N}_1^*$ is isomorphic to $\mathcal{N}^*$ since the function $\sigma : \mathcal{N}^* \to \mathcal{N}_1^*$ defined by: $\sigma(x) = y$ if and only if $\mathcal{N}^*$ satisfies $B(x, y)$, is an isomorphism by properties (i), (ii) and (iii) above.

From now on we will use the notation $(\mathbf{Q}_H^*, \mathcal{N}^*)$ for this particular model of K which is elementarily equivalent to $(\mathbf{Q}_H, \mathcal{N})$ where $\mathbf{Q}_H^* \subset \mathcal{N}^*$.

As pointed out by Madison, the proof of this theorem works for any A.D. structure, so in particular we have

THEOREM 4.2. *Given any strong non-standard model of arithmetic $\mathcal{N}^*$, there exists a p-adically closed field $H \supset \mathcal{N}^*$ such that $(H, \mathcal{N}^*) \equiv (\mathbf{Q}_p^{(R)}, \mathcal{N})$.*

Our next question is: In what sense can we say that $\mathbf{Q}_H^*$ is unique? To answer it we will need the following

LEMMA 4.3. *Let $\alpha \in \mathbf{Q}_H$. Then there exists a ploynomial $f(x) \in \mathbf{Q}[x]$, $r \in \mathbf{Q}$ and $n \in \mathbf{Z}$ such that r is a simple root of f mod p^n, α is of the form $r + p^{n+1}u$ for some u with $v(u) \geqq 0$, $f(\alpha) = 0$ and $f(\beta) \neq 0$ for all $\beta \neq \alpha$, β of the form $r + p^{n+1}u$ with $v(u) \geqq 0$.*

Proof. The lemma clearly follows from the case of α an integer in $\mathbf{Q}_H$.

Let $f(x) \in \mathbf{Q}[x]$ (in this case actually $f \in \mathbf{Z}[x]$) be the minimal polynomial for α over $\mathbf{Q}$, so $f(\alpha) = 0$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ be the distinct roots of f in $\mathbf{Q}_H$. There clearly exists an n such that $v(\alpha_i - \alpha_j) < n$ if $i \neq j$. A computation shows that it suffices to take $n = v(\mathscr{D}f) + 1$ where $\mathscr{D}f$ is the discriminant of the polynomial f. Let

$$r = \sum_{i=0}^{n} a_i p^i \quad \text{where} \quad \alpha = \sum_{i=0}^{\infty} a_i p^i.$$

Then $r \in \mathbf{Q}$, r is a simple root of f mod p^n, α is of the form $r + p^{n+1}u$ for some u with $v(u) \geqq 0$ and $f(\beta) \neq 0$ for all $\beta \neq \alpha$, β of the form $r + p^{n+1}u$ with $v(u) \geqq 0$.

Notice that, conversely, if $f(x) \in \mathbf{Q}[x]$ is monic, with integral coefficients and if there exists $r \in \mathbf{Q}$ such that $v(f(r)) > n$ where $n = \mathscr{D}f$, then by the Hensel-Rychlik Property there exists $\alpha \in \mathbf{Q}_H$ such that $f(\alpha) = 0$.

THEOREM 4.4. *Let $(\mathbf{Q}_H^*, \mathcal{N}^*)$ be as before and let H^* be another p-adically closed field containing N^*. The field of quotients of $\mathcal{N}^*$, say $\mathbf{Q}^*$, (a non-standard version of $\mathbf{Q}$) is contained in both $\mathbf{Q}_H^*$ and H^*. Assume $(\mathbf{Q}_H^*, \mathcal{N}^*)$ and $(H^*, \mathcal{N}^*)$ are elementarily equivalent with respect to $\mathbf{Q}^*$, thought of as a valued field, i.e. with constant symbols added for each $q \in \mathbf{Q}^*$ and each $z \in \mathbf{Z}^*$. Then these two models are isomorphic.*

Proof. With the aid of the previous lemma, we will construct a predicate $T(w, r, n, \alpha)$ expressible in the language of $(\mathbf{Q}_H, \mathcal{N})$ which will separate the

https://doi.org/10.4153/CJM-1974-046-0 Published online by Cambridge University Press

roots in $\mathbf{Q}_H$ of a polynomial with rational coefficients. Recall that $\mathcal{N}'(x) \equiv A(x) \,\&\, \exists y B(x, y)$ defines the natural numbers arithmetically. The predicates

$$I(x) \equiv \mathcal{N}'(x) \vee \exists y(\mathcal{N}'(y) \,\&\, S'(x, y, 0'))$$

and

$$R(x) \equiv \exists a \exists b[I(a) \,\&\, I(b) \,\&\, b \neq 0' \,\&\, P'(x, b, a)]$$

define arithmetically the integers and the rationals respectively.

