be used to refute this proposal; as in [4].) But on the borderline of game theory, in the subject of so-called Borel games, the use of uncountably many iterations of the power set operation has turned out to be demonstrably essential for solving problems about **R** (at least, if 'subsystems' of set theory are to be used, as in Martin's proof of the determinateness of all Borel games [Ann, of Math. (2) 102 (1975), 363-371]). Of course, this is a far cry from number theory and from those 'extravagantly' large cardinals which Gödel had in mind. (iii) To supplement the text where (a) spectacular uses of the skeptical, and (b) modest uses of the speculative tradition are given: (a') in physics, the atomic theory is the standard example of a success fitting into the speculative tradition (atoms being hardly much more plausible than ghosts, from ordinary experience); in mathematics, nonconstructive methods. (b') Modest uses abound of course; cf., for example, my review of Brouwer's work in 83 (1977) of this Bulletin (around p. 88).

Remark. It cannot have escaped the reader's notice that there is no counterpart in current foundations to what is surely the most glaring difference between modern natural science and the early speculations referred to in (i): the skillful use of a massive amount of empirical data. Certainly the history of mathematics-not, of course, mere snippets as in (i)-(iii) above-would seem to provide, at present, the most obvious source of empirical data for the general questions behind t.f., and, in particular, for a scientific study of Bourbaki's 'intuitive resonances' (in [1]). Of course, precautions are needed against overliteral interpretations of the data (cf. end of [2] about misplaced textual criticism) and artifacts (cf. Remark (ii) in [8]); as in all sciences, only more so because here the influence of the observer on the observation is particularly strong. The use of statistical data, as in [9], over long periods provides one way of taking precautions. It may well be that this historical perspective would be bad for mathematical practice (with busybodies drawing premature 'practical' conclusions from ill-digested data). But in the reviewer's opinion it is certainly good for foundational research, specifically, for opening up this subject to (genuine) problems raised by recent computer-assisted proofs: (a) Historically-and scientifically, if not artistically-speaking, such proofs, for example, of the 4-color conjecture, involve incomparably more progress than, say, the use of large cardinals in (ii) above. Compare the effort which would be needed to explain large cardinals to Archimedes with getting him to understand, let alone put together the largish computer used by Haken and Appel (and compare the general interest of the four color conjecture with that of Borel determinacy). (b) There are genuine doubts about the reliability of computer-aided proofs not resolved by the particular idealizations of reliability, that is, the doctrines of rigor in various branches of t.f. Inasmuch as reliability is a principal topic of foundations, these new proofs present novel data for foundations: it would seem premature (to put it mildly) to assume that these new data are less fundamental than the matters of 'principle' stressed in t.f.

BULLETIN OF THE G. KREISEL

AMERICAN MATHEMATICAL SOCIETY Volume 84, Number 1, January 1978 © American Mathematical Society 1978

The theory of numbers, S. Iyanaga, ed., (translated by K. Iyanaga), North-Holland, Amsterdam; American Elsevier, New York, 1975, xi + 541 pp., \$51.95.

The Legendre symbol $(\frac{a}{p})$ is defined for any odd prime p and any rational integer a that is not divisible by p. It is equal to +1 or to -1 according as the congruence $x^2 \equiv a \mod p$ does or does not have a solution in the ring of rational integers \mathbf{Z} . The quadratic law of reciprocity then states that the equations

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(-1\right)^{(p-1)/2 \cdot (q-1)/2}$$

and

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

hold for distinct odd primes p and q. In particular the law tells us how p's being a square mod q is related to q's being a square mod p. While the law was known to Legendre, it was first proved completely by Gauss in the 1790s and published in his *Disquisitiones arithmeticae* in 1801.

