AN ALMOST EVERYWHERE DIRECT POWER

BY

PHILIP OLIN[1]

0. Introduction and notation. Almost everywhere direct products were first introduced by Chang and Morel [1], and were discussed (and named) by Feferman and Vaught [2]. These products are reduced direct products (see [3]) in which the filter to be factored out is the filter of cofinite subsets of the index set. Alternatively, it can be obtained from the direct product by identifying any two members which differ at only a finite number of places, and defining the relations to hold if they do so "almost everywhere" among the factors.

Theorem 1.3 below was obtained independently by Bjarni Jónsson and the author. In one form it states that, assuming the continuum hypothesis, a countable almost everywhere direct product of models of the same countable similarity type and each of cardinality $\leq \aleph_1$ is saturated. A detailed proof of this theorem will appear in [15] and so we give only some indication of the method. The continuum hypothesis is used only to show that the cardinality of the product is $\leq \aleph_1$.

One almost everywhere direct power is of particular interest. Named Q, it is defined as follows: let E^* denote the integers and D the filter of cofinite subsets of ω; then $Q = E^{*\omega}/D$. Q was defined by Nerode in [9], where he obtained results connecting Q and the theory of isols. Other such results are obtained in §§1 and 3 below.

If $[x]$ is in Q, we say $[x]$ is indecomposable if, for every arithmetic formula $\phi(v)$ of one free variable, either $[i|\phi(x_i)]$ or $[i| \sim \phi(x_i)]$ is finite. An indecomposable subring of Q is a subring consisting entirely of indecomposable elements. The main results of this paper (aside from Theorem 1.3) are that every maximal indecomposable subring of Q is a nonstandard model of arithmetic (Corollary 2.9) and that every nonstandard model of arithmetic of power $\leq \aleph_1$ is embeddable in Q as an indecomposable subring (Theorem 2.11).

A ring A is said to be diophantine correct (cf. Nerode [10]) if every finite conjunction of formulas of the form $x+y=z$, $x \cdot y=z$ or $x \neq y$ which has a solution in A has a solution in the integers. If we restrict the condition to conjunctions involving at most one formula of the form $x \neq y$, A is said to be weakly diophantine correct. In Proposition 3.3 below it is shown that the subrings of Q of power $\leq \aleph_1$ are

---

exactly the weakly diophantine correct rings of power $\leqq \aleph_1$. In Proposition 3.11 the same result is obtained for indecomposable subrings of Q and diophantine correct rings.

Many of the results of this paper were announced in [11] and [12].

Frequently in what follows we shall be assuming the continuum hypothesis (C.H.) which states that $2^{\aleph_0} = \aleph_1$.

Let J be an arbitrary set and $t \in \omega^J$. A system $\mathfrak{A} = \langle A, R_j \rangle_{j \in J}$, formed by a nonempty set A and t_j-ary relations R_j among the elements of A, is a relational system having similarity type $t = t^{\mathfrak{A}}$, index set J, universe $A = |\mathfrak{A}|$, jth relation R_j (for $j \in J$). We will also consider more general systems $\mathfrak{A}' = \langle A, R_j, d_k \rangle_{j \in J, k \in K}$ where $\mathfrak{A} = \langle A, R_j \rangle_{j \in J}$ and $d_k \in A$.

Corresponding to t above is a first order language L_t with symbols $\sim$, $\wedge$, $\vee$, E, $=$, individual variables $v_0, v_1, v_2, \ldots$, t_j-placed relation symbols P_j for $j \in J$, and individual constants c_k for $k \in K$.

The theory of $\mathfrak{A}$, Th $(\mathfrak{A})$, is the set of all sentences θ which are true in $\mathfrak{A}$. If Th $(\mathfrak{A}) =$ Th $(\mathfrak{A}')$, we say $\mathfrak{A}$ and $\mathfrak{A}'$ are elementarily equivalent, written $\mathfrak{A} \equiv \mathfrak{A}'$. The elementary type of a relational system $\mathfrak{A}$ is the class of all $\mathfrak{B}$ such that Th $(\mathfrak{B}) =$ Th $(\mathfrak{A})$.

We shall use the usual set operations and relations: $\cup$, $\cap$, $-$, $\subseteq$. The empty set will be denoted by $\varnothing$, the set of integers by E^*, and the nonnegative integers by either E or ω. For a set A, $\mathscr{P}(A)$ denotes the power set of A and $\mathscr{P}_{\text{fin}}(A)$ the set of finite subsets of A. D is a filter over A if D is a collection of subsets of A; $\varnothing \notin D$; $x \in D$ and $x \subseteq y$ implies $y \in D$; and D is closed under intersection.

Finally, the phrases "almost everywhere" and "almost all" in the sequel shall always mean "except for a finite number".

1. Q.

DEFINITION 1.1. Let $\{\mathfrak{A}_i\}_{i \in I}$ be a class of similar relational systems, I infinite, D the filter of cofinite subsets of I. We define the almost everywhere direct product of the $\mathfrak{A}_i$'s (see Feferman and Vaught [3]), written $\mathfrak{B} = \prod_{i \in I} \mathfrak{A}_i / D$. First we form the direct product P of the $|\mathfrak{A}_i|$'s;

$$P = \left\{ g \,\middle|\, g : I \to \bigcup_{i \in I} |\mathfrak{A}_i|, \, g(i) \in |\mathfrak{A}_i| \text{ for all } i \in I \right\}.$$

We then form equivalence classes $[g]$ of members of P by setting g_1 equivalent to g_2 if $\{i \,|\, g_1(i) = g_2(i)\} \in D$. Then $|\mathfrak{B}|$ is the set of equivalence classes which we get in this way. Suppose j is fixed, R_i is the jth relation in $\mathfrak{A}_i$, and R_i is an n-ary relation. Define an n-ary relation R over $|\mathfrak{B}|$ as follows:

$$R([g_1], \ldots, [g_n]) \quad \text{iff} \quad \{i \,|\, R_i(g_1(i), \ldots, g_n(i))\} \in D.$$

This defines a relational system $\mathfrak{B}$ of the same type as the $\mathfrak{A}_i$'s. If $\mathfrak{A}_i = \mathfrak{A}$ for all i, we say $\mathfrak{B}$ is an almost everywhere direct power.

Theorem 1.3 below was obtained independently by Bjarni Jónsson and the author, using essentially the same proof. Since the proof will be published in [15] in detail, we give here only some indication of the method.

DEFINITION 1.2. Say the cardinality of $\mathfrak{A} = \kappa$. We say $\mathfrak{A}$ is saturated if the following condition holds: whenever $X \subseteq |\mathfrak{A}|$, the cardinality of $X < \kappa$, $\mathfrak{B} = (\mathfrak{A}, x)_{x \in X}$, and Σ is a set of formulas of $L_t \mathfrak{B}$ each having only v_0 free, if every finite subset of Σ is satisfiable in $\mathfrak{B}$ then so is Σ.

THEOREM 1.3 (C.H.). *Let $\{\mathfrak{A}_i\}_{i \in \omega}$ be a collection of relational systems with the same countable similarity type and such that the cardinality of $\mathfrak{A}_i \leq \aleph_1$. Let D be the filter of cofinite subsets of ω. Then the almost everywhere direct product $\mathfrak{B} = \prod_{i \in \omega} \mathfrak{A}_i / D$ is saturated.*

In order to simplify the saturation condition, we apply successively Theorem 3.1 of Feferman and Vaught [2], an elimination of quantifiers technique due to Skolem (see Theorem 6.1 of [2]), and König's infinity lemma. Finally we make a construction similar to the "cut-and-paste" construction used in Lemma 2.13 below.