If $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbf{Q}[x]$, define the Gödel number of f, say w, by $w = 2^n 3^{a_0'} \ldots p_{n+2}^{a_n'}$ where $a_i' = \varphi(a_i)$, φ an admissible indexing for the computability of $\mathbf{Q}$.

Let

$$\mathcal{G}(w) \equiv w = 0 \vee (\exists n)[((w)_0 = n) \,\&\, \exists y[lh(w) = y \,\&\, y \leqq n + 2] \,\&\, (i)(\exists x)[x = (w)_i \,\&\, 0 \leqq i \leqq n + 2 \Rightarrow R(x)]].$$

It is clear that we can choose the map φ and the Gödel numbering in such a way that the set of Gödel numbers of polynomials over $\mathbf{Q}$ is disjoint from the set $\varphi[\mathbf{Z}]$.

Let $\sigma(x, y)$ and $\pi(x, y)$ be the recursive functions determined by the predicates $S'(x, y, z)$, $P'(x, y, z)$ respectively. Define

$$\begin{cases} \rho(0, y) = 1' \\ \rho(n + 1, y) = \pi(y, \rho(n, y)) \end{cases} \qquad \lambda(w, i) = \begin{cases} 0', \text{ if } \chi_{\mathcal{G}}(w) = 1 \\ (w)_i, \text{ if } \chi_{\mathcal{G}}(w) = 0. \end{cases}$$

where $\chi_{\mathcal{G}}(w)$ is the characteristic function of $\mathcal{G}(w)$,

$$\psi(w, y, i) = \pi(\lambda(w, i), \rho(i, y))$$

and

$$s(w, y, 1) = (w)_1$$
$$s(w, y, k + 1) = \sigma(s(w, y, k), \psi(w, y, k + 1)).$$

With the aid of these arithmetical functions we can now construct a predicate $V(w, y, z)$ expressing the fact that "z is the result of substituting y for x in the polynomial with Gödel number w".

First, let $R(w, 0, n)$ be the predicate representing $(w)_0 = n$ and let

$$M(w, y, n, z) \equiv s(w, y, n) = z.$$

Now

$$V(w, y, z) \equiv \mathcal{G}(w) \,\&\, (n)[R(w, 0, n) \,\&\, M(w, n, y, z)]$$

is the desired arithmetical predicate, developed by E. Madison [**11**].

Consider now the following predicate:

$$\bar{B}(x, y) \equiv \exists a \exists b \exists a' \exists b'[N(a) \,\&\, N(b) \,\&\, N(a') \,\&\, N(b') \,\&\, R(y, a', b') \,\&\, B(a, a') \,\&\, B(b, b') \,\&\, P(b, x, a)]$$

where $R(y, a', b')$ is formed from $R(y)$ by deleting the two existential quanti-

https://doi.org/10.4153/CJM-1974-046-0 Published online by Cambridge University Press

fiers. Then $\bar{B}(x, y)$ expresses the fact that the natural number y represents the rational number x under the map φ which establishes the computability of $\mathbf{Q}$.

Let

$$T(w, r, n, \alpha) \equiv (\exists \beta)(\alpha = r + \beta \,\&\, v(\beta) \geqq n + 1) \,\&$$
$$(\lambda)(u)[\lambda = r + u \,\&\, v(u) \geqq n + 1 \,\&\, \lambda \neq \alpha \Rightarrow (\exists \lambda')(\exists v)(\exists u')$$
$$[\bar{B}(\lambda, \lambda') \,\&\, B(u, u') \,\&\, V(w, \lambda', v) \,\&\, v \neq 0']] \,\&\, (\exists r')(\exists r'')(\exists s)$$
$$[\bar{B}(r, r') \,\&\, V(w, r', r'') \,\&\, \bar{B}(s, r'') \,\&\, v(s) \geqq n].$$

Let

$$T(\alpha) \equiv \exists w \exists r \exists n T(w, r, n, \alpha).$$

The sentence $(x)T(x)$ holds in $(\mathbf{Q}_H, \mathcal{N})$ and hence in $(\mathbf{Q}_H{}^*, \mathcal{N}^*)$ since they are elementarily equivalent. Also, if $\alpha \in \mathbf{Q}_H$, then there exist $w, r \in \mathbf{Q}$, $b \in \mathbf{Z} = v(\mathbf{Q}^0)$ such that $T(w, r, n, \alpha)$ holds in $(\mathbf{Q}_H, \mathcal{N})$. Furthermore,

$$T(w, r, n, x) \Rightarrow [T(w, r, n, y) \Rightarrow x = y]$$

holds in $(\mathbf{Q}_H, \mathcal{N})$.