The quadratic reciprocity law is a special case of the Hilbert reciprocity law (1890s). Here I will use the language of the p-adic numbers which were not invented until some years later. For each prime p the p-adic numbers \mathbf{Q}_p are the completion of the field of rational numbers \mathbf{Q} with respect to the distance function $|\alpha - \beta|_p$ provided by the valuation $|\alpha|_p = 1/p'$ obtained by writing $\alpha = p'm/n$ with m and n prime to p. Then \mathbf{Q}_p can be made into an extension field of Q with an extended valuation $| \cdot |_p$. This construction parallels the construction of the real numbers **R** which, in number theory, are denoted \mathbf{Q}_{∞} with absolute value $| |_{\infty}$. In this way one obtains fields $\mathbf{Q}_2, \mathbf{Q}_3, \mathbf{Q}_5, \ldots, \mathbf{Q}_{\infty}$ which are completions of Q under essentially all the valuations that Q can possess. The valuation $|\cdot|_p$ is also written p with p either a prime or ∞ . There are two underlying principles in the use of all these fields. The first is that number theory is considerably easier in the Q_p 's than in Q itself; for example, if p is a finite valuation, then \mathbf{Q}_p is, so to speak, just one notch above the finite field \mathbf{F}_p with which it is naturally related, the passage from \mathbf{F}_p to \mathbf{Q}_p being provided by a process called Hensel's lemma. The second is that all the \mathbf{Q}_{p} 's, taken collectively, tell us a lot about \mathbf{Q} . Sometimes a statement is valid over \mathbf{Q} if and only if it is valid over all \mathbf{Q}_p , and when this happens we say that the Hasse principle holds. For example, every quadratic form in 3 variables over \mathbf{F}_{p} represents 0 (easy); this can be lifted to \mathbf{Q}_{p} where every quadratic form in 5 variables represents 0 (not hard); finally there is a Hasse principle, i.e. a quadratic form over Q represents 0 if and only if it does so in all Q_p including ∞ (hard). Situations in \mathbf{Q}_p are called local, those in \mathbf{Q} global. To what extent, then, is a global situation described by all the local situations taken together?

To get back to the Hilbert reciprocity law-it says that the product of Hilbert symbols over all p is 1, i.e.

$$\prod_{p=2}^{\infty} \left(\frac{\alpha, \beta}{p} \right) = 1$$

for α , β in $\dot{\mathbf{Q}}$ where the Hilbert symbol $(\alpha, \beta/p)$ is, by definition, equal to +1 or to -1 according as the equation $\alpha x^2 + \beta y^2 = 1$ does or does not have a solution in \mathbf{Q}_p . Almost all Hilbert symbols in the formula turn out to be 1 so there is no question of convergence.

Now consider an algebraic number field F, i.e. a finite extension field of \mathbf{Q} . In algebraic number theory F takes the place of \mathbf{Q} , and F contains a ring \mathfrak{o} , its ring of algebraic integers, which takes the place of \mathbf{Z} . Each valuation p on \mathbf{Q} has a finite number of extensions to valuations \mathfrak{p} on F. In this way one obtains an infinite number of finite valuations, and a finite number of infinite valuations, on F. The set of all these valuations is written Ω . Local situations occur in the completions $F_{\mathfrak{p}}$, global ones in F. Hilbert's reciprocity law becomes

$$\prod_{\mathfrak{p}\in\Omega}\left(\frac{\alpha,\,\beta}{\mathfrak{p}}\right)=1$$

in F, the quantities involved being defined essentially as they were for Q.

Hilbert's ninth problem (1900) called for a law of reciprocity in any algebraic number field. "For any field of numbers the law of reciprocity is to be proved for the residues of the lth power, when l denotes an odd prime, and further when l is a power of 2 or a power of an odd prime. The law, as well as the means essential to its proof, will, I believe, result by suitably generalizing the theory of the field of the lth roots of unity, developed by me, and my theory of relative quadratic fields." This was completed by Takagi in the early 1920s and Artin in the late 1920s, for abelian extensions of algebraic number fields, i.e. in a more general context that will be described in a moment. Here an abelian extension will be a finite extension with an abelian galois group.

