## NONSTANDARD ARITHMETIC<sup>1</sup>

## ABRAHAM ROBINSON

1. Introduction. In 1934 it was pointed out by Thoralf Skolem [23] that there exist proper extensions of the natural number system which have, in some sense, "the same properties" as the natural numbers. As the title of his paper indicates, Skolem was interested only in showing that no axiomatic system specified in a formal language (in his case the Lower Predicate Calculus) can characterize the natural numbers categorically; and he did not concern himself further with the properties of the structures whose existence he had established. In due course these and similar structures became known as nonstandard models of arithmetic and papers concerned with them, wholly or in part, including certain applications to other fields, appeared in the literature (e.g. [7], [9], [11], [14], [15], [16], [17]). Beginning in the fall of 1960, the application of similar ideas to analysis led to a rapid development in which nonstandard models of arithmetic played an auxiliary but vital part. It turned out that these ideas provide a firm foundation for the nonarchimedean approach to the Differential and Integral Calculus which predominated until the middle of the nineteenth century when it was discarded as unsound and replaced by the  $\epsilon$ ,  $\delta$  method of Weierstrass. Going beyond this area, which is particularly interesting from a historical point of view, the new method (which has come to be known as Nonstandard Analysis) can be presented in a form which is sufficiently general to make it applicable also to mathematical theories which do not involve any metric concept, e.g., to general topological spaces [18].

In the present paper we shall show how the experience gained with this more general approach can be used in order to throw new light also on arithmetic or more precisely, on the classical arithmetical theories which have grown out of elementary arithmetic, such as the theory of ideals, the theory of p-adic numbers, and class field theory. Thus we shall provide new foundations for infinite Galois theory and for the theory of idèles. Beyond that, we shall develop a theory of ideals for the case of infinite abelian extensions in class field theory. This is remarkable, for Chevalley introduced idèles [2] precisely in

<sup>&</sup>lt;sup>1</sup> An address delivered before the San Jose meeting of the Society on April 22, 1967 by invitation of the Committee to Select Hour Speakers for Far-Western Sectional Meetings. Research supported in part by the National Science Foundation, Grant No. GP-5600; received by the editors June 17, 1967.

order to deal with infinite extensions since, classically, the ideals in the ground field cannot cope with this case.

§5 below is related to the theory of p-adic completions and of idèles in Dedekind rings which is developed in [17], [20].

I acknowledge with thanks several stimulating conversations with W. A. J. Luxemburg, A. M. MacBeath and O. Todd while participating in a program on Nonstandard Analysis sponsored by the Office of Naval Research at the California Institute of Technology. Among others from whose knowledge I have benefited in connection with the problems considered here, I wish to mention particularly P. Roquette, E. G. Straus, and H. Zassenhaus.

2. Enlargements and ultrapowers. In this section we give an informal description of the framework which is required for our subsequent arguments. The reader may consult [18] for a formal development.

Let M be a mathematical structure of any kind and let R(x, y) be a binary relation of arbitrary type in M. Thus, R may be a relation between individuals of M or between individuals and functions, or between sets and binary relations, etc. By the *first domain* of R,  $D_R$ , we mean the set of all entities (individuals, relations, functions,  $\cdots$ ) a for which there exists a b such that R(a, b) holds (is satisfied) in M. We shall say that R is concurrent if, for every finite subset  $\{a_1, \dots, a_n\}$  of  $D_R$ ,  $n \ge 1$ , there exists an entity b in M such that  $R(a_1, b)$ ,  $R(a_2, b)$ ,  $\cdots$ ,  $R(a_n, b)$  all hold in M. Now let M' be an extension of M. We shall say that the relation R(x, y) in M is bounded in M' if there exists an entity  $b_R$  in M' such that  $R(a, b_R)$  holds in M' for all  $a \in D_R$ , i.e., for all elements of the first domain of R in M.  $b_R$  will be called a bound for R.

An extension  ${}^*M$  of M is called an *enlargement* of M if all concurrent relations of M are bounded in  ${}^*M$  and if, moreover, all statements which hold in M hold also in  ${}^*M$  in a sense which will now be explained.

Let K be the set of all statements which hold in M. We may imagine that these statements are expressed in a formal language L which includes symbols for all individuals of M, for all sets of M, and for all functions, relations, sets of relations, etc. of all (finite) types. In addition, L is supposed to include the usual connectives,  $\bigcap$  (not),  $\bigvee$  (or),  $\bigwedge$  (and),  $\bigcap$   $(if \cdots then)$ , and also variables and quantifiers (for all and there exists). Quantification is permitted with respect to entities of all types (e.g., "for all functions of two variables," "there exists a ternary relation between sets").

To every entity (individual, function, relation,  $\cdots$ ) R in M, there corresponds an entity R in M, which is denoted by the same symbol in L. A relation R holds between entities  $S_1, \dots, S_n$  in M if and only if \*R holds between  $*S_1, \dots, *S_n$  in \*M. On this basis, any statement X of K can be reinterpreted in M where we assign their usual meaning to the connectives and to quantification with respect to individuals. However, when interpreting quantification with respect to entities of higher type in \*M, we shall (in general) not refer to the totality of entities of the type in question but to a certain subclass of such entities called *internal*. Thus, the phrase which in M signifies "there exists a function of three variables" is to be interpreted in \*M as "there exists an internal function of three variables." and, similarly, "for all binary relations in M" corresponds to "for all internal binary relations in M. It is in this sense that the statements of K are required to hold also in M (for some fixed determination of the class of internal entities) where the bounds of concurrent relations introduced above also must be internal.

It is a simple consequence of the compactness theorem (finiteness principle) that every structure M possesses an enlargement \*M.\*M is a proper extension of M if and only if the number of individuals of M is infinite and, in this case, there are many nonisomorphic enlargements for the given M. In particular \*M can be constructed as a suitable ultrapower of M [4], [8], [10]. However, in many cases the mode of construction of \*M is irrelevant and all necessary information concerning it can be extracted from the defining properties of an enlargement as laid down above. There are exceptions to this and some of them will be discussed in due course.

The following example, which is fundamental, will show how we may be able to decide that a particular entity is not internal.

Let N be the system of natural numbers and let N be an enlargement of N. The operations of additions and multiplications extend automatically from N to N. The relation of order, n < n, is concurrent in n. It follows that it possesses a bound in n, to be denoted by n. Then n < n, and, quite generally, n < n for all natural numbers  $n \in N$ . This shows that n is a proper extension of n, in agreement with the general statement made above on enlargements of infinite structures. From now on all individuals of n will be called natural numbers, the numbers of n being standard and finite while the remaining numbers of n are nonstandard and infinite. It is not difficult to show that any infinite natural number is greater than every finite natural number.

The set of infinite natural numbers, \*N-N, cannot be internal.

For it is a fact of N that "every nonempty set of natural numbers includes a smallest element." Reinterpreting the statement in quotes for N, we conclude that every *internal* set of numbers of N includes a smallest element. For if N is a finite number, N also is finite; so if N is infinite, then N also is infinite. This shows that N cannot be internal.

For an example of an internal set, consider the set A of all infinite natural numbers greater than some infinite natural number a,  $A = \{y | y > a\}$ . It is true in N that "for every natural number x there exists a set z which consists of all natural numbers y such that y > x." But the statement in quotes must be true also in \*N in the sense that for every number x in \*N there exists an *internal* set z such that  $z = \{y | y > x\}$ . It follows in particular that  $A = \{y | y > a\}$  is an internal set.

When applying nonstandard analysis to other mathematical structures, e.g., to a topological space T, it is essential to consider not only an enlargement  ${}^*T$  of T but to enlarge simultaneously all other mathematical structures which occur in the argument, e.g., the natural numbers, N. This can be done by taking for M some structure (e.g., a model of Set Theory) which includes both T and N. We then work in an enlargement  ${}^*M$  of M which contains simultaneous enlargements  ${}^*T$  and  ${}^*N$  of T and N.

Although we have assumed for the definition of an enlargement that all concurrent binary relations in M possess bounds in \*M, only a small proportion of these will be required in practice. Thus, in retrospect, it is then possible to weaken the definitions of an enlargement by supposing that only the concurrent relations that are involved in the argument possess bounds in \*M. We shall then say that \*M is an enlargement for the relations in question.

In particular, let M be a structure which includes the natural numbers N and let \*M be an enlargement of M for the concurrent relation x < y between natural numbers. Then \*M contains an extension \*N of N which is an enlargement of N for the relation x < y. We claim that if R(x, y) is a concurrent relation in M, of any type, with countable first domain, then R(x, y) possesses a bound in \*M. Indeed, let  $A = \{a_0, a_1, a_2, \cdots\}$  enumerate the first domain of such a relation. By assumption, there exists a sequence of entities  $B = \{b_0, b_1, b_2, \cdots\}$  in M such that  $R(a_j, b_k)$  holds in M for  $j \le k$ ,  $k = 0, 1, 2, \cdots$ . The "sequences" \*A and \*B which correspond to A and B in M then have subscripts ranging over all numbers  $n \in *N$ . The statement "for every natural number x and for every natural number y < x,  $R(a_y, b_x)$  holds in M" must then be true also in \*M,

where it applies, more precisely, to the extension \*R of R. In particular, it is therefore true in \*M that, for an arbitrary *infinite* natural number  $\omega$ ,  $R(a_y, b_\omega)$  holds in \*M for all  $y \le \omega$  and, hence, for all finite y. This shows that  $b_\omega$  is a bound for R(x, y).

Suppose in particular that  ${}^*M$  is an ultrapower  $M_D^N$  of M where the natural numbers N are included in M and also serve as index set for copies of M, and D is a free ultrafilter on N. Then the internal entities of  ${}^*M$  are simply all sequences  $a = \{a_n\}$ ,  $b = \{b_n\}$ ,  $S = \{S_n\}$ ,  $\cdots$  of entities of corresponding types in M. Two entities of  ${}^*M$  are regarded as equal if the set of subscripts on which they coincide belongs to D. And if, for example, a and b are individuals in  ${}^*M$  and S is a binary relation, then S(a, b) holds in  ${}^*M$  by definition if the set

$$\{n \mid S_n(a_n, b_n) \text{ holds in } M\}$$

belongs to D. Then \*M is an enlargement of M for the concurrent relation < between natural numbers, for  $\{0, 1, 2, 3, \cdots\}$  is a number of \*N which is greater than any element of N. Accordingly, all concurrent relations of M with countable first domain possess bounds in \*M.