If $\alpha \in \mathbf{Q}_H{}^*$, there exist $w, r \in \mathbf{Q}^*$, $n \in v(\mathbf{Q}^{*0})$ such that $T(w, r, n, \alpha)$ holds in $(\mathbf{Q}_H{}^*, \mathcal{N}^*)$. Hence $\exists x T(w, r, n, x)$ holds in $(\mathbf{Q}_H{}^*, \mathcal{N}^*)$ and therefore it must hold in $(H^*, \mathcal{N}^*)$ because of elementary equivalence with respect to $\mathbf{Q}^*$. Let $\beta \in H^*$ be such that $T(w, r, n, \beta)$ holds in $(H^*, \mathcal{N}^*)$. Define $h: \mathbf{Q}_H{}^* \to H^*$ by $h(\alpha) = \beta$.

We claim that h is the desired isomorphism.

It is easy to check that h is well defined, 1-1 and onto.

To show that h is a homomorphism, suppose $\alpha_1, \alpha_2 \in \mathbf{Q}_H{}^*$ and let $\alpha = \alpha_1 + \alpha_2$. Let $\beta_1 = h(\alpha_1)$, $\beta_2 = h(\alpha_2)$, $\beta = \beta_1 + \beta_2$. There exist w_1, r_1, w_2, r_2, w, r in $\mathbf{Q}^*$, $n_1, n_2, n \in v(\mathbf{Q}^{*0})$ such that $T(w_1, r_1, n_1, \alpha_1)$, $T(w_2, r_2, n_2, \alpha_2)$, $T(w, r, n, \alpha)$ all hold in $(\mathbf{Q}_H{}^*, \mathcal{N}^*)$. Because of the definition of h, both $T(w_1, r_1, n_1, \beta_1)$ and $T(w_2, r_2, n_2, \beta_2)$ hold in $(H^*, \mathcal{N}^*)$. We must now show that $T(w, r, n, \beta)$ holds in $(H^*, \mathcal{N}^*)$.

Since $S(\alpha_1, \alpha_2, \alpha)$ holds in $\mathbf{Q}_H{}^*$, $(z)[S(\alpha_1, \alpha_2, z) \supset T(w, r, n, z)]$ holds in $(\mathbf{Q}_H{}^*, \mathcal{N}^*)$. Therefore

$$\exists\, !x \exists\, !y[[T(w_1, r_1, n_1, x) \,\&\, T(w_2, r_2, n_2, y)] \,\&\, (z)[S(x, y, z) \Rightarrow$$
$$T(w, r, n, z)]]$$

holds in $(\mathbf{Q}_H{}^*, \mathcal{N}^*)$ and hence in $(H^*, \mathcal{N}^*)$.

Since $h(\alpha_1) = \beta_1$, $h(\alpha_2) = \beta_2$, we have that

$$T(w_1, r_1, n_1, \beta_1) \,\&\, T(w_2, r_2, n_2, \beta_2)$$
$$\&\, (z)[S(\beta_1, \beta_2, z) \Rightarrow T(w, r, n, z)]$$

holds in $(H^*, \mathcal{N}^*)$. Hence $(z)S(\beta_1, \beta_2, z) \Rightarrow T(w, r, n, z)$ holds in $(H^*, \mathcal{N}^*)$; since $S(\beta_1, \beta_2, \beta)$ holds in H^*, we have that $T(w, r, n, \beta)$ holds in $(H^*, \mathcal{N}^*)$.

Clearly this proof works if we substitute P for S throughout. Therefore h is an isomorphism.

Note that, for a fixed $\mathcal{N}^*$, if we assume $(\mathbf{Q}_H^*, \mathcal{N}^*) \prec (H^*, \mathcal{N}^*)$, then in particular $(\mathbf{Q}_H^*, \mathcal{N}^*) \equiv_{\mathbf{Q}^*} (H^*, \mathcal{N}^*)$ since $\mathbf{Q}^*$ is contained in both H^* and $\mathbf{Q}_H^*$. Hence by the previous theorem, there exists an isomorphism $h: \mathbf{Q}_H^* \to H^*$. That this isomorphism is the identity on $\mathcal{N}^*$ (and hence on $\mathbf{Q}^*$) is clear from the definition of h and the fact that the polynomial $p(x) = x - a$ has a unique solution, namely a, for each $a \in \mathcal{N}^*$.