In [6] Keisler discussed $\mathscr{P}(E)/\mathscr{P}_{\mathrm{fin}}(E)$ as a Boolean algebra and showed that, assuming the C.H., it is the universal homogeneous Boolean algebra of power $\aleph_1$ (see [7]). Since this Boolean algebra is the countable almost everywhere direct power of the two-element Boolean algebra, by Theorem 1.3 it is saturated.

We now wish to consider a particular almost everywhere direct power, Q. This is defined in Nerode [9]. Let E^* denote the set of integers (positive, negative or zero). Let D be the filter of cofinite subsets of ω. Then $Q = E^{*\omega}/D$. That is, Q consists of equivalence classes of countably infinite sequences of integers, where we identify two such sequences if they differ at only a finite number of places. The ring operations in Q are pointwise and well defined. The 'zero' and 'one' of Q are obvious. So Q is a ring with unit. Notice that if we take $x, y \in E^{*\omega}$; $x = (x_0, x_1, x_2, \ldots)$, $y = (y_0, y_1, y_2, \ldots)$, $[x]$, $[y]$ the corresponding equivalence classes in Q; then $[x] = [y] \Rightarrow x_i = y_i$ for almost all $i \in \omega$, and $[x] \neq [y] \Rightarrow x_i \neq y_i$ for an infinite number of $i \in \omega$. Notice also that the cardinality of $Q = 2^{\aleph_0}$.

As a particular case of Theorem 1.3, assuming the C.H. (so that the cardinality of $Q = \aleph_1$), we have that Q is saturated.

REMARK 1.4 (C.H.). In [9], Nerode introduced the notion of arithmetic isolic integer, and called the ring of arithmetic isolic integers $\Lambda^*(A)$. He showed that $Q \equiv \Lambda^*(A)$. By the C.H., both have power $\aleph_1$. Since Q is saturated (homogeneous-universal) it follows from Theorem 3.5 of Morley and Vaught [7] that $Q \cong \Lambda^*(A)$ iff $\Lambda^*(A)$ is saturated.

DEFINITION 1.5 (JÓNSSON [4]). Let M be a class of similar relational systems and $\mathfrak{A} \in M$. Say the cardinality of $|\mathfrak{A}| = \kappa$. We say $\mathfrak{A}$ is M-universal if every $\mathfrak{B} \in M$ such that the cardinality of $|\mathfrak{B}| \leq \kappa$ is isomorphic to a subsystem of $\mathfrak{A}$.

The next proposition is a special case of a (well-known) more general result.

PROPOSITION 1.6 (C.H.). *Since Q is saturated, it is N-universal, where N is the elementary type of Q.*

Nerode introduced the isolic integers Λ^* in [8] and the arithmetic isolic integers $\Lambda^*(A)$ in [9].

PROPOSITION 1.7 (C.H.). *Λ^* and $\Lambda^*(A)$ can each be embedded as a subring of Q.*

Proof. (i) By the C.H., the cardinality of $Q = \Lambda^*(A) = \aleph_1$. We know Q is universal for its type. As remarked above, $Q \equiv \Lambda^*(A)$. Hence $\Lambda^*(A)$ can be embedded as a subring of Q.

(ii) Let T_Q denote the set of first order statements which hold in Q. Let $\Lambda^* = \{\lambda_i\}_{i \in I}$. Let

$$S = \{x_j \neq x_k \mid j, k \in I \text{ and } \lambda_j \neq \lambda_k\}$$
$$\cup \{x_j + x_k = x_l \mid j, k, l \in I \text{ and } \lambda_j + \lambda_k = \lambda_l\}$$
$$\cup \{x_j \cdot x_k = x_l \mid j, k, l \in I \text{ and } \lambda_j \cdot \lambda_k = \lambda_l\}.$$

Claim that $S \cup T_Q$ is consistent. Let ϕ be any finite conjunction of members of S. It suffices for the claim to show that ϕ is satisfiable in Q. Suppose ϕ has the form $\psi \wedge a_1 \wedge a_2 \wedge \cdots \wedge a_n$ where ψ is the conjunction of the positive equations in ϕ and the a_i's are the inequations (of the form $x_j \neq x_k$). Let $\phi_i = \psi \wedge a_i$, for $i = 1$ to n. Of course ϕ_i has a solution in Λ^*. So by Theorem 2.1 of Nerode [8], ϕ_i also has a solution in E^*. If some x_j appears in ϕ but not in ϕ_i, give it value $0 \in E^*$. Call this assignment of values to the variables appearing in ϕ α_i. Repeat for each i, $i = 1$ to n. Now for each variable x_m appearing in ϕ, define $r^m = (r_0^m, r_1^m, r_2^m, \ldots) \in E^{*\omega}$ by: $r_{(j-1)+kn}^m =$ the value assigned to x_m in α_j, for $j = 1$ to n and for $k = 0, 1, 2, \ldots$. If we now replace each x_m in ϕ by $[r^m]$, ϕ is satisfied in Q since each positive equation in ϕ is satisfied at every coordinate (using the r^m's) and each negative one is satisfied infinitely often.

So the claim is proven and $S \cup T_Q$ is consistent and so has a model by the Completeness Theorem. But by the C.H. and the downward Skolem-Löwenheim theorem (see Tarski and Vaught [14]), $S \cup T_Q$ has a model of power $\aleph_1$, call it $\mathfrak{A}$. So Λ^* is embedded in $\mathfrak{A}$. But $\mathfrak{A} \equiv Q$ and Q is universal for its type. Hence $\mathfrak{A}$ can be embedded in Q and thus so can Λ^*.

2. **Nonstandard models of arithmetic in Q.** We wish to introduce the notion of an indecomposable sequence x in $E^{*\omega}$, and consequently an indecomposable $[x] \in Q$.

We say ϕ is a formula of arithmetic if ϕ is a first-order formula involving the relations $+$, $\cdot$, $=$ and the constants 0 and 1. If $\phi(v)$ is an arithmetic formula of one free variable, then the arithmetic set A_ϕ is $\{p \mid p \in E^* \text{ and } \phi(p) \text{ is a true statement of arithmetic}\}$.

DEFINITION 2.1. Say $x = (x_0, x_1, x_2, \ldots) \in E^{*\omega}$. We say x is an indecomposable sequence if, for every arithmetic formula $\phi(v)$ of one free variable, either $\{i \mid \phi(x_i)$ is true$\}$ or $\{i \mid \sim\phi(x_i)$ is true$\}$ is finite. Clearly the definition extends (is well defined) to $[x] \in Q$.

We say $\phi(v)$ splits x (or $[x]$) if ϕ is a witness to the fact that x is *not* indecomposable.

Let $\psi_0, \psi_1, \psi_2, \ldots$ be a list of all arithmetic formulas of one free variable. The list is clearly countable. One of A_{ψ_0} and $A_{\sim\psi_0}$ is infinite, say A_{ψ_0}. Choose $x_0 \in A_{\psi_0}$. One of $A_{\psi_0} \cap A_{\psi_1}$ and $A_{\psi_0} \cap A_{\sim\psi_1}$ is infinite, say the latter. Choose $x_1 \in A_{\psi_0} \cap A_{\sim\psi_1}$, $x_1 \neq x_0$. One of $A_{\psi_0} \cap A_{\sim\psi_1} \cap A_{\psi_2}$ and $A_{\psi_0} \cap A_{\sim\psi_1} \cap A_{\sim\psi_2}$ is infinite, say the former. Choose $x_2 \in A_{\psi_0} \cap A_{\sim\psi_1} \cap A_{\psi_2}$, $x_2 \neq x_1$, $x_2 \neq x_0$. Repeat ad infinitum. Let $x = (x_0, x_1, x_2, \ldots)$. Clearly x is indecomposable; for if $\phi(v)$ splits x, then ϕ is ψ_i for some i and hence if we assume (without loss of generality) that in the process described above $A_{\sim\psi_i}$ was used, then $\{j \mid \psi_i(x_j)\}$ is finite (alternatively $\{j \mid \sim\psi_i(x_j)\}$ is finite), i.e. $\{j \mid \phi(x_j)\}$ is finite, and hence ϕ could not split x. In this way we can construct $2^{\aleph_0}$ such $[x]$'s which are indecomposable.