Our concepts at the moment are inadequate for the formulation of the general reciprocity law, but we get a clue as to what they should be by reinterpreting the Hilbert reciprocity law in a certain way. Consider α , β in \mathbf{Q} with β a nonsquare in \mathbf{Q} . Let E be the quadratic extension $E = \mathbf{Q}(\sqrt{\beta})$ of \mathbf{Q} . So the galois group \mathfrak{g} of E/\mathbf{Q} is a group of two elements. Write them $\{1, \sigma\}$. This group \mathfrak{g} , not just any group of two elements, is to be the target of the Hilbert symbol! Consider a valuation p of \mathbf{Q} . For the sake of discussion, suppose β is not a square in \mathbf{Q}_p . The galois group \mathfrak{g}_p of $\mathbf{Q}_p(\sqrt{\beta})/\mathbf{Q}_p$ is also a group of order two, it can be naturally imbedded in \mathfrak{g} , and its elements can be written $\{1, \sigma\}$. Define the new Hilbert symbol

$$\left(\frac{\alpha, \mathbf{Q}_p(\sqrt{\beta})/\mathbf{Q}_p}{p}\right) = 1 \text{ or } \sigma$$

depending on whether α is or is not a norm in the extension $\mathbf{Q}_p(\sqrt{\beta})/\mathbf{Q}$. Now being a norm is equivalent to solving

$$\alpha = \left(x_1 - \sqrt{\beta} \ y_1\right) \left(x_1 + \sqrt{\beta} \ y_1\right) = x_1^2 - \beta y_1^2,$$

and this is equivalent to solving $\alpha x^2 + \beta y^2 = 1$, so the new Hilbert symbol is really the same as the old one. The significance of the new interpretation lies in the fact that the Hilbert symbol can be regarded as a norm residue symbol which takes its values in the galois group of E/\mathbb{Q} . This is the key to extending the definition of the norm residue symbol from an extension E/\mathbb{Q} which is quadratic to one that is abelian. Indeed it is the basis of the definition in an abelian extension E/F of an arbitrary algebraic number field F, with $F=\mathbb{Q}$ as a special case.

Class field theory can be divided into two parts, local and global. In each part it is the study of all the abelian extensions of a certain base field. The underlying philosophy is to describe all abelian extensions in terms of objects residing within, or close to, the base field. First consider local class field theory. Here $F_{\mathfrak{p}}$ denotes any finite extension of \mathbb{Q}_p where, for the sake of discussion, we take p finite. The valuation on $F_{\mathfrak{p}}$ is written \mathfrak{p} . $F_{\mathfrak{p}}$ is an example

of what is known as a local field. The topology induced by $\mathfrak p$ makes $\dot F_{\mathfrak p}$ into a locally compact topological group and thereby provides $\dot F_{\mathfrak p}$ with a Haar measure that is essentially unique. Let $E_{\mathfrak P}$ be an abelian extension of $F_{\mathfrak p}$ with $\mathfrak P$ on $E_{\mathfrak P}$ inducing $\mathfrak p$ on $F_{\mathfrak p}$. So $E_{\mathfrak P}$ is also a local field. Let $\mathfrak g_{\mathfrak p}$ denote the galois group of $E_{\mathfrak P}/F_{\mathfrak p}$. One can naturally associate with $E_{\mathfrak P}/F_{\mathfrak p}$ a certain finite extension of finite fields, denoted $E_{\mathfrak P}(\mathfrak P)/F_{\mathfrak p}(\mathfrak p)$. (Remember, $\mathbf Q_p$ is associated with the prime field $\mathbf F_p$.) Local class field theory then tells us that there is a unique homomorphism of $\dot F_{\mathfrak p}$ into $\mathfrak g_{\mathfrak p}$ with certain properties. Its image is $\mathfrak g_{\mathfrak p}$. Its kernel is the group of norms $N_{E_{\mathfrak P}/F_{\mathfrak p}}\dot E_{\mathfrak P}$, so it deserves the name Norm Residue Symbol. It is written, rather its action is written,

$$\left(rac{lpha,\,E_{\mathfrak{P}}/F_{\mathfrak{p}}}{\mathfrak{p}}
ight)\in\mathfrak{g}_{\mathfrak{p}}\quadoralllpha\in\dot{F}_{\mathfrak{p}}.$$