For each $\alpha \in \mathbf{Q}_H^* \subset H^*$, we have

$(\mathbf{Q}_H^*, \mathcal{N}^*)$ satisfies $T(w, r, n, \alpha)$ if and only if $(H^*, \mathcal{N}^*)$ satisfies $T(w, r, n, \alpha)$

since $(\mathbf{Q}_H^*, \mathcal{N}^*) \prec (H^*, \mathcal{N}^*)$.

Hence $h(\alpha) = \alpha$ for all $\alpha \in \mathbf{Q}_H^*$, so in this case the isomorphism h is actually the identity.

As a corollary to the previous proof we get

THEOREM 4.5. *$(\mathbf{Q}_H, \mathcal{N})$ has no proper elementary extensions in which $\mathcal{N}$ is fixed.*

Proof. The sentence $(x)T(x)$ holds in $(\mathbf{Q}_H, \mathcal{N})$ but it could not possibly hold in any extension of the form $(\mathbf{Q}_H', \mathcal{N})$ with $\mathbf{Q}_H \subsetneq \mathbf{Q}_H'$ since $\mathbf{Q}_H'$ must contain transcendental elements.

5. Generalization. As we remarked earlier, the existence result holds for every arithmetically definable valued subfield of $\mathbf{Q}_p$, namely, if H is an A.D. p-valued subfield of $\mathbf{Q}_p$ and $\mathcal{N}^*$ is an arbitrary strong non-standard model of arithmetic, there exists a p-valued field H^* such that the pairs $(H, \mathcal{N})$ and $(H^*, \mathcal{N}^*)$ are elementarily equivalent.

Our next aim is to extend the uniqueness result to all A.D. p-valued subfields of $\mathbf{Q}_p$. In order to do this we will make use of the following

LEMMA 5.1. *Let $\alpha_1, \alpha_2 \in \mathbf{Q}_p$. Assume that for all $r \in \mathbf{Q}$, $v(r + \alpha_1) = v(r + \alpha_2)$. Then $\alpha_1 = \alpha_2$.*

Proof. Notice that, taking $r = 0$, we get $v(\alpha_1) = v(\alpha_2)$. Suppose $\alpha_1 \neq \alpha_2$; say

$$\alpha_1 = r_1 + \sum_{n=i}^{\infty} a_n p^n, \quad \alpha_2 = r_1 + \sum_{n=i}^{\infty} b_n p^n$$

where i is the first exponent such that $a_i \neq b_i$. Let $r = -r_1 - a_i p^i$. Then $r + \alpha_1 = \sum_{n=i+1}^{\infty} a_i p^i$ and thus $v(r + \alpha_1) = i + 1$. Now

$$r + \alpha_2 = (b_i - a_i)p^i + \sum_{n=i+1}^{\infty} b_n p^n.$$

Since $b_i - a_i \neq 0$ we have $v(r + \alpha_2) = i \neq i + 1$, contradiction. Thus $\alpha_1 = \alpha_2$.

This lemma will play a similar role to Lemma 4.3 in our uniqueness proof.

LEMMA 5.2. *Let H be an A.D. p-valued subfield of $\mathbf{Q}_p$; let $\varphi: H \to \mathcal{N}$ be an admissible indexing and let $\mathbf{Q}$ be the field of quotients of $\mathcal{N}$. Then $\varphi|\mathbf{Q}$ and $\varphi|\mathbf{Z}$ are expressible in the language of $(H, \mathcal{N})$, i.e. a formulation of the LPC containing all necessary extralogical constants.*

Proof. Recall that the predicates $N'(x)$, $I(x)$ and $R(x)$ define (respectively) the natural numbers, the integers and the rationals arithmetically. Notice that $\varphi|\mathcal{N}$ is expressible in the language of $(H, \mathcal{N})$ since $\varphi(a) = b$ if and only if $\mathcal{N}(a)$ & $N'(b)$ & $B(a, b)$ holds in $(H, \mathcal{N})$. Similarly, we get that $\varphi|\mathbf{Q}$ is expressible in the language of $(H, \mathcal{N})$, using the predicate $\bar{B}(x, y)$. As for the value group $\mathbf{Z} = v(\mathbf{Q}^0)$, $\varphi(a) = b$ if and only if

$$G(a) \;\&\; \exists z \exists z' [\mathbf{Q}(z) \;\&\; V(z, a) \;\&\; \varphi(z) = z' \;\&\; V'(z', b)]$$

holds in $(H, \mathcal{N})$.