In particular, suppose A_{ψ_0} is the set of nonnegative primes and we choose to begin the process with it. As described we get $x = (x_0, x_1, x_2, \ldots)$ with the x_i's distinct and positive primes. Let

$$y = (x_0, x_0, x_2, x_2, x_4, x_4, x_6, x_6, \ldots) = (y_0, y_1, y_2, \ldots).$$

Since x is indecomposable, y is too. Let

$$w = x \cdot y = (x_0^2, x_1 x_0, x_2^2, x_3 x_2, x_4^2, x_5 x_4, \ldots) = (w_0, w_1, w_2, \ldots).$$

Now w is *not* indecomposable since w_n, for n even, is a square, and w_n, for n odd, is not a square (product of two unequal positive primes cannot be a square); thus w can be split by the formula $(Ex)(v = x^2)$. We have thus found two indecomposable members of Q, $[x]$ and $[y]$, whose product in Q is not indecomposable.

Now let $z = -y = (-x_0, -x_0, -x_2, -x_2, -x_4, -x_4, \ldots) = (z_0, z_1, z_2, \ldots)$. Let $t = x + z = (0, x_1 - x_0, 0, x_3 - x_2, 0, x_5 - x_4, \ldots) = (t_0, t_1, t_2, \ldots)$. But t is not indecomposable since t_n is 0 for n even and is not 0 (we choose $x_i \neq x_j$ for $i \neq j$) for n odd; thus the formula $v = 0$ splits t. So we have found two indecomposable members of Q, $[x]$ and $[z]$ (z is indecomposable since y was), whose sum in Q is not indecomposable.

DEFINITION 2.2. R is an indecomposable subring of Q if R is a subring of Q all of whose members are indecomposable. R' is a maximal indecomposable subring of Q if R' is an indecomposable subring of Q and is contained in no other such subring.

For $n \in E^*$, $(n, n, n, \ldots)$ is clearly indecomposable. Thus E^* is "contained" in Q as an indecomposable subring, and we shall henceforth simply write $n \in Q$.

If $[z] \in Q$, then by $E^*([z])$ we mean the subring of Q generated by E^* and $[z]$.

PROPOSITION 2.3. *If* $[z]$ *is indecomposable, then* $E^*([z])$ *is an indecomposable subring of* Q.

Proof. Take any $[x] \in E^*([z])$. We must show that $[x]$ is indecomposable. But $[x] = p([z])$, where p is a polynomial with coefficients in E^*. That is, $x = p(z)$, where the operations are pointwise (given z, we can actually let x be $p(z)$). Suppose $\phi(v)$ splits $x = p(z)$. Then $\psi(v) = (Ey)[\phi(y) \wedge p(v) = y]$ will split z, which is a contradiction.

COROLLARY 2.4. *Maximal indecomposable subrings* R' *of* Q *do exist.*

Proof. Apply Zorn's Lemma.

Of course, for every R', $E^* \subseteq R'$.

There is a well-known recursive function $j: E \times E \to E$, which is one-one and onto, defined by $j(x, y) = (x + y)(x + y + 1)/2 + x$. Using this function we define $J: E^* \times E^* \to E^*$, a one-one recursive function (but not onto) as follows:

$$
\begin{aligned}
J(x, y) &= 2j(x, y) && \text{if } x \geqq 0 \text{ and } y \geqq 0, \\
&= -2j(-x, -y) && \text{if } x \leqq 0 \text{ and } y \leqq 0, \\
&= 2j(x, -y) + 1 && \text{if } x > 0 \text{ and } y < 0, \\
&= -[2j(-x, y) + 1] && \text{if } x < 0 \text{ and } y > 0.
\end{aligned}
$$

Define (abusing notation) $J: E^* \times E^* \times E^* \to E^*$, again one-one recursive and not onto, by $J(x, y, z) = J(J(x, y), z)$. Repeating, by induction we define $J: E^{*n} \to E^*$, one-one recursive for all n.

If $[x]$, $[y] \in Q$ define $J([x], [y])$ (pointwise) to be $[z] \in Q$ where $z_i = J(x_i, y_i)$ for all i. A similar definition defines $J: Q^n \to Q$ for all n.

Further, if J has n arguments, we can define in the usual way recursive functions $K_1, \ldots, K_n$ of one argument with the property that $J(K_1(v), \ldots, K_n(v)) = v$.

LEMMA 2.5. *If* R' *is a maximal indecomposable subring of* Q, *then* R' *is closed under* J.

Proof. We shall show that if $[x]$, $[y] \in R'$, then $J([x], [y]) \in R'$. The proof for three or more arguments follows at once from the definition of J.

Now $[x] \in R'$ implies x indecomposable, of course. So we must have (i) $x_i > 0$ for almost all i, (ii) $x_i < 0$ for almost all i, or (iii) $x_i = 0$ for almost all i; else one of these formulas could be used to split x. Similarly for y. Assume, without loss of generality, that $x_i > 0$ and $y_i < 0$ for almost all i. So in this case $J([x], [y]) = 2j([x], -[y]) + 1$. Thus it suffices to show $j([x], -[y]) \in R'$. Now $j([x], -[y]) = j([x], [-y]) = (j(x_0, -y_0), j(x_1, -y_1), j(x_2, -y_2), \ldots)$. At once, $([x] + [-y])([x] + [-y] + 1) \in R'$. Call it $[z]$. Claim $[z]/2 = [(z_0/2, z_1/2, z_2/2, \ldots)] \in R'$. Let $[z]/2 = [w]$ $(w_i = z_i/2)$ and suppose $[w] \notin R'$. Let M be the subring of Q generated by R' and $[w]$. Take $[b] \in M$; $[b]$ has the form $[a_n][w]^n + \cdots + [a_0] = [a_n w^n + \cdots + a_0]$, where $[a_j] \in R'$ for $j = 0$ to n. If b is not indecomposable, suppose $\phi(v)$ splits it. Now

$$[2^n b] = [a_n (2w)^n + a_{n-1} \cdot 2 \cdot (2w)^{n-1} + a_{n-2} \cdot 2^2 \cdot (2w)^{n-2} + \cdots + 2^n a_0].$$

(Of course, we are operating pointwise on these sequences.) So

$$[2^n b] = [a_n z^n + 2a_{n-1} z^{n-1} + 2^2 a_{n-2} z^{n-2} + \cdots + 2^n a_0] \in R'.$$

So $2^n b$ is an indecomposable sequence. But the formula $\psi(v) = (Eu)[2^n \cdot u = v \wedge \phi(u)]$ splits $2^n b$, which is a contradiction. Thus b is indecomposable, and so M is an indecomposable subring of Q properly containing R', again a contradiction. So $[z]/2 = [w] \in R'$. That is,

$$([x] + [-y])([x] + [-y] + 1)/2 \in R'.$$

Consequently

$$j([x], [-y]) = ([x] + [-y])([x] + [-y] + 1)/2 + [x] \in R'.$$

Clearly the procedure just described could be repeated if we were considering a case other than $x_i > 0$ and $y_i < 0$ for almost all i. The lemma is proved.