3. Infinite Galois theory. Let F be a commutative algebraic field and let  $\Phi$  be a separable and normal algebraic extension of F. That is to say,  $\Phi$  is an algebraic extension of F and if a polynomial  $f(x) \in F[x]$  which is irreducible in F possesses a root in  $\Phi$ , then f(x) splits into distinct linear factors in  $\Phi$ .

If  $\Phi$  is of finite degree over F, we have the standard Galois theory for  $\Phi/F$  which establishes a bijection between the subgroups of the group of automorphisms G of  $\Phi/F$  and the subfields of  $\Phi$  which are extensions of F. Dedekind pointed out that this correspondence breaks down if  $\Phi$  is of infinite degree over F, and Krull showed [11] that the situation can be saved by restricting consideration to subgroups of G which are closed in a certain topology. Here we shall give an independent approach to the problem and shall then establish its connection with Krull's theory. We shall suppose from now on that  $\Phi$  is an infinite extension of F.

Let \* $\Phi$  be an enlargement of  $\Phi$  and let \*F be the corresponding enlargement of F, \* $F \subset \Phi$ . Let G be the Galois group of  $\Phi/F$  so that \*G is the corresponding group for \* $\Phi/F$ . Consider the binary relation R(x, y) in  $\Phi$  which is defined as follows:

"x and y are finite normal algebraic extensions of F and subfields of  $\Phi$  and  $x \subset y$ ."

It is not hard to see that R(x, y) is concurrent and hence possesses a bound  $\Psi$  in \* $\Phi$ . By the definition of a bound,  $\Psi$  is a subfield of \* $\Phi$ and an extension of \*F, and moreover,  $\Psi \supset A$ , where A is any subfield of  $\Phi$  which is a finite normal extension of F. But the union of such fields A is equal to  $\Phi$ , and  $A \supset A$ , and so  $\Psi \supset \Phi$ . At the same time, reinterpreting the defining properties of R(x, y) in \* $\Phi$ , we see that  $\Psi$  is a "finite" extension of \*F in the sense of the enlargement. That is to say, there exists a natural number  $n \in N$ , which may and will be infinite, such that n is the degree of  $\Psi$  over \*F. Following a suggestion of M. Machover, we shall say that  $\Psi$  is of starfinite degree over \*F (in place of *O-finite* for *quasi-finite* as in [18]). There exists a "polynomial" f(x) of degree n with coefficients in F such that  $\Psi$  is the splitting field of f(x). That is to say, all general statements which can be made about splitting fields of polynomials in the ordinary case can be made also about  $\Psi$  and f(x), with the appropriate interpretation in the enlargement. In particular, there exists the Galois group H of  $\Psi$  over \*F. H consists of all internal automorphisms of  $\Psi$  which leave the elements of \*F invariant, where the word internal will be used throughout in the sense introduced in §2 above. We have the usual Galois correspondence between the *internal* subgroups of H and the *internal* subfields of  $\Psi$  which are extensions of \*F.

Let  $\sigma \in H$ . By a standard result on extensions of isomorphisms,  $\sigma$  is the restriction of some element of  ${}^*G$  to  $\Psi$ . Moreover, since  $\Phi$  is a union of finite normal extensions of F,  $\sigma \Phi \subset \Phi$  and  $\sigma^{-1}\Phi \subset \Phi$  and so  $\sigma \Phi = \Phi$ . Thus, the restriction  ${}^{\circ}\sigma$  of  $\sigma$  to  $\Phi$  is an automorphism of  $\Phi$  which leaves the elements of F invariant. Then  ${}^{\circ}\sigma \in G$ , and  $\sigma \to {}^{\circ}\sigma$  determines a homomorphism from H onto G, whose kernel consists of the elements of H that leave all elements of  $\Phi$  invariant. We write  $H \to {}^{\circ}H = G$ .

Let  $\Theta$  be a subfield of  $\Phi$  and an extension of F,  $F \subset \Theta \subset \Phi$ , and put  $(*\Theta)_{\Psi} = *\Theta \cap \Psi$ . Let  $H_{\Theta}$  be the subgroup of H which corresponds to  $(*\Theta)_{\Psi}$  under the Galois correspondence. Define  ${}^{\circ}H_{\Theta}$  by

$${}^{\circ}H_{\Theta} = \{ \tau \mid \tau = {}^{\circ}\sigma \text{ for some } \sigma \in H_{\Theta} \}.$$

As shown, the elements of  ${}^{\circ}H_{\Theta}$  are automorphisms of  $\Phi/F$  so that  ${}^{\circ}H_{\Theta} \subset G$ . More precisely,  ${}^{\circ}H_{\Theta}$  is a subgroup of G.

We claim that  $\Theta$  is the set of invariants of  $\Phi$  under  ${}^{\circ}H\Theta$ .

In fact,  $\Theta \subset ({}^*\Theta)_{\Psi}$ , and the elements of  $({}^*\Theta)_{\Psi}$  are invariant under the automorphisms of  $H\Theta$ . On the other hand, if  $a \in \Phi$ , but  $a \notin \Theta$ , then  $a \notin \Phi$  and so  $a \notin ({}^*\Theta)_{\Psi}$ . It follows that there exists  $a \sigma \in H\Theta$  such that  $\sigma a \neq a$  and so  $\sigma a \neq a$ . This proves our assertion.

Conversely,  ${}^{\circ}H_{\Theta}$  is the set of automorphisms of G which leave the elements of  $\Theta$  invariant.

Suppose that  $\sigma \in G$  leaves the elements of  $\Theta$  invariant. Then \* $\sigma$  leaves the elements of \* $\Theta$  invariant. Thus  $(*\sigma)_{\Psi}$ , the restriction of \* $\sigma$  to  $\Psi$ , leaves the elements of  $(*\Theta)_{\Psi}$  invariant. Hence,  $(*\sigma)_{\Psi} \in H_{\Theta}$  and, further,  $\sigma = ((*\sigma)_{\Psi}) \in H_{\Theta}$ . This completes the argument.

Accordingly, we have a mapping  $\gamma \colon \Theta \to^{\circ} H_{\Theta}$  from the subfields of  $\Phi$  which are extensions of F into the set of subgroups of G. The main question is how to characterize the subgroups of G which belong to the image of  $\gamma$ .

For any  $\sigma \in {}^*G$ , we define  ${}^\circ\sigma$  as the restriction of  $\sigma$  from  ${}^*\Phi$  to  $\Phi$ .  ${}^\circ\sigma$  is then identical with  ${}^\circ(\sigma_\Psi)$  where  $\sigma_\Psi$  is the restriction of  $\sigma$  from  ${}^*\Phi$  to  $\Psi$  and  ${}^\circ(\sigma_\Psi)$  is the further restriction of  $\sigma_\Psi$  from  $\Psi$  to  $\Phi$  as introduced previously. For any subset S of G, which may be internal or external, we define  ${}^\circ S$  by

$${}^{\circ}S = \{ \tau \mid \tau = {}^{\circ}\sigma \text{ for some } \sigma \in S \}.$$

3.1 THEOREM. A subgroup J of G belongs to the image of  $\gamma$  if and only if  $\circ(*J) = J$ .

Observe that  ${}^{\circ}({}^*J) \supset J$  for all subsets J of G. Accordingly, the condition of the theorem may be replaced by  ${}^{\circ}({}^*J) \subset J$ .

The condition is necessary. For suppose J belongs to the image of  $\gamma$ , so that  $J={}^{\circ}H\Theta$  for some field  $\Theta$ ,  $F\subset\Theta\subset\Phi$ , as above. Then J is the set of  $\sigma\in G$  under which the elements of  $\Theta$  are invariant; and so, by one of the basic properties of enlargements,  ${}^{*}J$  is the set of  $\sigma\in {}^{*}G$  under which the elements of  ${}^{*}\Theta$  are invariant. It follows that all elements of  $\Theta$  are invariant under the automorphisms which belong to  ${}^{\circ}({}^{*}J)$  and so  ${}^{\circ}({}^{*}J)\subset J$ , as asserted.

Conversely, suppose that  ${}^{\circ}(*J) = J$ . Let  $(*J)_{\Psi}$  be the group which consists of the restrictions of the elements of \*J to  $\Psi$ . Then  $(*J)_{\Psi}$  is internal. Let  $\Lambda$  be the subfield of  $\Psi$  which corresponds to  $(*J)_{\Psi}$  under the Galois correspondence for  $\Psi$ . Then the elements of  $\Lambda$  are invariant under the automorphisms of  $(*J)_{\Psi}$  and so the elements of  $\Theta = \Lambda \cap \Phi$  are invariant under the elements of  $(*J)_{\Psi} = (*J) = J$ . Moreover, if  $a \in \Phi - \Theta$ , then  $a \in \Psi - \Lambda$  and so  $\sigma a \neq a$  for some  $\sigma \in (*J)_{\Psi}$ . Hence  $\sigma a \neq a$  where  $\sigma \in ((*J)_{\Psi}) = J$ . Thus,  $\Theta$  consists of all elements of  $\Theta$  which are invariant under J, and further,  $*\Theta$  consists of all elements of  $*\Theta$  which are invariant under \*J. But this shows that  $(*\Theta)_{\Psi} = *\Theta \cap \Psi$  consists of all elements of  $\Psi$  which are invariant under the automorphisms of  $(*J)_{\Psi}$ ; and so,  $\Theta_{\Psi} = \Lambda$ . Thus, in our previous notation,  $(*J)_{\Psi} = H_{\Theta}$  and  $J = {}^{\circ}H_{\Theta}$ . Hence  $\gamma : \Theta \rightarrow J$ , as required. This completes the proof of 3.1.

- 3.1 can be used for the proof of standard results, for example of the well known
- 3.2 THEOREM.  $J = \gamma(\Theta)$  is a normal subgroup of G if and only if  $\Theta$  is a normal extension of F.

PROOF. If  $\Theta \subset \Psi$  is a normal extension of F then  ${}^*\Theta$  is a normal extension of  ${}^*F$ . Hence,  $({}^*\Theta)_{\Psi}$  is a normal extension of  ${}^*F$ . Conversely, if  $({}^*\Theta)_{\Psi}$  is normal over  ${}^*F$  then  $\Theta = ({}^*\Theta)_{\Psi} \cap \Phi$  is normal over F. On the other hand, if J is a normal subgroup of G then  ${}^*J$  is a normal subgroup of  ${}^*G$  and so  $\sigma^*J\sigma^{-1}\subset {}^*J$  for any  $\sigma \in {}^*G$ . Hence, if  $J' = ({}^*J)_{\Psi}$ , then  $\sigma_{\Psi}J'\sigma_{\Psi}^{-1}\subset J'$ , so J' is normal in the Galois group H of  $\Psi$  over  ${}^*F$ . Also,  $J={}^\circ(J')$  so J, which is the image of J' in the mapping  $H {\to} {}^\circ H = G$ , also is normal. Thus, if  ${}^\circ({}^*J) = J$  then J is normal if and only if  $({}^*J)_{\Psi}$  is normal; and for any subfield  $\Theta$  of  $\Phi$  over F,  $\Theta$  is normal if and only if  $({}^*\Theta)_{\Psi}$  is normal. But  $({}^*J)_{\Psi}$  and  $({}^*\Theta)_{\Psi}$  correspond in the Galois correspondence of  $\Psi/{}^*F$  if J and  $\Theta$  correspond in the Galois correspondence  $\sigma$  of  $\Phi/F$ . Hence J is normal if and only if  $\Theta$  is normal. This proves 3.2.