THEOREM 5.3. *Let H be an A.D. p-valued subfield of $\mathbf{Q}_p$. Then there exists a 1-1 function $\psi: H \cup \mathbf{Z} \to \mathcal{N}$ such that the predicate $\psi(x) = y$ is expressible in the language of $(H, \mathcal{N})$.*

Proof. Let $\varphi: H \cup \mathbf{Z} \to \mathcal{N}$ be an admissible indexing for the valued field H. Define $\psi: H \cup \mathbf{Z} \to \mathcal{N}$ as follows:

$$\begin{aligned}
&\text{if } x \in \mathbf{Z} = v(\mathbf{Q}^0),\ \psi(x) = \varphi(x)\\
&\text{if } x \in H,\ \psi(x) = y \text{ if and only if } [x = 0 \;\&\; y = 0'] \vee [x \neq 0 \;\&\; F(x) \;\&\;\\
&\qquad y \in \varphi[H] \;\&\; (r)[r \in \mathbf{Q} \Rightarrow \exists m (G(m) \;\&\; v(r + x) = m \;\&\;\\
&\qquad v'(\varphi(r) +' y) = \varphi(m))]
\end{aligned}$$

holds in $(H, \mathcal{N})$, where v', $+'$ are the arithmetical functions induced by the predicates $V'(x, y)$ and $S'(x, y, z)$. The fact that φ is an admissible indexing for the arithmetical definability of H, together with Lemma 5.2 ensure that $\psi(x) = y$ is expressible in the language of $(H, \mathcal{N})$, To show that ψ is 1-1, use Lemma 5.1 together with the fact that ψ is 1-1 on $\mathbf{Q}$ and on $\mathbf{Z} = v(\mathbf{Q}^0)$.

Let $\psi: H \cup \mathbf{Z} \to \mathcal{N}$ be as in the previous theorem. Define $\chi: \mathcal{N} \to H \cup \mathbf{Z}$ by

$$\chi(n) = \begin{cases} x, \text{ if } \psi(x) = n \\ 0, \text{ otherwise.} \end{cases}$$

Then clearly $\chi(x) = y$ is expressible in the language of $(H, \mathcal{N})$, say by the predicate $A(x, y)$.

It is easy to see that the following hold in $(H, \mathcal{N})$:

(i) $(x)(y)(z)[A(x, y) \;\&\; A(x, z) \Rightarrow y = z]$
(ii) $(x)[\mathcal{N}(x) \Rightarrow \exists\, !y A(x, y)]$
(iii) $(y)(\exists x)[\mathcal{N}(x) \;\&\; A(x, y)]$
(iv) $(y)[y \neq 0 \Rightarrow \exists\, !x A(x, y)]$.

We can now prove the uniqueness result

https://doi.org/10.4153/CJM-1974-046-0 Published online by Cambridge University Press

THEOREM 5.4. *Let H be an A.D. p-valued subfield of $\mathbf{Q}_p$, let $\mathcal{N}^*$ be any strong non-standard model of arithmetic, Assume H^*, H^{**} are two p-valued fields containing $\mathcal{N}^*$ such that*

$$(H,\mathcal{N}) \equiv (H^*,\mathcal{N}^*) \underset{\mathcal{N}^*}{\equiv} (H^{**},\mathcal{N}^*).$$

Then H^* and H^{**} are isomorphic.

Proof. Notice that elementary equivalence with respect to $\mathcal{N}^*$ implies elementary equivalence with respect to $\mathbf{Q}^*$ and $\mathbf{Z}^* = v(\mathbf{Q}^{*0})$. Since H is an A.D. p-valued subfield of $\mathbf{Q}_p$, there exists a map $\chi:\mathcal{N} \to H \cup \mathbf{Z}$ such that $\chi(x) = y$ is expressible in the language of $(H, \mathcal{N})$, say by the predicate $A(x, y)$ and, furthermore, $A(x, y)$ satisfies (i) to (iv) above. The proof now proceeds in essentially the same way as the proof of Theorem 4.4.