LEMMA 2.6. *Suppose* $f(v_0, \ldots, v_n)$ *is an arithmetic function of* $n+1$ *free variables; and* $[a^0], [a^1], \ldots, [a^n] \in R'$, *a maximal indecomposable subring of* Q. *Then if* $[b] = f([a^0], \ldots, [a^n]) = [f(a^0, \ldots, a^n)]$ *is the result of applying* f *to the* a^i's *pointwise, then* $[b] \in R'$.

Proof. Suppose $[b] \notin R'$ and let M be the subring of Q generated by R' and $[b]$. If $[c] \in M$, then $[c] = p([b])$ where p is a polynomial in one variable with coefficients in R'. So $[c] = [g(b, d^0, \ldots, d^m)]$ where $[d^i] \in R'$ for $i = 0$ to m and g is an arithmetic function. But $[b] = [f(a^0, \ldots, a^n)]$. Thus $[c] = [g(f(a^0, \ldots, a^n), d^0, \ldots d^m)]$ with $[a^i]$ and $[d^i] \in R'$ and f and g arithmetic functions. Claim c is indecomposable. If $\phi(v)$ splits c, define $\psi(v_0, \ldots, v_n, v_0', \ldots, v_m') = \phi(g(f(v_0, \ldots, v_n), v_0', \ldots, v_m'))$. Since $[a^0], \ldots, [a^n], [d^0], \ldots, [d^m] \in R'$, $[e] = [J(a^0, \ldots, a^n, d^0, \ldots, d^m)] \in R'$ by Lemma 2.5. But $\theta(v) = \psi(K_1(v), \ldots, K_{m+n+2}(v))$ is an arithmetic formula, since ϕ, K_i, g, f are all arithmetic. Moreover, θ clearly splits e, which is a contradiction. So c is indecomposable and M is an indecomposable subring of Q properly containing R'. This is another contradiction. Hence $[b] \in R'$.

The next theorem is one of the main results of this section. We assume E^* is well-ordered in such a way that if $\phi(v)$ is an arithmetic formula of one free variable and $(Ev)\phi(v)$ is true in E^*, then the least v such that $\phi(v)$, i.e. $\mu v \phi(v)$, is an arithmetic function.

THEOREM 2.7. *Suppose* R' *is a maximal indecomposable subring of* Q, $\phi(v_0, \ldots, v_n)$ *is an arithmetic formula of* $n+1$ *free variables, and* $[a^0], \ldots, [a^n] \in R'$. *Further, assume* $\phi(a_i^0, \ldots, a_i^n)$ *is true in* E^* *for almost all* i. *Then* $\phi([a^0], \ldots, [a^n])$ *is true in* R'.

Proof. Writing ϕ in prenex disjunctive normal form, we can assume the first block of quantifiers is universal. (Otherwise we just tack on at the beginning a superfluous universal quantifier.) We write ϕ as

$$(z_1) \cdots (z_q)(Ey_1) \cdots (Ey_m)(w_1) \cdots (w_p)(Eu_1) \cdots (Eu_t) \cdots [\vee \wedge T]$$

where T is of the form (or the negation of the form) $\alpha + \beta = \gamma$, $\alpha \cdot \beta = \gamma$, or $\alpha = \beta$ where α, β, and γ may be variables or the constants $[a^0], \ldots, [a^n]$. Usually we will omit from the notation the variables and constants of which T is a function. In the formula above we should write

$$T(z_1, \ldots, z_q, y_1, \ldots, y_m, w_1, \ldots, w_p, u_1, \ldots, u_t, \ldots, [a^0], \ldots, [a^n]).$$

This notation will be used only when changes in the T's are made.

Suppose we are given $[b^1], \ldots, [b^q] \in R'$. Let i be a fixed coordinate. Let c_i^1 be the least member of E^* such that

$$(Ey_2) \cdots (Ey_m)(w_2) \cdots [\vee \wedge T(b_i^1, \ldots, b_i^q, c_i^1, y_2, \ldots, y_m, \ldots, a_i^0, \ldots, a_i^n)].$$

Notice that we are using the ith coordinates of the a^j's and the b^j's. Now let c_i^2 be the least member of E^* such that

$$(Ey_3) \cdots (Ey_m)(w_1) \cdots [\vee \wedge T(b_i^1, \ldots, b_i^q, c_i^1, c_i^2, y_3, \ldots, y_m, \ldots, a_i^0, \ldots, a_i^n)]$$

and we again use the ith coordinates of the given sequences. Repeat this and get $c_i^1, \ldots, c_i^m$. Now suppose we are given $[d^1], \ldots, [d^p] \in R'$. Let e_i^1 be the least such that

$$(Eu_2) \cdots [\vee \wedge T(b_i^1, \ldots, b_i^q, c_i^1, \ldots, c_i^m, d_i^1, \ldots, d_i^p, e_i^1, u_2, \ldots, a_i^0, \ldots, a_i^n)].$$

Repeat in this way through all the variables of ϕ. So given $[b^1], \ldots, [b^q], [d^1], \ldots, [d^p], \ldots \in R'$, we define $[c^1], \ldots, [c^m], [e^1], \ldots, [e^t], \ldots \in Q$ in this way. Claim $\vee \wedge T([b^1], \ldots, [c^1], \ldots, [d^1], \ldots, [e^1], \ldots, [a^0], \ldots)$. Suppose there is a disjunct $\wedge T$ such that at an infinite number of coordinates (using the values from $b^1, \ldots, c^1, \ldots,$ etc.), $\wedge T$ is true in E^*; and at an infinite number of coordinates, $\wedge T$ is false in E^*. Define

$$\psi(z_1, \ldots, z_q, w_1, \ldots, w_p, \ldots) = (Ey_1) \cdots (Ey_m)(Eu_1) \cdots (Eu_t) \cdots$$

$\{y_1$ is the least such that $(Ey_2') \cdots (Ey_m')(w_1') \cdots (w_p')(Eu_1') \cdots (Eu_t') \cdot [\vee \wedge T]$

$\wedge y_2$ is the least such that $(Ey_3') \cdots (Ey_m')(w_1') \cdots (w_p')(Eu_1') \cdots (Eu_t') \cdot [\vee \wedge T(\cdots y_1 \cdots)]$

$\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad \vdots$

$\wedge y_m$ is the least such that $\qquad\qquad (w_1') \cdots (w_p')(Eu_1') \cdots (Eu_t') \cdot [\vee \wedge T(\cdot y_1 \cdot \cdot y_m \cdot)]$

$\wedge u_1$ is the least such that $\qquad\qquad\qquad (Eu_2') \cdot (Eu_t') \cdot [\vee \wedge T(\cdot y_1 \cdot y_m u_1 \cdot)]$

$\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots$

etc.

$$\wedge (\wedge T)\}.$$

Now $J([b^1], \ldots, [b^q], [d^1], \ldots, [d^p], \ldots) = [\alpha] \in R'$. But $\psi(K_1(v), K_2(v), \ldots)$ splits α, a contradiction. So there must be a disjunct $\wedge T$ from $\vee \wedge T$ with the property that at *almost all* coordinates (using the values from $a^1 \cdots b^1 \cdots c^1 \cdots$ etc.), $\wedge T$ is true in E^*. Hence the claim has been proven.

Now we claim that $[c^1], \ldots, [c^m], [e^1], \ldots, [e^t], \ldots \in R'$. $\mu y_1 (Ey_2) \cdots (Ey_m)(w_1) \cdots (w_p)(Eu_1) \cdots (Eu_t) \cdots [\vee \wedge T(x_1 \cdots z_1 \cdots)]$ is an arithmetic function with free

variables $x_1, \ldots, z_1, \ldots$. We obtained $[c^1]$ from $[a^1] \cdots [b^1] \cdots$ by pointwise applications of this function. So by Lemma 2.6, $[c^1] \in R'$. In a similar way $[c^2], \ldots,$ $[c^m] \in R'$. Then again $[e^1] \in R'$ because we can use

$$\mu u_1 (E u_2) \cdots [\vee \wedge T(x_1 \cdots z_1 \cdots y_1 \cdots w_1 \cdots w_p, u_1)]$$

and apply it to $[a^1] \cdots [b^1] \cdots [c^1] \cdots [d^1] \cdots [d^p]$. Thus we have the second claim, and so $\phi([a^0], \ldots, [a^n])$ is true in R'.