The connection of our condition  $\circ(*J) = J$  with Krull's theory is provided by the following observations.

If  $\circ(*J) = J$  and  $\sigma \in G - J$ , then there exist  $a_1, \dots, a_n \in \Phi$  such that all  $\sigma' \in G$  which coincide with  $\sigma$  on  $a_1, \dots, a_n, \sigma' a_i = \sigma a_i$   $(i = 1, \dots, n)$  do not belong to J either.

In this condition, we might replace  $a_1, \dots, a_n$  by a single a such that F(a) includes  $a_1, \dots, a_n$ .

**PROOF.** Given  $\sigma \in G - J$ , suppose on the contrary that for every  $a_1, \dots, a_n \in \Phi$  there exists  $\sigma' \in G$  which coincides with  $\sigma$  on  $a_1, \dots, a_n$  and such that  $\sigma' \in J$ . Then the relation R(x, y) which is defined by " $x \in \Phi$  and  $y \in J$  and  $\sigma x = yx$ " is concurrent. Thus, there exists a  $y = \tau$  in \*J such that  $\sigma a = \tau a$  for all  $a \in \Phi$ . But then  $\sigma = {}^{\circ}\tau \in {}^{\circ}(*J) = J$ , a contradiction.

Conversely, given a subgroup  $J \subset G$ , suppose that for every  $\sigma \in G - J$  there exists a finite set  $\{a_1, \dots, a_n\} \subset \Phi$  such that  $\sigma' \in G - J$  for all  $\sigma' \in G$  which coincide with  $\sigma$  at  $a_1, \dots, a_n$ , i.e.,  $\sigma a_i = \sigma' a_i$ ,  $(i = 1, \dots, n)$ . Then  $\circ(*J) = J$ .

For suppose  $\sigma \in G - J$ , but  $\sigma = {}^{\circ}\tau$  for  $\tau = {}^{*}J$ . Then  $\sigma a = \tau a$  for all  $a \in \Phi$  and, in particular,  $\sigma a_i = {}^{*}\sigma a_i = \tau a_i$  for  $i = 1, \dots, n$ . Hence, applying the condition of the theorem to  ${}^{*}\Phi$ ,  $\tau \in {}^{*}G - {}^{*}J$ . This contradiction proves the assertion.

In the Krull topology, a fundamental system of neighborhoods of the identity in G is provided by the subgroups which leave finite extensions of F invariant. We have just shown that  $^{\circ}(*J) = J$  if and only if J is closed in that topology.

If  $\Phi$  is an algebraic number field, the Krull topology satisfies the first (and also the second) axiom of countability. It is then true (compare Theorem 9.3.12 of [18]) that the standard part °A of any internal subset A of G is closed. It follows that, in that case, a subgroup J of G is closed in the Krull topology and, equivalently, belongs to the Galois correspondence for  $\Phi$  over F if and only if J is the standard part of an internal subgroup H of \*G, i.e.,  $J = {}^{\circ}H$ . W. A. J. Luxemburg showed recently [13] that even without assuming the validity of an axiom of countability, the standard part of any internal subset of an enlargement \*T of a topological space T must be closed provided \*T is a particular kind of enlargement, a so-called saturated model. For this type of enlargement, the above conclusion concerning closed subgroups of G applies for uncountable  $\Phi$  also.

Coming back to the general case, we observe, for future reference, that the Krull topology of G can be defined without mention of  $\Phi$ , since a fundamental system of neighborhoods of the identity in G is given by the set of subgroups of G which are of finite index in G.

As we have seen, G is a homomorphic image of the starfinite group H,  $H \rightarrow^{\circ} H = G$ . G is also pro-finite ([22], i.e., it is a projective limit of finite groups. We are going to show that every pro-finite group is a homomorphic image of a starfinite group. To see this, let the group G be the projective limit of a set of finite groups  $\{G_{\alpha}\}$  which is indexed on a preordered set I, filtered to the right, with a specified system of homomorphic maps  $f_{\alpha\beta} \colon G_{\beta} \rightarrow G_{\alpha}$ . Passing to an enlargement, we see that there exist elements  $\omega \in I$  which majorize all elements of I,  $\alpha \leq \omega$  for all  $\alpha \in I$ . Then  $G_{\omega}$  is a starfinite group since the  $G_{\alpha}$  are finite for standard  $\alpha$ . In order to map  $G_{\omega}$  homomorphically on G, we observe that the elements of G are points  $g = \{\gamma_{\alpha}\}$  of the cartesian product  $\prod G_{\alpha}$  where  $\gamma_{\alpha} \in G_{\alpha}$  for each  $\alpha \in I$ . We define a mapping  $\phi \colon G_{\omega} \rightarrow G$  by

$$\gamma \to \{\gamma_{\alpha}\} = \{f_{\alpha\omega\gamma}\} = g$$

for any  $\gamma \in G$ . Then  $\gamma_{\alpha} = f_{\alpha\beta}\gamma_{\beta}$  for all  $\alpha$  and  $\beta$  in I so that  $g = \phi$  belongs to G. Evidently,  $\phi$  is a homomorphism. It only remains to be shown that it is onto.

Let  $g = \{\gamma_{\alpha}\}$  be an arbitrary element of I and set  $\gamma = \gamma_{\omega}$ . Then  $\phi \gamma = \{f_{\alpha \omega} \gamma_{\omega}\} = \{\gamma_{\alpha}\} = g$ . This completes the argument.

4. Absolutely algebraic fields of prime characteristic. Let p be a standard prime number. p will remain fixed throughout this section. Let F be the prime field of characteristic p. For every positive integer n there exists a field  $\Phi_n$  which contains just  $p^n$  elements.  $\Phi_n$  is unique

up to isomorphism, and all finite extensions of F are obtained in this way. If  $m \mid n$  then  $\Phi_n$  contains just one field (isomorphic to)  $\Phi_m$ . The elements of  $\Phi_n$  constitute the set of roots of the equation  $x^{p^n} - x = 0$ .

Suppose now that  $\Phi$  is any algebraic extension of F, possibly infinite. We consider an enlargement \* $\Phi$  of  $\Phi$ . \* $\Phi$  contains an enlargement \*F of F but in the present case, \*F = F, since F is finite. An argument similar to that given at the beginning of §3 above shows that there exists a natural number n (which may now be infinite) such that  $\Phi \subset \Phi_n \subset \Phi$ . To continue, we introduce Steinitz' g-numbers, now known also as *surnatural* or supernatural numbers ([5], [12], [21]). A surnatural number is a symbolic expression  $g = 2^{\nu_0}3^{\nu_1} \cdots p_k^{\nu_k} \cdots$ where  $\phi_k$  ranges over all (standard) primes and the  $\nu_k$  are natural numbers,  $\nu_k \in \mathbb{N}$ , or else  $\nu_k = \infty$  where the "symbol"  $\infty$  is taken to be greater than any  $\nu \in \mathbb{N}$ . Surnatural numbers are multiplied by adding exponents with the convention that for all natural  $\nu$ ,  $\infty + \nu$  $=\nu+\infty=\infty+\infty=\infty$ . The surnatural number  $g=2^{\nu_0}3^{\nu_1}\cdots p_k^{\nu_k}\cdots$ divides the surnatural number  $h = 2^{\mu_0}3^{\mu_1} \cdot \cdot \cdot p_k^{\mu_k} \cdot \cdot \cdot$ , and we write  $g \mid h$ , if  $\nu_k \leq \mu_k$  for all k. The g.c.d. and l.c.m. of a finite or infinite set of surnatural numbers are defined in the usual way.

Observe that so far the notions concerning natural numbers, including the introduction of the "symbol"  $\infty$ , were constructed entirely within a framework M regarded as standard. Passing to an enlargement  ${}^*M$  of M, we now define the surnatural part, [n], of any finite or infinite number  $n \in {}^*N$  by  $[n] = 2^{n_0}3^{n_1} \cdots p_k^{n_k} \cdots$  where  $\nu_k$  is the exponent of  $p_k$  in the prime power decomposition of n if that exponent is finite; and  $\nu_k = \infty$  if the exponent in question is infinite, with  $p_k$  ranging over the finite primes. Thus [n] is a standard surnatural number, and the mapping  $n \rightarrow [n]$  is external (not internal).

For  $\Phi \subset \Phi_n$ , as above,  $\Phi_n$  contains exactly the same absolutely algebraic elements as  $\Phi$ . For if  $\overline{F}$  is the algebraic closure of F (unique up to isomorphism) and  $a \in \overline{F} - \Phi$ , then  $a \in {}^*\overline{F} - {}^*\Phi$  in the enlargement and so  $a \notin {}^*\Phi$  and, a fortiori,  $a \notin \Phi_n$ .

Now let m be any finite natural number which divides n. This will be the case if and only if m divides [n]. Then  $\Phi_n$  contains (a field isomorphic to)  $\Phi_m$  as in the standard case. Since all elements of  $\Phi_m$  are absolutely algebraic, it follows that  $\Phi$  contains  $\Phi_m$ . Conversely, if  $\Phi_m \subset \Phi$  for finite m then  $\Phi_m \subset \Phi_n$  and so m divides both n and [n]. Thus [n] (but not n) depends only on  $\Phi$  and is the l.c.m. of all finite m such that  $\Phi_m \subset \Phi$ . We call [n] the Steinitz number of  $\Phi$ ,  $g(\Phi)$ .