Of course $\dot{F}_{\rm p}/N_{E_{\rm g}/F_{\rm p}}\dot{E}_{\rm g}\cong {\rm g}_{\rm p}$. For so-called unramified extensions $E_{\rm g}$ of $F_{\rm p}$, the norm residue symbol is closely related to the Frobenius automorphism in the galois group of the extension of finite fields $E_{\rm g}({\rm g})/F_{\rm p}({\rm p})$, and for such $E_{\rm g}$ it can be defined without much difficulty. One has a number of ways of defining the symbol for other $E_{\rm g}$, all of them difficult and circuitous. In the end, there is a unique norm residue symbol for $E_{\rm g}/F_{\rm p}$; the group $N_{E_{\rm g}/F_{\rm p}}\dot{E}_{\rm g}$ is an open subgroup of finite index in $\dot{F}_{\rm p}$; every subgroup $H_{\rm p}$ of $\dot{F}_{\rm p}$ with this property comes from some abelian $E_{\rm g}$ in this way; and there is a one-one inclusion reversing correspondence $E_{\rm g} \leftrightarrow H_{\rm p}$ between the abelian extensions $E_{\rm g}$ of $F_{\rm p}$ on the one hand, and the subgroups $H_{\rm p}$ of the above type on the other, in which $E_{\rm g}$ corresponds to $N_{E_{\rm g}/F_{\rm p}}\dot{E}_{\rm g}$. The group $H_{\rm p}$ corresponding to $E_{\rm g}$ is said to be the class group belonging to $E_{\rm g}$, and the abelian extension corresponding to $H_{\rm p}$ is called the class field belonging to $H_{\rm p}$. This, then, is the central message of local class field theory.

In global class field theory one starts with an algebraic number field F, i.e. a finite extension of Q. Instead of using the classical language of moduli to describe the general reciprocity law we will use the language of ideles. Ideles were invented by Chevalley in the 1930s. An idele $i = (i_n)_{n \in \Omega}$ is an element of the Cartesian product $\prod_{p \in \Omega} F_p$ in which almost all $|i_p|_p = 1$. The ideles form a subgroup J_F of the above product. \dot{F} can be imbedded in J_F by $\alpha \to (\alpha)_{n \in \Omega}$, these ideles are called principal, and they form a subgroup P_F of J_F . The group J_F is made into a locally compact topological group in a certain natural way. Let E be an abelian extension of F. It is then possible to define a certain homomorphism $N_{E/F}$ from J_E to J_F which is called the norm and which agrees with the usual norm from P_E to P_F , i.e. from \dot{E} to \dot{F} . For each valuation \mathfrak{P} on F fix a valuation \mathfrak{P} on E which induces \mathfrak{P} on F, take completions $F_{\mathfrak{p}} \subseteq E_{\mathfrak{P}}$, let $\mathfrak{g}_{\mathfrak{p}}$ denote the galois group of $E_{\mathfrak{P}}/F_{\mathfrak{p}}$, and note that g_p is naturally imbedded in the galois group g of E/F. In particular each situation $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ is local with $\mathfrak{g}_{\mathfrak{p}}$ abelian and so the local class field theory applies to it. (For the sake of discussion we continue to ignore the infinite valuations.) In particular, if we take an idele $i = (i_p)_{p \in \Omega}$, the quantity

$$\left(\frac{\mathfrak{i}_{\mathfrak{p}},\,E_{\mathfrak{P}}/F_{\mathfrak{p}}}{\mathfrak{p}}\right)\in\mathfrak{g}_{\mathfrak{p}}$$

is defined for all p and can be realized not just in g_p but also in g. One defines

$$(\mathfrak{i}, E/F) = \prod_{\mathfrak{p} \in \Omega} \left(\frac{\mathfrak{i}_{\mathfrak{p}}, E_{\mathfrak{P}}/F_{\mathfrak{p}}}{\mathfrak{p}} \right) \in \mathfrak{g},$$

where almost all terms in the infinite product turn out to be $1 \in \mathfrak{g}$. This provides a homomorphism $i \to (i, E/F)$ of J_F into \mathfrak{g} . It is called the reciprocity map. Its image is all of \mathfrak{g} . Its kernel is the group $P_F N_{E/F} J_E$. In particular $J_F/P_F N_{E/F} J_E \cong \mathfrak{g}$. Since P_F is in the kernel one has

$$\prod_{\mathfrak{p}\in\Omega}\left(\frac{\alpha,\,E_{\mathfrak{P}}/F_{\mathfrak{p}}}{\mathfrak{p}}\right)=1\quad\text{if }\alpha\in\dot{F}.$$