COROLLARY 2.8. *Assume ϕ and $[a^0], \ldots, [a^n]$ are as in the theorem. Then $\phi([a^0], \ldots, [a^n])$ true in $R' \Leftrightarrow \phi(a_i^0, \ldots, a_i^n)$ true in E^* for almost all i.*

Proof. One direction is just the theorem. Suppose $\phi([a^0], \ldots, [a^n])$ is true in R'. If it is not the case that $\phi(a_i^0, \ldots, a_i^n)$ is true in E^* for almost all i then $\phi(a_i^0, \ldots, a_i^n)$ is false in E^* for almost all i, because otherwise $\phi(K_1(v), \ldots, K_{n+1}(v))$ would split $J([a^0], \ldots, [a^n]) \in R'$. So $\sim \phi(a_i^0, \ldots, a_i^n)$ is true in E^* for almost all i, and hence by the theorem $\sim \phi([a^0], \ldots, [a^n])$ is true in R', a contradiction.

COROLLARY 2.9. *Every maximal indecomposable subring R' of Q is a nonstandard model of the true statements of arithmetic $\langle E^*, +, \cdot, =, 0, 1 \rangle$.*

Proof. In Corollary 2.8, take $[a^0], \ldots, [a^n] \in E^* \subseteq Q$. This gives at once that R' is a proper elementary extension of E^*, and hence is a strong nonstandard model of arithmetic (see Robinson [13, p. 243]).

COROLLARY 2.10. *Assume $f(x_0, \ldots, x_n)$ is an arithmetic function and $[a^0], \ldots, [a^n] \in R'$. Then $f(a_i^0, \ldots, a_i^n) = b_i$ is true in E^* almost everywhere $\Leftrightarrow f([a^0], \ldots, [a^n]) = [b]$ is true in R'.*

Proof. The '$\Leftarrow$' follows at once by considering f as a relation and applying Corollary 2.8 ($[b] \in R'$ by assumption). Now assume that $[b] \in Q$ is gotten by pointwise applications of f to $[a^0], \ldots, [a^n]$. But then $[b] \in R'$ by Lemma 2.6. So now again, considering f as a relation, apply Corollary 2.8 and we have the '$\Rightarrow$' part.

Suppose $\mathfrak{A} = \langle A, =, +, \cdot, 0, 1 \rangle$ is a strong nonstandard model of arithmetic.

THEOREM 2.11. *If $\mathfrak{A}$ is a strong nonstandard model of arithmetic and the cardinality of $A \leq \aleph_1$, then $\mathfrak{A}$ can be embedded in Q as an indecomposable subring.*

To prove this theorem we require Lemma 2.13 below.

DEFINITION 2.12. We wish to define the notion of a primitive formula (cf. Robinson [13, p. 92]). Let $d_0, d_1, d_2, \ldots$ be constants; $x_0, x_1, x_2, \ldots$ variables. Let $\phi_0, \phi_1, \phi_2, \ldots$ be a list of all arithmetic formulas of one free variable. $T_0, T_1, T_2, \ldots$ shall denote formulas of the form $u + v = w$, $u \cdot v = w$, and $u \neq v$, where u, v, and w may be d_i's or x_i's. A primitive formula (or sentence) is a quantified conjunction of T_i's, $\phi_j(x_k)$'s, and $\phi_j(d_k)$'s with all quantifiers of the form $(E x_i)$.

LEMMA 2.13. *We assume that: D is a countable subring of $\mathfrak{A}$; $D \supseteq E^*$; f is a ring isomorphism of D into a fixed R_0', a maximal indecomposable subring of Q; and $b \in A - D$. Further assume that if $\psi(d_0, \ldots, d_n)$ is a primitive sentence with constants $d_0, \ldots, d_n \in D$ and ψ is true in $\mathfrak{A}$, then $\psi(f(d_0), \ldots, f(d_n))$ is true in R_0'. Then there is a maximal indecomposable subring R_1' of Q such that f can be extended to f', a ring isomorphism of the ring D' generated by D and $\{b\}$ into R_1', with the property that if $\psi(d_0', \ldots, d_m')$ is a primitive sentence, $d_i' \in D'$, and true in $\mathfrak{A}$, then $\psi(f'(d_0'), \ldots, f'(d_m'))$ is true in R_1'.*

Proof. Let $D = \{d_0, d_1, d_2, \ldots\}$, countable. Let $\psi_0, \psi_1, \psi_2, \ldots$ be a list (countable) of all primitive sentences which have constants out of the set $D \cup \{b\}$, with b definitely appearing in each ψ_i, and which are true in $\mathfrak{A}$. Of course each $c \in A$ has the property that for every ϕ_i, either $\phi_i(c)$ or $\sim\phi_i(c)$ is true in $\mathfrak{A}$. Notice that any finite conjunction of primitive sentences is equivalent to a primitive sentence. Now $\psi_0(b)$ is true in $\mathfrak{A}$. Thus $(Ex)\psi_0(x)$ is also true in $\mathfrak{A}$, and by assumption then, if we replace the constants d_i by the constants $f(d_i)$, $(Ex)\psi_0(x)$ is true in R_0'. So we get indecomposable sequences in $E^{*\omega}$ b^0, $x^{i,0}$, e^i (replacing respectively b, the variables x_i in ψ_0, the constants d_i in ψ_0) such that every conjunct of ψ_0 is satisfied in R_0', when these substitutions are made. Now, by Corollary 2.8, we get the existence of a coordinate p_0 such that every conjunct of ψ_0 is satisfied coordinate-wise in E^* at every coordinate $\geq p_0$, when the above substitutions are made. $\psi_0(b) \wedge \cdots \wedge \psi_n(b)$ leads to the sentence $(Ex)[\psi_0(x) \wedge \cdots \wedge \psi_n(x)]$ which is equivalent to a primitive sentence. We can now repeat the process above, getting indecomposable sequences b^n, $x^{i,n}$, e^i (replacing respectively b, the variables x_i, and the constants d_i used in $\psi_0(b) \wedge \cdots \wedge \psi_n(b)$) with each conjunct of $\psi_0(b^n) \wedge \cdots \wedge \psi_n(b^n)$ satisfied coordinate-wise in E^* at each coordinate $\geq p_n$. (We choose $p_n > p_{n-1}$ also.) We repeat for all n. Notice that the sequences e^i which we get are the same each time; they are the (fixed) representatives from $f(d_i)$. However the b^j and $x^{i,j}$ may differ with each j.