Within this framework, Steinitz' result, that to every surnatural number g there exists one and (up to isomorphism) only one absolutely algebraic field of characteristic p whose Steinitz number is g,

can be proved as follows. Given g, it is easy to show that there exists a finite or infinite natural number n such that [n] = g. Let  $\Phi_n$  be the corresponding field which contains  $p^n$  elements and let  $\Phi$  be the subfield of  $\Phi_n$  which consists of the absolutely algebraic elements of  $\Phi_n$ . Then the argument of the preceding paragraph shows that g is the l.c.m. of all finite natural numbers m such that  $\Phi_m \subset \Phi$  and hence,  $g = \gamma(\Phi)$ . On the other hand, let  $\Phi$  and  $\Psi$  be two absolutely algebraic fields of characteristic p with the same Steinitz number g. In order to prove that  $\Phi$  and  $\Psi$  are isomorphic, we may suppose more particularly that they are contained in the same algebraic closure of F,  $\overline{F}$ , and we shall then show that  $\Phi$  and  $\Psi$  actually coincide. Choose a field  $\Phi_n \supset \Phi$ as in the preceding paragraphs and choose a field  $\Phi_m \supset \Psi$  in the same way for  $\Psi$ . Then  $\Phi_n \subset \Phi \subset \overline{F}$  and  $\Phi_m \subset \Psi \subset \overline{F}$  and [n] = [m] = g. Let k be the g.c.d. of n and m so that again [k] = g. Let  $\Phi_k$  be the subfield of \* $\overline{F}$  which contains just  $p^k$  elements. Then  $\Phi_k \subset \Phi_n \cap \Phi_m$ . Let  $\Theta$  be the field which consists of the absolutely algebraic elements of  $\Phi_k$ , then we claim that  $\Theta = \Phi$ . For let  $\alpha \in \Phi$ , then the field  $\Lambda$  generated by  $\alpha$  over F contains just  $p^l$  elements for some finite l. Then  $l \mid n$  and hence  $l \mid g$  and  $l \mid k$ . This implies  $\Lambda \subset \Phi_k$ , and further,  $\alpha \in \Phi_k$ ,  $\alpha \in \Theta$ . Accordingly,  $\Theta = \Phi$  and, similarly,  $\Theta = \Psi$ , and hence  $\Phi = \Psi$ , as asserted.

5. P-adic numbers and valuation theory. Let F be a finite algebraic extension of the field of rational numbers Q (e.g., Q itself), and let \*F be an enlargement of F. For a given archimedean valuation V of Fand hence, of \*F, we denote by  $F_0$  the set of elements a of \*F such that |a| is *finite* in the given valuation, i.e., such that  $|a| \leq r$  for some standard real number r. Also, we denote by  $F_1$  the set of elements a of \*F such that |a| is *infinitesimal*, i.e., such that |a| < r for all standard positive r. Then it is not difficult to see that  $F_0$  is a valuation ring and  $F_1$  is a valuation ideal. The valuation V' which is induced in \*F by the ring  $F_0$  is nonarchimedean although the original valuation V was archimedean. The valuation group  $\Gamma'$  of V' is (isomorphic to) the multiplicative quotient group of  $*F - \{0\}$  with respect to the group  $F_0 - F_1$ . If V is real,  $F_0/F_1$  is isomorphic to the field of real numbers R as can be seen most directly by injecting Finto R and hence \*F into \*R. The corresponding homomorphism  $\phi: F_0 \rightarrow R$  consists of taking the standard part of any  $a \in F_0$  in the metric induced by V. That is to say, for any  $a \in F_0$ ,  $\phi(a) = a$  is the uniquely determined real number such that  $\phi(a) - a \in F_1$ . The mapping  $\phi$  is surjective; for if r is any standard real number, then there exists a standard sequence  $\{s_n\}$ ,  $s_n \in F$ ,  $n \in N$  such that  $\lim_{n \to \infty} s_n = r$ . Passing to the enlargement, we then have  $s_{\omega} - r \in F_1$  for any infinite natural  $\omega$  and so  ${}^{\circ}s_n = r$ . Similarly, if V is complex then  $F_0/F_1$  is isomorphic to the field of complex numbers.

Now let P be a prime ideal in F. For any  $a \in F$ ,  $a \neq 0$ , we define  $\operatorname{ord}_{P}(a)$  as usual as the exponent of P in the prime power decomposition of the ideal (a),  $\operatorname{ord}_{P}(a) \leq 0$ ; and we set  $\operatorname{ord}_{P}(a) = \infty$  for a = 0, by convention. The definition of  $\operatorname{ord}_{P}(a)$  extends to F and then ranges over the finite and infinite rational integers and F. We define F0 (for the given F1) as the set of elements F2 of F3 such that  $\operatorname{ord}_{P}(a)$ 3 is greater than some finite negative integer, and we define F3 as the set of F4 such that  $\operatorname{ord}_{P}(a)$ 4 is an infinite natural number or F5. As before, F7 is a valuation ring in F7 and F7 is its valuation ideal; the corresponding valuation group is the multiplicative quotient group of F6 with respect to F7, and the valuation F9 thus obtained is nonarchimedean. However, F9 is still different from the F9-adic valuation F7 or F8.

It is not difficult to show that  $F_0/F_1$  is (isomorphic to) the P-adic completion of F. In particular, if F is the field of rational numbers and  $P = \{p\}$  where p is a standard prime number, then  $F_0/F_1$  coincides with the field of p-adic numbers. Thus, we obtain the archimedean and nonarchimedean completions of F within the framework of Nonstandard Arithmetic by introducing appropriate valuation rings and ideals in all cases. The uniformity of the procedure becomes even more apparent if we put  $\operatorname{ord}(a) = -|a|$ , for we then have  $a \in F_1$  if  $\operatorname{ord}(a)$  is infinite or equal to  $\infty$ , just as in the non-archimedean case. The analogy can be pursued further, but here we observe only that it motivates the notation used in the sequel for archimedean divisors.

From now on, we shall use the notation  $\operatorname{ord}_P(a)$  for both  $a \in F$  and  $a \in *F$ , and both for prime ideals in F and for "infinite primes" P where the word "infinite" is used here in the sense of valuation theory, not in the sense of nonstandard arithmetic. In order to minimize confusion, we shall call such symbolic primes (places) from now on only archimedean, while the primes (places) which correspond to prime ideals will be called nonarchimedean replacing the terms infinite and finite of valuation theory in this context. (Observe that in nonstandard arithmetic it is just the finite primes that have a good claim to being called archimedean!) As for the "symbol"  $\infty$ , it is neither finite nor infinite in our sense but is a standard entity which is greater than any finite or infinite natural number in the enlargement since it was taken to be greater than any finite natural number in the standard framework.

By a surdivisor g in F, we mean a formal infinite product  $g = \prod P_{j}^{r_j}$ 

where  $P_j$  ranges over the standard archimedean and nonarchimedean primes and  $\nu_j$  may be any standard natural number or  $\infty$ . However, if  $P_j$  is archimedean, then we admit for  $\nu_j$  only the values 0 and  $\infty$ .  $\nu_j$  is the exponent of  $P_j$  in g and  $P_j$  occurs in g if  $\nu_j > 0$ . For F = Q we may replace  $P_j$  by the corresponding rational prime number  $p_j$  so that the surdivisors of Q in which the archimedean prime of Q does not occur may be regarded also as surnatural numbers. A surdivisor will be called a divisor if the number of primes which occur in it is finite, and if  $\nu_j \neq \infty$  for all nonarchimedean  $P_j$ . Surdivisors are multiplied by adding exponents. Divisibility, g.c.d., and l.c.m. are defined in the usual way.

Surdivisors are defined as standard entities which have a meaning relative to both F and \*F. Only such surdivisors will be considered. We observe, however, that the notion of divisibility and related notions which are defined in the next paragraph are not standard and not even internal.

Let  $a \in {}^*F$ . The surdivisor  $g = \prod P_j^{\nu_j}$  divides a if  $\operatorname{ord}_{P_j}(a) \ge \nu_j$  in case  $\nu_j$  is a natural number  $\nu_j \in N$ , and  $\operatorname{ord}_{P_j}(a)$  is an infinite natural number in case  $\nu_j = \infty$ . a is said to be *entire* for g if  $\operatorname{ord}_{P_j}(a) \ge 0$  for  $\nu_j \in N$  and  $\operatorname{ord}_{P_j}(a)$  is greater than some standard negative integer for  $\nu_j = \infty$ . For the given g, the ring  $F_g \subset {}^*F$  is then defined as the set of  $a \in {}^*F$  which are entire for g; and  $J_g \subset F_g$  is defined as the set of  $a \in {}^*F$  which are divisible by g. Then  $J_g$  is an ideal in  $F_g$ . Let  $K_g$  be the quotient ring  $F_g/J_g$ .

The following special cases are basic.

5.1. g=1, i.e.,  $\nu_j=0$  for all  $P_j$ . Then  $F_g=J_g=*F$  and so  $K_g=\{0\}$ .

5.2.  $g = P_j$  where  $P_j$  is a nonarchimedean prime, i.e.,  $\nu_j = 1$  and  $\nu_i = 0$  for all other  $P_i$ . Let  ${}^{\circ}F_{g}$  and  ${}^{\circ}J_{g}$  be, respectively, the restrictions of  $F_{g}$  and  $J_{g}$  to F. Then  ${}^{\circ}F_{g}$  is the valuation ring for the  $P_j$ -adic valuation  $V_{P_j}$  and  ${}^{\circ}J_{g}$  is the corresponding valuation ideal. It follows that  ${}^{\circ}F_{g}/{}^{\circ}J_{g}$  is a finite field of characteristic p where p is the rational prime number contained in  $P_j$ . But finite sets are not extended on passing from F to  ${}^{*}F$  and so

$$*({}^{\circ}F_{g}/{}^{\circ}J_{g}) = *({}^{\circ}F_{g})/*({}^{\circ}J_{g}) = F_{g}/J_{g} = K_{g}$$

is the same finite field of characteristic p.

5.3.  $g = P_j^{\nu_j}$  where  $P_j$  is a nonarchimedean prime and  $\nu_j$  is a natural number greater than 1 ( $\nu_i = 0$  for all other  $P_i$ ). We see, similarly as in 5.2, that  $K_g$  is now a finite ring of prime characteristic.

5.4.  $g = P_f^{\infty}$  where  $P_f$  is an archimedean or nonarchimedean prime (and  $\nu_i = 0$  for all other  $P_i$ ). In this case,  $F_g$  and  $J_g$  reduce to the ring  $F_0$  and the ideal  $F_1$  introduced at the beginning of this section. It follows that  $K_g$  is the  $P_f$ -adic completion of F if  $P_f$  is nonarchimedean,

or the field of real or of complex numbers if  $P_j$  is real or complex archimedean, respectively.