We can also show that the analogue of Theorem 4.5 holds for any A.D. p-valued subfield of $\mathbf{Q}_p$, namely

THEOREM 5.5. *Let H be any A.D. p-valued subfield of $\mathbf{Q}_p$. Then $(H,\mathcal{N})$ has no proper elementary extensions in which $\mathcal{N}$ is fixed.*

Proof. Assume $(H',\mathcal{N})$ is a proper elementary extension of $(H,\mathcal{N})$. Let $\alpha \in H' - H$. Since (iii) holds in $(H,\mathcal{N})$, it must hold in $(H',\mathcal{N})$ by elementary equivalence. Let $n \in \mathcal{N}$ be such that $A(n, \alpha)$ holds in $(H',\mathcal{N})$.

Since (ii) holds in $(H,\mathcal{N})$, there exists $\beta \in H$ such that $A(n, \beta)$ holds in $(H,\mathcal{N})$. But by assumption $(H,\mathcal{N}) \prec (H',\mathcal{N})$, thus $A(n, \alpha)$ & $A(n, \beta)$ holds in $(H',\mathcal{N})$. Hence, by (ii), $\alpha = \beta$ holds in $(H',\mathcal{N})$ which is impossible since $\alpha \in H'$-H, $\beta \in H$. Thus no such elementary extension exists.

To use the terminology of E.W. Madison we have shown that all A.D. p-valued subfields of $\mathbf{Q}_p$ are elementarily closed relative to $\mathcal{N}$. He has obtained similar results for the real numbers in his paper "Structures elementarily closed relative to the natural numbers", to appear soon.

REFERENCES

1. J. Ax and S. Kochen, *Diophantine problems over local fields, I*, Amer. J. Math. *87* (1965), 605–630.
2. ——— *Diophantine problems over local fields, II*, Amer. J. Math. *87* (1965), 631–648.
3. ——— *Diophantine problems over local fields, III*, Ann. of Math. *83* (1966), 437–456.
4. P. J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. *22* (1969), 131–151.
5. Yu. L. Ershov, *Numbered fields*, Logic, Methodology and the Philosophy of Science, Proceedings of the 1967 International Congress (North-Holland Publishing Co., Amsterdam, 1968), 31–34.
6. ——— *On the elementary theory of maximal normed fields* (Russian), Dokl. Akad. Nauk. SSSR *165* (1965), 21–23; translated in Soviet Math. Dokl. *6* (1965), no. 6.
7. A. Frolich and J. C. Shepherdson, *Effective procedures in field theory*, Trans. Roy. Soc. London Ser. A*248* (1956), 407–432.

8. S. C. Kleene, *Introduction to metamathematics* (D. Van Nostrand Company, Inc., Princeton, New Jersey, 1952).
9. S. Kochen, *Integer-valued rational functions over the p-adic numbers: A p-adic analogue of the theory of real fields*, "Number Theory", Amer. Math. Soc., Proc. of Symp. in Pure Math. *12* (1969), 57–73.
10. A. H. Lachlan and E. W. Madison, *Computable fields and arithmetically definable ordered fields*, Proc. Amer. Math. Soc. *24* (1970), 803–807.
11. E. W. Madison, *Computable algebraic structures and non-standard arithmetic*, Trans. Amer. Math. Soc. *130* (1968), 38–54.
12. A. Nerode, *A decision method for p-adic integral zeros of diophantine equations*, Bull. Amer. Math. Soc. *69* (1963), 513–517.
13. M. O. Rabin, *Computable algebra*, Trans. Amer. Math. Soc. *95* (1960), 341–360.
14. P. Ribenboim, *Théorie des valuations* (University of Montreal Press, Montreal, 1964).
15. H. G. Rice, *Recursive real numbers*, Proc. Amer. Math. Soc. *5* (1954), 784–791.
16. A. Robinson, *Complete theories* (North-Holland Publishing Company, Amsterdam, 1956).
17. ——— *Introduction to model theory and to the meta-mathematics of algebra* (North-Holland Publishing Company, Amsterdam, 1963).
18. ——— *Model theory and non-standard arithmetic*, Infinitistic Methods (Symposium on Foundations of Mathematics), Warsaw, 1959.
19. H. Rogers, *Theory of recursive functions and effective computability* (McGraw-Hill Book Company, New York, 1967).
20. B. L. van der Waerden, *Modern algebra*, revised English edition (Frederick Unger Publishing Co., New York, 1953).

Université de Montréal,
Montréal, Québec