Now define the new sequences in $E^{*\omega}$ as follows:

$$c_i = a_i^0 \quad \text{for all coordinates } i \text{ satisfying } i < p_1,$$
$$ = a_i^n \quad \text{for all coordinates } i \text{ satisfying } p_n \leqq i < p_{n+1},$$

$$y_i^j = x_i^{j,0} \quad \text{for all coordinates } i \text{ satisfying } i < p_1,$$
$$ = x_i^{j,n} \quad \text{for all coordinates } i \text{ satisfying } p_n \leqq i < p_{n+1}.$$

Of course it is intended that $c \in E^{*\omega}$ correspond to $b \in A$, and $y^j \in E^{*\omega}$ to the variables x_j. The sequence c is indecomposable because, from the construction, if b satisfied ϕ_j in $\mathfrak{A}$, then from some coordinate on, c_i satisfies ϕ_j and hence ϕ_j could not split c. (Since b satisfies ϕ_j in $\mathfrak{A}$, $\phi_j(b)$ will eventually appear as a conjunct in some ψ_k.) Similarly the sequences y^j are indecomposable. Moreover any polynomial z in the y^j's, e^j's, and c is also indecomposable since z will eventually be defined and its properties "discussed" in the ψ_i's and hence, for the same reasons as above,

it will be indecomposable. Consequently the y^j's, e^j's, and c generate an indecomposable subring R in Q and we get a maximal indecomposable subring $R'_1 \cong R$ $\cong f(D) \cup \{c\}$. We define $f' = f$ on D, $f'(b) = [c]$, and we define f' on the subring D' of $\mathfrak{A}$ generated by D and b in the usual way. Clearly $f'(D') \subseteq R \subseteq R'_1$. Let $\psi(d'_0, \ldots, d'_m)$ be a primitive sentence, constants in D', and true in $\mathfrak{A}$. But the d'_i are generated by d_j's $\in D$ and by b. Hence there is a primitive sentence $\theta(b, d_0, \ldots, d_t)$, with constants in $D \cup \{b\}$, which is equivalent to ψ and which is true in $\mathfrak{A}$. From the construction above, $\theta([c], f(d_0), \ldots, f(d_t))$ is true in R'_1. But then so is $\psi(f'(d'_0), \ldots, f'(d'_m))$, and the lemma is proved.

Proof of Theorem 2.11.   Let $a_0, a_1, a_2, \ldots, a_\alpha, \ldots, \alpha < \omega_1$ be a list of $A - E^*$. Apply Lemma 2.13 with $D = E^*$, $b = a_0$, $f =$ the identity map, R'_0 any fixed maximal indecomposable subring of Q. The condition on primitive sentences holds because $\mathfrak{A}$ and R'_0 are strong nonstandard models of arithmetic. By transfinite induction, we successively apply the lemma to the a_i's and this embeds $\mathfrak{A}$ in Q as an indecomposable subring.

COROLLARY 2.14. *Every maximal indecomposable subring R' of Q is uncountable.*

Proof. Suppose R'_0 has power $\aleph_0$. There exists a proper elementary extension $\mathfrak{B}$ of R'_0 with the cardinality of $|\mathfrak{B}| = \aleph_0$. Take $b \in |\mathfrak{B}| - R'_0$. Apply Lemma 2.13 with $D = R'_0$, $f =$ the identity map, $R'_0 = R'_0$. We get $R'_1 \supseteq R'_0$ and $R'_1 \neq R'_0$. This contradicts the maximality of R'_0.

A well-known method for obtaining nonstandard models of arithmetic is the ultraproduct construction.

We shall denote nonprincipal ultrafilters over ω by D_F. If D is the filter of cofinite subsets of ω, then $D \subseteq D_F$ for every D_F. Thus if $[x] \in E^{*\omega}/D = Q$, then $[x] \subseteq [x]_F \in E^{*\omega}/D_F$. Suppose R' is a maximal indecomposable subring of Q. Then there is a natural embedding of R' into $E^{*\omega}/D_F$ for every D_F, gotten simply by mapping $[x] \in R'$ to $[x]_F \in E^{*\omega}/D_F$. One can then ask the questions: Given any R', is there a D_F such that the natural embedding is onto? And given any D_F, is there an R' such that the natural embedding is onto? In the remainder of the section we answer the latter question negatively (Proposition 2.16), and present some further results connecting indecomposable sequences and nonprincipal ultrafilters.

DEFINITION 2.15 Suppose $x = (x_0, x_1, x_2, \ldots) \in E^{*\omega}$, $A \in \mathscr{P}(E) - \mathscr{P}_{\text{fin}}(E)$. Let $A = \{a_0, a_1, a_2, \ldots\}$, enumerated without repetitions in increasing order. Then we define $x_A \in E^{*\omega}$ by $x_A = (x_{a_0}, x_{a_1}, x_{a_2}, \ldots)$.

PROPOSITION 2.16. *There is a nonprincipal ultrafilter D_F and a sequence $s \in E^{*\omega}$ such that $[s]_F$ contains no indecomposable sequences.*

Proof. Let $s = (0, +1, -1, +2, -2, +3, -3, \ldots)$. Define $\mathfrak{A} = \{\overline{A} \mid A \subseteq \omega$ and s_A is indecomposable}. Claim that $\mathfrak{A}$ generates a filter. It suffices to show that if $\overline{A}_1, \ldots, \overline{A}_n \in \mathfrak{A}$ then $\bigcap_{i=1}^n \overline{A}_i \neq \varnothing$. Suppose $\bigcap_{i=1}^n \overline{A}_i = \varnothing$. Then $\bigcup_{i=1}^n A_i = \omega$. Now it is a simple task to obtain $n+1$ infinite arithmetic sets $B_1, \ldots, B_{n+1}$ such that

$B_i \cap B_j = \varnothing$ for $i \neq j$ and $\bigcup_{i=1}^{n+1} B_i = E^*$. Suppose $\phi_i(v)$ defines B_i, $i = 1$ to $n+1$. Let $T_A = \{a \in E^* \mid a \text{ appears in the sequence } s_A\}$. Then for each i, $i = 1$ to n, there must be a B_j such that $B_j \cap T_{A_i}$ is infinite and $T_{A_i} - B_j$ is finite; otherwise there would be a B_k such that both $B_k \cap T_{A_i}$ and $T_{A_i} - B_k$ are infinite and then $\phi_k(v)$ would split s_{A_i}. But there are $n+1$ B_j's and only n A_i's. Thus for some B_j, $B_j - \bigcup_{i=1}^{n} T_{A_i}$ is infinite. This contradicts $\bigcup_{i=1}^{n} A_i = \omega$. So $\mathfrak{A}$ generates a filter. It is a trivial fact that any integer is contained in some indecomposable sequence. Hence $\bigcap_{\bar{A} \in \mathfrak{A}} \bar{A} = \varnothing$. So there is a nonprincipal ultrafilter $D_F \supseteq \mathfrak{A}$. Consider $[s]_F \in D_F$. If x is an indecomposable sequence and $x \in [s]_F$ then $s_i = x_i$ for $i \in A \in D_F$ and then s_A is indecomposable. But then we would have put $\bar{A} \in \mathfrak{A} \subseteq D_F$, which contradicts $A \in D_F$. Then $[s]_F$ contains no indecomposable sequences.

Using the D_F of this theorem we form $E^{*\omega}/D_F$. No R' can map onto $E^{*\omega}/D_F$ under the natural embedding because if $[x] \in R' \to [s]_F \in E^{*\omega}/D_F$ where $s = (0, +1, -1, \ldots)$, then $[x] \subseteq [s]_F$ and then $[s]_F$ would contain the indecomposable sequence x.

LEMMA 2.17. *Let D_F be a nonprincipal ultrafilter over ω, and $E^{*\omega}/D_F$ the ultra-power of E^* defined by D_F. Then every member of $E^{*\omega}/D_F$ contains an indecomposable sequence $\Leftrightarrow$ for every $x \in E^{*\omega}$ there is an $A \in D_F$ such that x_A is indecomposable.*

Proof. Assume the first condition and consider $x \in E^{*\omega}$. Then $[x]_F \in E^{*\omega}/D_F$ and there is a $y \in [x]_F$ with y indecomposable. Since x and y are in the same equivalence class of $E^{*\omega}/D_F$, there is an $A \in D_F$ such that $x_i = y_i$ iff $i \in A$. Thus x_A is y_A and y_A is indecomposable since y is.