Now let  $g = \prod P_j^{\nu_j}$  be any surdivisor,  $g \neq 1$ . For any  $P_j$  which occurs in g, we call  $P_j^{\nu_j}$  a primary factor of g and we denote it by  $g_j$ . We regard  $g_j$  as a surdivisor in which  $\nu_i = 0$  for  $i \neq j$  and we write  $g = \prod g_j$  where j ranges only over the subscripts for which  $\nu_j > 0$ .

We are going to prove

5.5 THEOREM. For any ultra-power enlargement,  $K_g$  is isomorphic to  $\prod K_{g_i}$  where  $\prod$  indicates the strong direct product (strong direct sum).

PROOF. We may suppose that g possesses at least two distinct primary factors. For any primary factor  $g_j$  of g, we construct a homomorphism  $\alpha_j \colon K_g \to K_{g_j}$  as follows. Let  $h_j = \prod_{i \neq j} g_i$  so that  $g = g_j h_j$ . Then  $F_g = F_{g_j} \cap F_{h_j}$  and  $J_g = J_{g_j} \cap J_{h_j}$ . Put  $J'_{g_j} = J_{g_j} \cap F_g$  and  $J_{h_j}' = J_{h_j} \cap F_g$  so that  $J'_{g_j}$  are ideals in  $F_g$ .

We claim that  $(J'_{g_j}, J'_{h_j}) = F_g$ . That is to say, we assert the existence of a,  $b \in {}^*F$  such that a+b=1 where a and b are entire for g and, moreover,  $a \in J_{g_i}$  and  $b \in J_{h_j}$ . In order to find an appropriate a, we have to satisfy the conditions

$$5.6 ord_{P_i}(x) \ge \nu_i,$$

5.7 
$$\operatorname{ord}_{P_i}(x-1) \ge \nu_i$$
 for any other  $P_i$  occurring in g.

If  $\nu_j = \infty$  or  $\nu_i = \infty$  we now replace 5.6 and 5.7 by sequences of conditions,

5.8 
$$\operatorname{ord}_{P_j}(x) \ge 0$$
,  $\operatorname{ord}_{P_j}(x) \ge 1$ ,  $\cdots$ ,  $\operatorname{ord}_{P_j}(x) \ge n$ ,  $\cdots$ 
or

$$\operatorname{ord}_{P_{i}}(x-1) \geq 0, \operatorname{ord}_{P_{i}}(x-1) \geq 1, \cdots,$$

$$\operatorname{ord}_{P_{i}}(x-1) \geq n, \cdots,$$

respectively, where n ranges over all finite natural numbers. The approximation theorem of valuation theory shows that any finite number of conditions as in 5.8 and 5.9 can be satisfied already by some x in F. Using an appropriate concurrent relation, we may conclude that all conditions 5.6, 5.7, or if  $\nu_j$ ,  $\nu_i = \infty$ , 5.8, 5.9 can be satisfied simultaneously by some x = a in \*F. Since  $\operatorname{ord}_{P_i}(x-1) \ge \nu_i > 0$  implies  $\operatorname{ord}_{P_i}(x) \ge 0$ , we conclude that  $a \in F_g$ , while  $\operatorname{ord}_{P_j}(a) \ge \nu_j$  shows that  $a \in J_{g_i}$ . Hence  $a \in J'_{g_j}$ .

that  $a \in J_{g_i}$ . Hence  $a \in J'_{g_j}$ . Next we determine  $b' \in {}^*F$  such that x = b' satisfies the conditions  $\operatorname{ord}_{P_j}(x-1) \ge \nu_j$  while  $\operatorname{ord}_{P_i}(x) \ge \nu_i$  for all other  $P_i$ . This can again be done by means of an appropriate concurrent relation, and yields an x = b' which belongs to  $J'_{h_i}$ . Furthermore, if  $P_j$  is nonarchimedean,

$$\operatorname{ord}_{P_i}(a+b'-1) \geq \min(\operatorname{ord}_{P_i}(a), \operatorname{ord}_{P_i}(b'-1)) \geq \nu_i$$

while if  $P_j$  is archimedean, so that  $\nu_j = \infty$ , then at any rate  $\operatorname{ord}_{P_j}(a+b'-1) = \infty$  also. Similarly, for  $i \neq j$ ,  $\operatorname{ord}_{P_i}(a+b'-1) = \operatorname{ord}_{P_i}((a-1)+b') \geq \nu_i$  in all cases, and so  $a+b'-1 \in J_g$ . But  $J_g \subset J'_{h_j}$  and so  $b=b'-(a+b'-1)=1-a \in J'_{h_j}$  where a+b=1. This shows that  $(J'_{g_j}, J'_{h_j}) = F_g$ , i.e.,  $J'_{g_j}$  and  $J'_{h_j}$  are comaximal in  $F_g$ .

Now let c be any element of  $F_g$ . With a and b as above, put  $c_j = cb$ . Then  $c_j \in J'_{h_j}$  and  $c - c_j = c(a + b) - cb = ca \in J'_{g_j}$ . Suppose that some element  $c' \in F_g$  satisfies the same conditions as  $c_j$ , i.e.,

$$5.10 c' \in J'_{h_i}, c - c' \in J'_{g_i}.$$

Then  $c'-c_j \in J'_{h_j}$ ,  $c'-c_j \in J'_{g_j}$  and so  $c'-c_j \in J_g$ . Hence, denoting by  $\phi_j$  the canonical map from  $J'_{h_j}$  onto  $J'_{h_j}/J_g$ , we see that  $c \to \phi_j(c')$ , for c' satisfying 5.10, defines a mapping  $\psi_j$  from  $F_g$  into  $J'_{h_j}/J_g$ . It is not difficult to show that  $\psi_j$  is a homomorphism.

On the other hand,

$$J'_{h_j}/J_g = J_{h_j} \cap F_g/J_{h_j} \cap J_{g_j} = J_{h_j} \cap F_{g_j}/J_{h_j} \cap J_{g_j},$$

since  $J_{h_j} \cap F_g = J_{h_j} \cap F_{h_j} \cap F_{g_j} = J_{h_j} \cap F_{g_j}$ . We claim that  $J_{h_j} \cap F_{g_j}/J_{h_j} \cap F_{g_j}$  is isomorphic to  $F_{g_j}/J_{g_j} = K_{g_j}$ . Indeed, the cosets of  $J_{h_j} \cap F_{g_j}$  with respect to  $J_{h_j} \cap J_{g_j}$  are subsets of the cosets of  $F_{g_j}$  with respect to  $J_{g_j}$  and every coset of the latter class contains at most one of the former. Accordingly, it only remains to be shown that every coset of the second class contains at least one coset of the first class. Thus, given any  $f \in F_{g_j}$  we are required to find an  $f' \in J_{g_i}$  such that  $f - f' \in J_{h_j}$ . In other words, we have to show that there exists an x = f' which satisfies the conditions  $\operatorname{ord}_{P_j}(x) \geq \nu_j$ ,  $\operatorname{ord}_{P_i}(f-x) \geq \nu_i$  for any other  $P_i$ , and this can again be done by combining an application of the approximation theorem with the introduction of a suitable concurrent relation. Hence, if we map every coset of  $J_{h_j} \cap F_{g_j}$  on the coset of  $F_{g_j}$ , in which it is contained, we obtain an isomorphic mapping  $\chi_j$  from  $J'_{h_j}/J_g$  onto  $K_{g_j}$ . It follows that  $\lambda_j = \chi_j \psi_j$  is a homomorphic mapping from  $F_g$  into  $K_{g_j}$  and

$$\lambda: c \longrightarrow (\lambda_1(c), \lambda_2(c), \cdots, \lambda_j(c), \cdots),$$

where  $\lambda_j$  is included only for  $P_j$  which occur in g, is a homomorphic mapping from  $F_g$  into  $\prod K_{g_j}$ . The kernel of  $\lambda$  is the set  $\{c | \psi_j(c) = 0 \}$  for all  $P_j$  in g. For such  $P_j$  the corresponding c' (see 5.10) belongs to  $J_g$ . Hence  $c \in J_{g_j}$  for all appropriate  $g \cdot g$ , and so  $c \in J_g$ .

Accordingly,  $\lambda$  induces an injection  $\sigma$  of  $K_{\theta} = F_{\theta}/J_{\theta}$  into  $\prod K_{\theta j}$ . It remains to be shown that  $\lambda$  is a surjection. For this purpose we

employ, once again, the approximation theorem. Let  $(c_0, c_1, \cdots, c_j, \cdots)$  be an arbitrary element of  $\prod K_{g_j}$ . We have to find a  $c \in F_g$  such that  $\lambda_j(c) = c_j$ , i.e., we have to find a  $c \in F_g$  such that c is entire for g and  $\lambda_j(c) = c_j$ . Thus, for arbitrary  $d_j = \chi_j^{-1}(c_j) \in J'_{h_j}/J_g$ , we have to find  $c \in F_g$ , which is entire for g such that  $\phi_j(c) = d_j$ . Or, again, we may give  $c'_j \in J'_{h_j}$  arbitrarily (where  $d_j = \phi_j(c'_j)$ ) and we then have to find  $c \in F_g$  such that (compare 5.10)

5.11 
$$c - c'_i \in J'_{e_i}$$
 for all  $P_i$  which occur in  $g$ 

where c is entire for g. However, the last condition is now redundant since  $c'_i \in J'_{h_i} \subset F_g$  and  $J'_{g_i} \subset F_g$ , so any c which satisfies 5.11 must be entire for g and this is true even if we relax the condition  $c'_i \in J'_{g_i}$  and require only

$$c_1 \in F_a$$
.

In order to satisfy 5.11 subject to the condition 5.12 it is sufficient to find x = c, which satisfies

5.13 
$$\operatorname{ord}_{P_j}(x-c_j') = \infty \text{ for all } P_j \text{ in } g;$$

for since  $c'_j \subseteq F_g$ , we then have  $c-c'_j \subseteq F_g$  automatically and we certainly have  $\operatorname{ord}_{P_j}(c-c'_j) \ge \nu_j$ . Furthermore, we may replace 5.13 by sequences of conditions,

5.14 
$$\operatorname{ord}_{P_j}(x - c_i') \ge 0$$
,  $\operatorname{ord}_{P_j}(x - c_i') \ge 1$ ,  $\cdots$ ,  $\operatorname{ord}_{P_i}(x - c_i') \ge k$ ,  $\cdots$ 

where k ranges over the finite natural numbers.

At this point, we make use of our assumption that \*F is an ultrapower. It can then be shown [20] that for any sequence of internal entities  $\{S_n\}$  of the enlargement, with subscripts ranging over N, there exists an *internal* sequence  $T_n$  in \*F, n ranging over \*N such that  $S_n = T_n$  for all  $n \in N$ .