Now assume the second condition and consider $[x]_F \in E^{*\omega}/D_F$. We have, fixing x, an $A \in D_F$ such that x_A is indecomposable. Define $y \in E^{*\omega}$ as follows:

if $i \in A$, $y_i = x_i$,
if $i < a_0$ (the smallest member of A), $y_i = x_{a_0}$,
if $a_j < i < a_{j+1}$, $y_i = x_{a_{j+1}}$.

From the construction it is clear that y is indecomposable. Furthermore, $B = \{i \mid x_i = y_i\} \supseteq A$ and so $B \in D_F$. Thus $y \in [x]_F$.

LEMMA 2.18. *Given $s \in E^{*\omega}$ and A an infinite subset of E. Then there exists an infinite $B \subseteq A$ such that s_B is indecomposable.*

Proof. The proof proceeds in much the same way as the method, used earlier in this section, to construct indecomposable sequences. If $T_A = \{a \in E^* \mid a \text{ appears in the sequence } s_A\}$ is finite, then we can make s_B a constant sequence. If T_A is infinite, then we use the method just mentioned, but we arrange to choose all values from T_A.

PROPOSITION 2.19 (C.H.). *There is a nonprincipal ultrafilter D_F over ω such that every $[x]_F \in E^{*\omega}/D_F$ contains an indecomposable sequence.*

Proof. Let $[s^0]$, $[s^1]$, $[s^2]$, ..., $[s^\alpha]$, ..., $\alpha < \omega_1$ be a listing of the members of Q. The proof proceeds by induction. We assume that for a countable number of s^i's we have found $A^i \subseteq E$ such that $s^i_{A^i}$ is indecomposable and any finite number of the A^i's has an infinite intersection. Let us relabel these s^i's as t^0, t^1, t^2, ... and the A^i's corresponding to them as B^0, B^1, B^2, ... Now consider a new s^i, call it s. Choose $b_0 \in B^0$, $b_1 \in B^1 \cap B^0 - \{b_0\}$, ... and, in general, $b_n \in B^n \cap B^{n-1} \cap \cdots \cap B^0 - \{b_0, \ldots, b_{n-1}\}$. This is possible because any finite intersection of the B^i's is infinite. Define $A = \{b_0, b_1, b_2, \ldots\}$. Clearly A is infinite. Now apply Lemma 2.18 to s and A. We get an infinite $B \subseteq \{b_0, b_1, b_2, \ldots\}$ such that s_B is indecomposable. For any finite number of the B's, say $B^{i_1}, \ldots, B^{i_m}$, we have $B \cap \bigcap_{j=1}^m B^{i_j} \supseteq B - \{b_0, \ldots, b_{k-1}\}$ where $k \geq i_j$ for all $j = 1$ to m. Since B is infinite, so is $B \cap \bigcap_{j=1}^m B^{i_j}$. Thus we have $\{t^i\}_1^\infty \cup \{s\}$ and $\{B^i\}_1^\infty \cup \{B\}$ satisfying the induction hypothesis. By transfinite induction, we have the result for all the s^α, $\alpha < \omega_1$. It is a trivial matter to perform the above construction in such a way that for every $e \in E^*$ there is an A^i associated with some s^i such that $e \notin A^i$. We assume this was done. Hence the A^i's generate a filter F over ω, and there is a nonprincipal ultrafilter $D_F \supseteq F$. Suppose $x \in E^{*\omega}$, and $x \in [s^i] \in Q$ for some fixed i. Since $s^i_{A^i}$ is indecomposable, so is x_{A^i}. Of course $A^i \in D_F$. We then have the result by Lemma 2.17.

3. Diophantine correct rings.

DEFINITION 3.1 (CF. NERODE [10]). A ring D is weakly diophantine correct (w.d.c.) if every finite conjunction of formulas of the form $d_i + d_j = d_k$, $d_i \cdot d_j = d_k$, or $d_i \neq d_j$, which contains at most one formula of the last type and which is true in D, has a solution in E^*.

For example, by Theorem 2.1 of Nerode [8], Λ^* is w.d.c. It is also easy to see that

PROPOSITION 3.2. *Q and all its subrings are w.d.c.*

Proof. Clearly it suffices to show that Q is w.d.c. Let ϕ be a conjunction such as in Definition 3.1. ϕ has the form $\psi \wedge x_i \neq x_j$. (It suffices to consider this since it is the worst case.) Since ψ is a conjunction of positive equations holding in Q, we can fix representatives from all the equivalence classes of ϕ and get a coordinate k_0 such that for all coordinates greater than k_0, ψ holds coordinatewise (in E^*). Now $x_i \neq x_j$ is satisfied infinitely often coordinatewise. Let $k_1 > k_0$ be one of these coordinates. Hence the k_1th coordinate of the representatives provides the required solution.

PROPOSITION 3.3. *A necessary and sufficient condition for a ring D of power $\leq \aleph_1$ to be embeddable in Q is that D be w.d.c.*

Proof. The necessity was shown above. Suppose now that D is w.d.c. The proof proceeds exactly as in Proposition 1.7 (ii), replacing Λ^* by D and appealing to the w.d.c. property of D instead of to the theorem of Nerode. We do not need the C.H. here because we assume the cardinality of $D \leq \aleph_1$.

COROLLARY 3.4 (C.H.). *If M is the class of w.d.c. rings, then Q is M-universal (see Definition 1.5).*

Proof. By the C.H., the cardinality of $Q = \aleph_1$. By the proposition, every member of M of power $\leq \aleph_1$ can be embedded in Q. And of course, $Q \in M$.

Let M be a class of similar relational systems. The following conditions and their numbering are from Jónsson [5].

(V) The union of any chain of members of M belongs to M.

(VI)$_\kappa$ If $\mathfrak{A} \in M$ and $X \subseteq |\mathfrak{A}|$, the cardinality of $X < \kappa$, then $X \subseteq |\mathfrak{B}|$ for some $\mathfrak{B} \in M$, $|\mathfrak{B}| \subseteq |\mathfrak{A}|$, the cardinality of $|\mathfrak{B}| < \kappa$.

DEFINITION 3.5 (JÓNSSON [5]). Let M be a class of similar relational systems and $\mathfrak{A} \in M$, the cardinality of $|\mathfrak{A}| = \kappa$. $\mathfrak{A}$ is *M-homogeneous* if for any $\mathfrak{B} \in M$, $|\mathfrak{B}| \subseteq |\mathfrak{A}|$, the cardinality of $|\mathfrak{B}| < \kappa$ and for any isomorphism f of $\mathfrak{B}$ into $\mathfrak{A}$, f can be extended to an automorphism of $\mathfrak{A}$.

PROPOSITION 3.6 (C.H.). *Q is not M-homogeneous, for M the class of w.d.c. rings.*

Proof. It is easy to see that M satisfies (V) and (VI)$_{\aleph_1}$. We have $Q \in M$ and the cardinality of $Q = \aleph_1$. So we can apply Corollary 2.4(d) of Morley and Vaught [7], and hence it will suffice to construct $\mathfrak{B}_1$, $\mathfrak{B}_2$, subrings of Q, each countable, $\mathfrak{B}_1 \subseteq \mathfrak{B}_2$, and an isomorphism f of $\mathfrak{B}_1$ into Q such that f cannot be extended to an isomorphism g of $\mathfrak{B}_2$ into Q.