We range the conditions 5.14 in a simply infinite sequence with subscripts in N and we denote the  $P_j$ ,  $c_j'$ , and k which occur in the nth condition by  $P^{(n)}$ ,  $c^{(n)}$ , and  $k^{(n)}$ , respectively. Evidently each  $P_j$ ,  $c_j$ , and k will appear repeatedly in the sequence. We now consider the sequence of ordered triples  $S_n = (P^{(n)}, c^{(n)}, k^{(n)})$ ,  $n \in \mathbb{N}$ , and we extend it to an internal sequence  $\{T_n\}$  as above,  $n \in \mathbb{N}$ . The following sentence then holds in F, by virtue of the approximation theorem, for every finite or infinite m.

"There exists a  $\xi \in {}^*F$  such that  $\operatorname{ord}_{P^{(n)}}(\xi - c^{(n)}) \ge k^{(n)}$  for all  $n \le m$ ." For any infinite m, a corresponding  $x = \xi$  then satisfies all the conditions of 5.14. This completes the proof of Theorem 5.5.

Notice that we introduced the assumption that \*F is an ultrapower for the last part of our proof because the argument from concurrent relations applies in our present framework only to *standard* binary relations.

Consider in particular the surdivisors  $\gamma = \prod P_j^{\infty}$  where  $P_j$  ranges over all archimedean and nonarchimedean primes in F and  $\delta = \prod P_j^{\infty}$  where  $P_j$  ranges over the nonarchimedean primes only. We call these the adelic (the restricted adelic) surdivisors, respectively. Still supposing that we are dealing with an ultrapower enlargement, we know that  $K_{\gamma}$  ( $K_{\delta}$ ) is isomorphic to  $\prod K_{g_j}$  where  $g_j = P_j^{\infty}$  and  $P_j$  ranges over all primes (over all nonarchimedean primes) in F. Writing  $\phi$  for the isomorphism in question,  $\phi(K_{\gamma}) = \prod K_{g_j}$  or  $\phi(K_{\delta}) = \prod K_{g_j}$ , as the case may be, we then have for any  $c \in K_{\gamma}$  (for any  $c \in K_{\delta}$ )

$$\phi(c) = (c_0, c_1, \cdots, c_j, \cdots)$$

where  $c_i$  ranges over the P-adic and archimedean completions of F (over the P-adic completions only).

The adèle ring  $A_{\gamma}$  (the restricted adèle ring  $A_{\delta}$ ) is defined classically as the ring of elements  $(c_0, c_1, \dots, c_j, \dots) \in \prod K_{g_j}$  such that  $\operatorname{ord}_{P_j}(c_j) \geq 0$  for all but a finite number of j. Similarly, the idèle group  $I_{\gamma}$  (the restricted idèle group  $I_{\delta}$ ) is defined as the multiplicative group of elements of  $\prod K_{g_j}$  such that  $c_j \neq 0$  for all j and  $\operatorname{ord}_{P_j}(c_j) = 0$  for all but a finite number of j. Recalling that  $K_{\gamma} = F_{\gamma}/J_{\gamma}$  ( $K_{\delta} = F_{\delta}/J_{\delta}$ ), we write  $\mu_{\gamma}$  ( $\mu_{\delta}$ ) for the homomorphism  $F_{\gamma} \to \prod K_{g_j}$  ( $F_{\delta} \to \prod K_{g_j}$ ) with kernel  $J_{\gamma}$  ( $J_{\delta}$ ). For  $a \in F_{\gamma}$  ( $a \in F_{\delta}$ ) we then have  $\operatorname{ord}_{P_j}(a) \geq 0$  if and only if  $\operatorname{ord}_{P_j}(\mu_{\gamma}(a)) \geq 0$  for nonarchimedean  $P_j$  and  $\operatorname{ord}_{P_j}(a) \geq 0$  if and only if  $\operatorname{ord}_{P_j}(\mu_{\gamma}(a)) \geq 0$  for archimedean  $P_j$ .

The properties of adèles and idèles are reflected in the properties of their inverse images in  $F_{\gamma}$  and  $F_{\delta}$  by  $\mu_{\gamma}$  and  $\mu_{\delta}$  (compare [20] where the corresponding question is discussed for Dedekind rings). Let a be any element of  $F_{\gamma}$  ( $F_{\delta}$ ) such that  $a \neq 0$ . Then the entire or fractional ideal (a) can be written as a product of finite or infinite powers  $\operatorname{ord}_{Q_j}(a)$  of a finite or infinite number of prime ideals  $Q_j$  in \*F where the  $Q_j$  may be standard or nonstandard. However, for standard  $Q_j$  the exponent of  $Q_j$  cannot be negative infinite, since a belongs to  $F_{\gamma}$  (belongs If to  $F_{\delta}$ ). If  $\operatorname{ord}_{Q_j}(a)$  is finite for all standard  $Q_j$  and is zero for almost all such  $Q_j$ , then we call a Prüfer-finite. Then  $\mu_{\gamma}(a)$  ( $\mu_{\delta}(a)$ ) is an idèle (a restricted idèle) if and only if a is Prüfer-finite and  $\mu_{\gamma}(a)$  ( $\mu_{\delta}(a)$ ) is an idèle unit if and only if  $\operatorname{ord}_{Q_j}(a) = 0$  for all standard  $Q_j$ , i.e., if a has nonstandard prime ideal factors only. Thus, for standard a,  $\mu_{\gamma}(a)$  and  $\mu_{\delta}(a)$  are idèle units if and only if a is a unit (invertible algebraic integer) in \*F.

Now let A be a standard entire ideal in F, so that A is the cor-

responding ideal in \*F. Then \*A has a two element basis, \* $A = (\alpha, \beta)$ where  $\alpha$  and  $\beta$  are algebraic integers in \*F and where  $\beta$  may be any arbitrary nonzero element of \*A. In particular, we may choose a  $\beta \neq 0$  which is divisible by the restricted adelic surdivisor  $\delta$ . Then  $\mu_{\delta}(\beta) = 0$ , while  $\alpha \in F_{\delta}$  since  $\alpha$  is an integer. Hence,  $\mu_{\delta}(*A) = \mu_{\delta}(\alpha)$ , and so \*A corresponds to a principal ideal in  $\prod K_{q_i}$  (as is also evident from the theory of idèles). It follows that  $\operatorname{ord}_{P_i}(A) = \operatorname{ord}_{P_i}(\alpha)$  for all standard prime ideals  $P_i$  and there exists an entire ideal B in \*F such that  $*AB = (\alpha)$  where B is divisible only by nonstandard prime ideals. This shows, incidentally, that to every class \*C of ideals (multiplicative coset of principal ideals) in \*F and to every preassigned finite set of standard prime ideals S, there exist entire ideals in \*F which are not divisible by any ideal in S. Indeed, we only have to take the standard ideal \*A as a representative of the class  $C^{-1}$ , then the above B is an ideal of the required type. And since our conclusion holds for \*F, it holds also in F, by the usual argument for transferring conclusions from F to \*F and vice versa. In this case, however, only the argument is of interest, since the result is a simple consequence of the classical theory.

To sum up the results of the present section, we have seen that the fields and rings which are commonly associated by the theory of valuations with a given algebraic number field can all be obtained by a uniform procedure as homomorphic images of internal or external (noninternal) subrings of \*F.

6. Class field theory. Up to this point, we have used enlargements, in a sense, only as auxiliary concepts, that is to say, we have shown how they can be employed in the construction and investigation of classical theories. We shall now consider a situation in which a classical theory is known to fail in the standard model but can still be carried out in an enlargement. This situation occurs in the class field theory of infinite abelian extensions and was in fact the occasion for the introduction of idèles by Chevalley [2], although not their only justification. To quote the example pointed out by Chevalley, let F = Q be the field of rational numbers and, for a given prime number  $p \ge 3$ , let  $F_n = F(\zeta_n)$  where  $\zeta_n$  is a primitive  $p^n$ th root of unity. Also, let  $F_{\infty} = \bigcup_{n} F_{n}$ . In order to define the class group for  $F_{n}$  in accordance with the standard precept, we introduce  $Q_0$  as the multiplicative group of rational numbers prime to p and entire for p, and  $I_n$  as the subgroup of  $Q_0$  which is given by  $I_n = \{q \mid q \equiv 1(p^n)\}$ . Then the multiplicative quotient group  $Q_0/I_n$  is the class group of  $F_n$ . By analogy with the finite case, we might now expect  $Q_0/\bigcap_n I_n$  to be the class group of  $\bigcup_n F_n$ , but this conclusion is spurious since  $\bigcap_n I_n = \{1\}$ .

For any finite algebraic extension of the rationals Q, as in §5, let

 $g=\prod P_j^{\nu_j}$  be a surdivisor in F. An entire or fractional internal ideal A in F is called *entire for* g if  $A\neq 0$  and if  $\operatorname{ord}_{P_j}A\geq 0$  for all non-archimedean primes  $P_j$  which occur in g. Notice that if  $\nu_j$  is infinite for some nonarchimedean  $P_j$  in g, then  $a\in F$  may be entire for g according to the definition of the previous section which was introduced relative to the valuation ring  $F_{\nu_j^n}$ , although A=(a) is not entire for g according to our present definition. A is called *prime for* g if  $A\neq 0$ , and if for any nonarchimedean  $P_j$  which occurs in g,  $\operatorname{ord}_{P_j}A \leq 0$ .

We define the ray modulo g,  $R_g$ , as the subset of \*F whose elements a are defined by the following conditions. If  $P_j^{\nu_j}$  is a primary factor of g and  $P_j$  is nonarchimedean, then a-1 is divisible by  $P_j^{\nu_j}$ ; while if  $P_j$  is real archimedean then a>0 in the corresponding embedding of \*F in the enlargement of the real numbers, \*R; and (to provide for a trivial case)  $a \neq 0$ .  $R_g$  is a multiplicative group. We denote by  $I_g$  the corresponding ideal ray group, i.e., the group of principal ideals (a) in \*F such that  $a \in R_g$ .