Define $s \in E^{*\omega}$ to be $(4, 9, 16, 25, \ldots)$, and $r \in E^{*\omega}$ to be $(2, 3, 4, 5, \ldots)$. Then $[s], [r] \in Q$. Let $\mathfrak{B}_1 = E^*([s])$, i.e. $[s]$ adjoined to E^* in Q. Let $\mathfrak{B}_2 = E^*([s], [r])$. Define $f: \mathfrak{B}_1 \to Q$, isomorphism, by $f([s]) = [r]$. Say g, as above, exists. Let $g([r]) = [x]$. Then $g([s]) = g([r]^2) = g([r])^2 = [x]^2$. But $g([s]) = f([s]) = [r]$. So $[r] = [x]^2$, i.e. $r_i = x_i^2$ almost everywhere. Contradiction. So no such g can exist and Q is not M-homogeneous.

In [10], Nerode has shown (without stating it) that every countable diophantine correct ring (see Definition 3.8) can be embedded in Λ^* and in $\Lambda^*(A)$.

Let $X_\omega E^*$ consist of all countably infinite sequences x of elements of E^* such that $\{i \in E \mid x_i \neq 0\}$ is finite. Let L^* be the lattice of finitary recursively enumerable relations $R \subseteq E^{*\omega}$. Every $R \in L^*$ has an extension $R_{\Lambda^*} \subseteq \Lambda^{*\omega}$ (see Nerode [8]).
Define

$$R_{ijk} = \{x \in X_\omega E^* \mid x_i + x_j = x_k\},$$
$$\dot{S}_{ijk} = \{x \in X_\omega E^* \mid x_i \cdot x_j = x_k\},$$
$$T_{ij} = \{x \in X_\omega E^* \mid x_i \neq x_j\},$$

and

$$U_{ij} = X_\omega E^* - T_{ij} = \{x \in X_\omega E^* \mid x_i = x_j\}.$$

PROPOSITION 3.7. *Every countable w.d.c. ring D can be embedded in Λ^* and in $\Lambda^*(A)$.*

Proof. Let $D = \{d_0, d_1, d_2, \ldots\}$, enumerated without repetitions. Let F^* be the filter generated by the R_{ijk}'s such that $d_i + d_j = d_k$ and the S_{ijk}'s such that $d_i \cdot d_j = d_k$. Since D is w.d.c., F^* is a proper filter in L^*. By Theorem 4.7 of Nerode [10], we get $x \in \Lambda^{*\omega}$ such that $F^* = \{A \in L^* \mid x \in A_{\Lambda^*}\}$. Claim $x_i \neq x_j$ for $i \neq j$. If $x_i = x_j$, $x \in (U_{ij})_{\Lambda^*}$. Hence $U_{ij} \in F^*$. So there exists a finite number of R_{ijk}'s and S_{ijk}'s whose intersection, call it I, satisfies $I \subseteq U_{ij}$. Now since D is w.d.c., $I \cap T_{ij} \neq \varnothing$. But then $U_{ij} = X_\omega E^* - T_{ij} \not\supseteq I$. Contradiction. Hence $x_i \neq x_j$, and D is embedded in Λ^* by $d_i \to x_i$. The same proof works for $\Lambda^*(A)$.

COROLLARY 3.8. *Every countable subring of Q can be embedded in Λ^* and in $\Lambda^*(A)$.*

In [10], Nerode defined the notion of a diophantine correct nonstandard model of arithmetic. Generalizing from this, we have

DEFINITION 3.8. A ring D is diophantine correct (d.c.) if every finite conjunction of formulas of the form $d_i + d_j = d_k$, $d_i \cdot d_j = d_k$, or $d_i \neq d_j$, which is true in D, has a solution in E^*.

Clearly if D is d.c. then D is w.d.c.

LEMMA 3.9. *Every indecomposable subring R of Q is diophantine correct.*

Proof. Let ψ be a conjunction as described in Definition 3.8 involving $[r^0], \ldots, [r^n] \in R$. We assume ψ is true in R. Clearly if $[r^i] + [r^j] = [r^k]$ or $[r^i] \cdot [r^j] = [r^k]$ is true in R, then the relation holds coordinate-wise among the r^i's for almost all coordinates. Say $[r^i] \neq [r^j]$. Then $[r^i - r^j] \neq 0$. But $[r^i] - [r^j] \in R$, since R is a ring, and hence $r^i - r^j$ is indecomposable. So $r^i_k - r^j_k \neq 0$ for almost all coordinates k or else the formula $v = 0$ would split $[r^i - r^j]$. Thus the inequality relation holds between r^i and r^j at almost all coordinates. So there is a coordinate p beyond which all the conjuncts of ψ hold in E^* coordinate-wise. Take $k > p$ and the r^i_k's provide the desired solution in E^*.

LEMMA 3.10. *If D is a d.c. ring of power $\leq \aleph_1$, then D can be embedded in Q as an indecomposable subring.*

Proof. Let ϕ be any finite conjunction of members of

$$S = \{d_i \neq d_j \mid d_i \neq d_j \text{ is true in } D\}$$
$$\cup \{d_i + d_j = d_k \mid d_i + d_j = d_k \text{ is true in } D\}$$
$$\cup \{d_i \cdot d_j = d_k \mid d_i \cdot d_j = d_k \text{ is true in } D\}.$$

Let T^* denote the set of all statements of arithmetic true in $\langle E^*, =, +, \cdot, 0, 1 \rangle$. Then we have at once that $T^* \cup \{\phi\}$ is satisfiable in E^*. Hence by the downward Skolem-Löwenheim theorem (see Tarski and Vaught [14]), D is embeddable in a model $\mathfrak{A}$ of T^* of power $\aleph_1$. By Theorem 2.11, $\mathfrak{A}$ is embeddable in Q as an indecomposable subring. Hence D is embeddable in Q as an indecomposable subring.

PROPOSITION 3.11. *A necessary and sufficient condition for a ring D of power $\leqq \aleph_1$ to be embeddable in Q as an indecomposable subring is that D be diophantine correct.*

Proof. The proof is immediate from Lemmas 3.9 and 3.10.

BIBLIOGRAPHY

1. C. C. Chang and A. C. Morel, *On closure under direct product*, J. Symbolic Logic **23** (1958), 149–154.

2. S. Feferman and R. L. Vaught, *The first order properties of products of algebraic systems*, Fund. Math. **47** (1959), 57–103.

3. T. Frayne, A. C. Morel and D. Scott, *Reduced direct products*, Fund. Math. **51** (1962/1963), 195–228; errata, ibid. **53** (1963), 117.

4. B. Jónsson, *Universal relational systems*, Math. Scand. **4** (1956), 193–208.

5. ———, *Homogeneous universal relational systems*, Math. Scand. **8** (1960), 137–142.

6. H. J. Keisler, *Universal homogeneous Boolean algebras*, Michigan Math. J. **13** (1966), 129–132.

7. M. Morley and R. Vaught, *Homogeneous universal models*, Math. Scand. **11** (1962), 37–57.

8. A. Nerode, *Extensions to isolic integers*, Ann. of Math. **75** (1962), 419–448.

9. ———, *Arithmetically isolated sets and nonstandard models*, pp. 105–116, Proc. Sympos. Pure Math., Vol. 5, Amer. Math. Soc., Providence, R. I., 1962.

10. ———, *Diophantine correct nonstandard models in the isols*, Ann. of Math. **84** (1966), 421–432.

11. P. Olin, *Nonstandard models of arithmetic and some embedding theorems*, Notices Amer. Math. Soc. **14** (1967), 141.

12. ———, *Amost everywhere direct products and saturation*, Notices Amer. Math. Soc. **14** (1967), 370.

13. A. Robinson, *Introduction to model theory and to the metamathematics of algebra*, North-Holland, Amsterdam, 1963.

14. A. Tarski and R. Vaught, *Arithmetical extensions of relational systems*, Compositio Math. **13** (1958), 81–102.

15. B. Jónsson and P. Olin, *Almost direct products and saturation*, Compositio Math. **20** (1968), 125–132.

CORNELL UNIVERSITY,
   ITHACA, NEW YORK