Now let m be a divisor in F, where we recall that a surdivisor is called a divisor if the number of its primary factors  $P_j^{\nu_j}$  is finite and if at the same time  $\nu_j = \infty$  only for archimedean  $P_j$ . To m, there corresponds an ideal ray group  $J_m$  in F, in the classical sense, where  $J_m$  consists of the ideals  $A \neq 0$  in F such that A = (a) for some  $a \in F$  that satisfies  $\operatorname{ord}_{P_j}(a-1) \geq \nu_j$  for all nonarchimedean  $P_j$  occurring in m, and a > 0 for the order corresponding to any real archimedean  $P_j$  in m. It is not difficult to see that  $I_m = {}^*J_m$ . Standard class field theory assigns to  $J_m$  an abelian normal extension  $F_m$  of F as its class field.  $F_m$  is unique up to isomorphism and hence is determined uniquely if we require  $F_m \subset \overline{F}$  where  $\overline{F}$  is a fixed algebraic closure of F. For any surdivisor  $F_m$  we now define the class field for  $F_m$ , as the compositum of all fields  $F_m \subset \overline{F}$  as  $F_m$  ranges over the divisors of  $F_m$  such that  $F_m$  (For  $F_m$ ), the notations  $F_m$  and  $F_m$  are consistent.)

Let h be any internal divisor in  ${}^*F$ ,  $h = \prod Q_j^{\mu_j}$  where, by the definition of a divisor in  ${}^*F$ ,  $Q_j$  ranges over the primes of  ${}^*F$ , and the set of  $Q_j$  for which  $\mu_j \neq 0$  is starfinite. Moreover,  $\mu_j$  may now be a finite or infinite natural number or  $\infty$ , but the latter case is possible only if  $Q_j$  is archimedean. In general,  $Q_j$  may be standard or nonstandard internal, but if  $Q_j$  is archimedean then it must be standard since the set of archimedean primes in F is finite and, accordingly, is not enlarged on passing to  ${}^*F$ . If  $Q_j$  is standard then we may write  $Q_j = {}^*P_j$  for some prime  $P_j$  in F and there is no essential limitation in assuming that the subscript (j) is the same on both sides. Let  ${}^*g$  be the injection of a surdivisor g into the enlargement (where we append the star in

order to avoid misunderstandings). For example, if  $g = P_j^{\infty}$  then  $*g = *P_j^{\infty}$ . Suppose that  $P_j$  is nonarchimedean and let h be the divisor  $h = *P_j^{\omega}$  where  $\omega$  is an infinite natural number. Then the standard definition of divisibility, when transferred to the enlargement, forces us to conclude that  $h \mid *g$  but not  $*g \mid h$  in \*F. On the other hand, consider any  $a \in *F$  such that  $\operatorname{ord}_{P_j}(a) = \omega - 1$ . By our definition of divisibility by surdivisors,  $g \mid a$  but not  $h \mid a$ . In order to cope with this discrepancy we need a new notion of divisibility of a divisor by a surdivisor. We shall say that the surdivisor  $g = \prod P_j^{\nu_j}$  surdivides the divisor  $h = \prod Q_j^{\nu_j}$  if for any finite natural  $\nu_j$  and  $Q_j = *P_j$  we have  $\mu_j \geq \nu_j$  (including the possibility that  $\mu_j = \infty$ ); while if  $\nu_j = \infty$ , then  $\mu_j$  is an infinite natural number, or  $\mu_j = \infty$ . We denote this relation by  $g \mid h$ . It holds in the special case considered above although  $*g \mid h$  does not hold in that case. If, however, h is a standard divisor then  $g \mid h$  only if  $*g \mid h$ .

For any surdivisor in F there exists a divisor h in \*F which is surdivisible by g. In order to see this, range all standard  $P_j$  in a sequence with subscripts in N, beginning with the archimedean primes. Put

6.1 
$$g_k = P_0^{\nu_0(k)} P_1^{\nu_1(k)} \cdots P_k^{\nu_k(k)}, \qquad k = 0, 1, 2, \cdots$$

where  $\nu_j(k) = \nu_j$  if  $\nu_j$  is a natural number,  $\nu_j(k) = \infty$  if  $\nu_j = \infty$  and  $P_j$  is archimedean and  $\nu_j(k) = k$  if  $\nu_j = \infty$  and  $P_j$  is nonarchimedean. Then the  $g_k$  are divisors in F. Passing to the enlargement and putting  $h = g_\omega$  for arbitrary infinite  $\omega$ , we see that h is a divisor in \*F. It is not difficult to verify that g || h, for if  $\nu_j = \infty$  and  $P_j$  is nonarchimedean then  $\nu_j(\omega) = \omega$ .

Applying the standard theory to a divisor h in F, we obtain an ideal ray group  $J_h$  and a class field  $F_h$  of  $J_h$  where  $F \subset F_h$  and where we may suppose that  $F_h \subset \overline{F}$ . Let  $F_h = F_h \cap \overline{F}$ , then  $F_h = F_h \cap \overline{F}$ , then  $F_h = F_h \cap \overline{F}$ , then  $F_h = F_h \cap \overline{F}$ , which are standard.

If g is a surdivisor and \*g||h then  $J_h \subset I_g$ . In that case, also,  ${}^{\circ}F_h \supset F_g$  where  $F_g$  is the class field of g, as before. For let  $\alpha \in F_g$ , then  $\alpha$  belongs to the compositum of a finite number of fields  $F_{m_1}, \dots, F_{m_k}$  corresponding to divisors  $m_1|g, \dots, m_k|g$ . It follows that  $\alpha \in F_m$  where m is the l.c.m. of  $m_1, \dots, m_k$ . But m|g with g||h entails \*m|h in the enlargement and so  $F_m \subset *F_m = F_{*m} \subset F_h$ . Hence  $\alpha \in {}^{\circ}F_h$ ;  $F_g \subset {}^{\circ}F_h$  as asserted.

Let H be the intersection of the fields  ${}^{\circ}F_h$  as h ranges over the divisors which are surdivided by g. We claim that  $H = F_g$ .

Since we have already shown that  $F_h \supset F_g$  for g || h, it follows that  $H \supset F_g$ . It only remains for us to establish inclusion in the opposite direction. Let  $\alpha \in H$ , then  $\alpha \in F_h$  for any h such that g || h. Also, in the notation of 6.1 above,  $g || g_k$  for all infinite natural numbers k and so  $\alpha \in F_{g_k}$  for all infinite k. But  $\{F_{g_k}\}$  is an internal sequence and so we may conclude that  $\alpha \in F_{g_k}$  also for sufficiently large finite k. Now, for all finite k,  $g_k || g$  and so  $F_{g_k} \subset F_g$ . Hence  $\alpha \in F_g$ , as asserted.

Let  $\Gamma_g$  be the Galois group of  $F_g/F$ . For any divisor h which is surdivided by g as before, let  $\Gamma_h$  be the Galois group of  $F_h/*F$ . Let  $C_h$  be the group of ideals in \*F which are entire and prime for h, then  $J_h \subset C_h$ . Moreover, there is a homomorphism from  $C_h$  onto  $\Gamma_h$ , with kernel  $J_h$ , which is given by the Artin symbol

$$Q \to \sigma = \left(\frac{F_h/^*F}{O}\right), \quad Q \in C_h, \quad \sigma \in \Gamma_h.$$

Let  $\phi$  be the canonical mapping from  $\Gamma_h$  to  $\Gamma_g$  with kernel K where K consists of the  $\sigma \in \Gamma_h$  that leave the elements of  $F_g \subset F_h$  invariant. K is not necessarily internal. The mapping  $\phi$  is onto, since every automorphism of  $F_g$  over F can be extended to an automorphism of  $F_h$  over F which can then be extended to an automorphism of  $\overline{F}$  over F. On passing to the enlargement, this in turn can be extended to an internal automorphism of  $F_g$  over  $F_g$ , and then restricted to an automorphism of  $F_h$  over  $F_g$ . Further restriction to  $F_g$  and then to  $F_g$  leads us back to the original automorphism, which therefore belongs to the range of  $F_g$ .

Let  $C_g$  be the group of ideals in \*F which are entire and prime for g. We define a generalized Artin symbol to indicate a mapping from  $C_g$  to  $\Gamma_g$  by

$$Q \to \sigma = \left(\frac{F_g/F}{Q}\right) = \phi\left(\frac{F_h/^*F}{Q}\right)$$

for all ideals  $Q \in C_q$ . The mapping is onto, since  $\phi$  is onto.

We claim that this definition is independent of our particular choice of h (provided g||h, as above). Indeed, let k be any other divisor such that g||k. We may suppose that h|k, for if this is not the case from the outset we may then prove that we obtain the same interpretation of the generalized Artin symbol by taking the g.c.d. of h and h as we do by taking h or h.

Suppose that g||h and h|k and hence g||k. If  $C_k$  is the group of ideals of F which are entire and prime for k, we then have  $I_g \supset J_h \supset J_k$  and  $C_g \supset C_h \supset C_k$  and  $F_g \subset F_h \subset F_k$ . Also, if  $\Gamma_k$  is the Galois group of

 $F_k/^*F$  and  $\phi'$  is the canonical mapping from  $\Gamma_k$  to  $\Gamma_g$  (corresponding to  $\phi$  for h) and  $\psi$  is the mapping from  $\Gamma_k$  to  $\Gamma_h$  whose kernel consists of the automorphisms in  $\Gamma_k$  that leave the elements of  $F_h$  invariant, then  $\phi' = \phi \psi$ . Now let Q be any prime ideal in  $C_k$  with norm NQ. Then if

$$\sigma = \left(\frac{F_k / *F}{O}\right)$$

we have, for all  $\alpha \in F_h$ ,

$$6.2 \sigma\alpha \equiv \alpha^{NQ}(Q).$$

But the same condition is satisfied by the restriction of  $\sigma$  to  $F_h$ , i.e., by  $\psi \sigma$ , and so

$$\left(\frac{F_h/^*F}{O}\right) = \psi\left(\frac{F_k/^*F}{O}\right).$$

Hence

$$\phi\left(\frac{F_{k}/^{*}F}{Q}\right) = \phi\psi\left(\frac{F_{k}/^{*}F}{Q}\right) = \phi'\left(\frac{F_{k}/^{*}F}{Q}\right),$$

which shows that our definition of the generalized Artin symbol is independent of the particular choice of h, if Q is a prime ideal. The general result now follows from the multiplicativity of the symbol.

Let e be the identity in  $\Gamma_g$ , while  $I_g$  is the ideal ray group of g as introduced previously. We claim that for any  $Q \in C_g$ ,  $Q \in I_g$  if and only if

$$\left(\frac{F_g/F}{O}\right) = e.$$

To see this, observe that

$$\left(\frac{F_h/^*F}{Q}\right)$$

is the identity in  $\Gamma_{\gamma}$  if and only if  $Q \in J_h$ . Now suppose  $Q \in I_g$  so that Q = (q) where  $q \in R_g$ . Take  $h = \prod Q_i^{\mu_i}$  where  $\mu_i = \operatorname{ord}_{Q_i}(q-1)$  for any nonarchimedean  $Q_i$  and  $\mu_i = \infty$  for any archimedean  $Q_i$  which occurs in g. Then g || h and  $Q \in J_h$ , and hence

$$\left(\frac{F_h/^*F}{Q}\right) = e$$

and so

$$\left(\frac{F_o/F}{Q}\right) = \epsilon.$$

Conversely, suppose that

$$\left(\frac{F_g/F}{O}\right) = e$$

but that  $Q \in I_g$ . Let  $\{g_k\}$  be the sequence defined by 6.1.  $\{g_k\}$  is internal and  $g || g_k$  for all infinite k. It follows that, for such k,  $Q \in I_{g_k}$ . Hence,  $Q \in I_m$  where  $m = *g_k$  for sufficiently large finite k, and so

$$\left(\frac{F_m/F}{O}\right) \neq e.$$

On the other hand,  $m \mid g$  and so another argument involving 6.2, applied this time to  $\alpha \in F_m$ , shows that

$$\left(\frac{F_m/F}{O}\right) = e$$

in  $\Gamma_m$ , a contradiction which proves our assertion.

We have now shown that  $I_{g}$  is the kernel of the homomorphism provided by the generalized Artin symbol. Thus, the symbol induces an isomorphism between  $C_{g}/I_{g}$  and  $\Gamma_{g}$ ,  $C_{g}/I_{g} \simeq \Gamma_{g}$ , as one would like to expect of a class field. The isomorphism also provides a correspondence between the subfields of  $F_{g}$  on one hand and certain subgroups of  $C_{g}/I_{g}$  on the other hand via the Galois group  $\Gamma_{g}$ . Thus the subgroups of  $C_{g}/I_{g}$  which appear in this correspondence are just those that are closed in the Krull topology.

Suppose in particular that  $g = \gamma$ , where  $\gamma$  was defined in the preceding section, although the complex archimedean factors of  $\gamma$  are now irrelevant. Then  $F_{\gamma}$  is the compositum of all abelian extensions of F, i.e., it is the maximal abelian extension of F over F. The group F now consists of all principal ideals (a) such that F is totally real and F is divisible by F or some infinite natural number F or The group F can also be expressed in terms of the idèles of F. However, the discussion of this and other topics which are evidently still required in order to complete the picture must be left for another occasion (compare [21]).

While in the present section we have made effective use of infinite prime numbers or nonstandard prime ideals as elements of fields or of multiplicative groups, they have not, so far, occurred as divisors or as characteristics of fields. A simple application of infinite prime numbers in this direction is as follows (see [16]). Suppose that a sentence X which is formulated in the Lower Predicate Calculus in terms of equality, addition, and multiplication is false for fields of arbitrarily high characteristic. Thus, the statement "for every natural number n there exists a prime number p > n such that X is false in a field of characteristic p" is true for the standard natural numbers and hence is true also in an enlargement. Choosing n infinite, we see that there is a field F of infinite characteristic p such that X is false in F. But when looked at from the outside, F is actually of characteristic 0 since it is not of any finite characteristic. We have proved the well-known result that if X is true for all fields of characteristic 0 then it is also true for all fields of characteristic  $p > p_0$  where  $p_0$  depends on X.

A much deeper result which can be stated readily in terms of infinite primes is the famous theorem of Ax and Kochen. Let  $F_p$  be the prime (minimal) field of infinite prime characteristic p and let  $F_p\{x\}$  be the field of formal power series of x adjoined to  $F_p$  within an enlargement. Thus, the subscripts of a series  $\sum_{n=-q}^{\infty} a_n x^n \in F_p\{x\}$  range over the nonstandard integers of the enlargement. Let  $\overline{F}_p$  be the field of p-adic numbers in the same enlargement. Then  $F_p\{x\}$  is elementarily equivalent to  $\overline{F}_p$  with respect to the standard language of the Lower Predicate Calculus with a vocabulary for the field operations and for valuation in an ordered group. This is a rather elegant reformulation of the Ax-Kochen result, but the available methods of proof are based either on model theoretic methods [1] or on the elimination of quantifiers [3]. It would be interesting to handle the problem effectively by nonstandard methods.

7. Concluding remarks. As we have seen, our methods offer, in many cases, alternatives to familiar infinitary constructions and passages to the limit. It is quite likely that at some future date a deeper understanding of the structure of definitions and proofs will enable us to provide systematic translations from one framework to the other. And we may recall here that already Pascal and Leibniz maintained that the respective infinitesimal methods employed by them differed from the Greek method of exhaustion only in the manner of speaking. Coming next to the mathematician's desire for obtaining an intuitive picture of his universe of discourse, the use of ultrapowers as representations of enlargements is entirely appropriate, although even this does not lead to a categorical (unique) enlargement except by means of artificial restrictions. Beyond that, the use of ultrapowers (see Theorem 5.5) or of other special models (see Luxemburg's result quoted in §3 above) may actually be required in order to prove particular propositions.

As far as the results of the present paper on algebraic number fields are concerned, the argument at the end of §3 shows that they all remain true in an ultrapower on a countable index set for a free ultrafilter. Within this framework, the infinite numbers and ideals may be regarded as just another kind of limit. Moreover, the procedure by which we obtain an ultrapower  $F_D^N$  from a countable direct product of fields  $F^N$  can be combined into a single step with the further homomorphisms  $F_0 \rightarrow F_0/F_1$  onto various completions of F. In particular, we may thus obtain the real numbers R by taking a countable direct power of the rational numbers  $Q^N$  and a free ultrafilter D on N. An element  $q = \{q_n\} \in Q^N$  will be called *finite* if there exists a rational number r such that  $\{n \mid |q_n| < r\} \in D$ . Let  $Q_0$  be the set of finite elements of  $Q^N$ ; then  $Q_0$  is a subring of  $Q^N$ . Let  $Q_1$  be the set of infinitesimal elements of  $Q^N$ , i.e., of elements  $q = \{q_n\}$ , such that  $\{n \mid |q_n| < r\}$  $\in D$  for the positive rational numbers r. Then  $Q_1 \subset Q_0$  and  $Q_1$  is an ideal in  $Q_0$ . The quotient ring  $Q_0/Q_1$  is isomorphic to the field of real numbers. In this way we obtain a procedure which bears a general similarity to the method of completion by Cauchy sequences but is quite different from it in detail.

On the other hand, it would seem wasteful to give up the logical basis of our method altogether, for it alone provides the setting within which we may deduce the validity of statements in  ${}^*M$  quite generally from their validity in M and vice versa. Without this setting, any property which is known to apply to M has to be established for  ${}^*M$  separately in each case, and while this is certainly possible it has been contrary to good mathematical practice ever since the days of Theaetetus.

It may be too early to say whether the methods of Nonstandard Analysis will ever become accepted (or "standard") tools of mathematics. At any rate, it is remarkable that an idea which once formed the basis for most of the work in the Differential and Integral Calculus and which was declared bankrupt one hundred years ago (after a long but admittedly fraudulent career) has, after all, enough vitality to make a meaningful contribution to a subject as far removed from its origins as the theory of algebraic number fields.

## BIBLIOGRAPHY

- 1. J. Ax and S. Kochen, *Diophantine problems over local fields*, Amer. J. Math. 87 (1965), 605-630, 631-698.
- 2. C. Chevalley, Généralisation de la théorie du corps de classes pour les extensions infinies, J. Math. Pures Appl. (9) 15 (1936), 359-371.
  - 3. P. J. Cohen, Decision procedures for real and p-adic fields, Unpublished.

- 4. T. Frayne, D. C. Morel and D. S. Scott, Reduced direct products, Fund. Math. 51 (1962), 195-227.
- 5. D. K. Harrison, Finite and infinite primes for rings and fields, Mem. Amer. Math. Soc. No. 68 (1966).
- 6. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, Klassenkörpertheorie, Jber. Deutsch. Math.-Verein. 35 (1926), 1-66; 36 (1927), 233-311.
- 7. L. Henkin, The completeness of the first order functional calculus, J. Symbolic Logic 14 (1949), 159-166.
- 8. H. J. Keisler, *Ultraproducts and elementary classes*, Proc. Roy. Acad. Sci. Amsterdam Ser. A 64 (1962), 477-495.
- 9. J. G. Kemeny, Undecidable problems of elementary number theory, Math. Ann. 135 (1958), 160-169.
- 10. S. Kochen, Ultraproducts in the theory of models, Ann. of Math. (2) 79 (1961), 221-261.
- 11. W. Krull, Galoissche Theorie unendlicher algebraischer Erweiterungen, Math. Ann. 100 (1928), 678-698.
  - 12. S. Lang, Rapport sur la cohomologie des groupes, Benjamin, New York, 1966.
- 13. W. A. J. Luxemburg, A new approach to the theory of monads, Symposium on Applications of Model Theory to Analysis and Algebra, Pasadena, May 1967, (to appear).
- 14. R. MacDowell and E. Specker, *Modelle der Arithmetik*, Infinitistic Methods (Symposium on Foundations of Mathematics, Warsaw, 1959), Państwowe Wydawnictwo Naukowe, Warsaw, 1961, pp. 257–263.
- 15. E. Mendelson, On non-standard models for number theory, Essays on the Foundations of Mathematics (Fraenkel anniversary volume), Magnes Press, Jerusalem, 1961, pp. 259–268.
- 16. A. Robinson, Les rapports entre le calcul déductif et l'interprétation sémantique d'un système axiomatique, Colloques Internationaux du Centre National de la Recherche Scientifique, No. 36, Paris, 1953, pp. 35-52.
- 17. ——, Model theory and non-standard arithmetic, Infinitistic Methods (Symposium on Foundations of Mathematics, Warsaw, 1959), Państwowe Wydawnictwo Naukowe, Warsaw, 1961, pp. 265–302.
- 18. ——, Non-standard analysis, Studies in Logic and the Foundations of Mathematics, North-Holland, Amsterdam, 1966.
- 19. ——, A new approach to the theory of algebraic numbers, Accad. Naz. Lincei Rend. (8) 40 (1966), 222–225, 770–774.
- 20. ——, Non-standard theory of Dedekind rings, Proc. Roy. Acad. Sci., Amsterdam, (to appear).
- 21. ——, Non-standard algebraic number theory, Symposium on Applications of Model Theory to Analysis and Algebra, Pasadena, May 1967, (to appear).
- 22. J.-P. Serre, Cohomologie Galoisienne. Lecture Notes in Mathematics No. 5, Springer, Berlin, 1964.
- 23. T. Skolem, Über die Nichtcharakterisierbarkeit der Zahlenreihe mittels endlich oder unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen, Fund. Math. 23 (1934), 150-161.

University of California, Los Angeles, and Yale University