This is the general reciprocity law. It is the focal point of class field theory. It contains the Hilbert reciprocity law as the special case where E is a quadratic extension of $F = \mathbf{Q}$. The group $P_F N_{E/F} J_E$ is an open subgroup of finite index in J_F that contains P_F ; every subgroup H of J_F with this property comes from some abelian extension E in this way; and there is a one-one inclusion reversing correspondence $E \leftrightarrow H$ between the abelian extensions E of F on the one hand, and the subgroups H of the above type on the other, in which E corresponds to $P_F N_{E/F} J_E$. The group H corresponding to E is said to be the class group belonging to E, and the abelian extension E corresponding to H is called the class field belonging to H. Furthermore, the manner in which the valuation \mathfrak{p} extends to E can be described in terms of the group H belonging to E. (In classical terminology—the manner in which a prime ideal p of o decomposes in E can be described in terms of the class group Hbelonging to E.) The class field belonging to $P_F J_{\infty}$, where J_{∞} denotes the group of ideles $i = (i_p)_{p \in \Omega}$ with $|i_p|_p = 1$ for all finite valuations p, is of particular significance and has a name, the Hilbert class field of F. If E is an abelian extension of \mathbf{Q} (not of any F!) there is the remarkable theorem of Kronecker that $E \subseteq \mathbf{Q}(\zeta)$ with ζ a root of unity.

There is also a class field theory in characteristic p > 0 in which the starting point of the field of rational numbers Q is replaced by the field of rational functions k(t) with k a finite field, and algebraic number fields are replaced by algebraic function fields, i.e. by finite extensions of k(t).

So much for the message. In class field theory, however, there is more than the message. There is also the medium. As far as the hard work is concerned, and class field theory is hard whatever way you look at it, you have a choice. You can take the route of classical analysis in which the zeta function and the L-series play a crucial role; you can take the noncommutative algebraic approach based on the theory of simple algebras; you can replace this with ad hoc cohomology of 2-cocycles; or with systematic cohomology of finite groups; you can use modern analysis, specifically harmonic analysis in locally compact groups; and you can take varying doses of all these theories at the same time. Which medium is best? The answer for the moment is the Lang dictum—"... no one piece of insight which has been evolved since the beginning of the subject has every been superseded by subsequent pieces of insight. They may have moved through various stages of fashionability, and various authors may have claimed to give so-called modern treatments. You

should be warned that acquaintance with only one of the approaches will deprive you of techniques and understanding reflected by the other approaches . . . ".

Today it is possible to gain access to class field theory through a number of books. Hasse uses classical analysis. The Artin and Artin-Tate route is via ideles, topology, no Haar measure, no analysis, 2-cocycles in the local theory, modern cohomology in the global theory; four fundamental chapters on cohomology are missing, however. Cassels-Fröhlich is idelic and cohomological; it goes far beyond the main theorems. Weil uses simple algebras but no cohomology; it is heavily analytical in the modern sense. Lang uses a blend of moduli and ideles, a blend of classical and modern analysis, and a trace of cohomology. Goldstein is similar to Lang, but with a greater emphasis on ideles and modern analysis. Janusz gives the traditional approach to the subject.

The theory of numbers, the book being reviewed, is about local and global class field theory. The approach is idelic, heavily cohomological, and mildly analytical in a modern way. Algebraic function fields, as well as algebraic number fields, are included. The first chapter is an abstract development of the cohomology of groups leading to the cup product, the cohomology of finite groups, and galois cohomology. Chapter two is standard fare about valuations, Hensel's lemma, Hilbert ramification theory, the different and the discriminant. The third chapter discusses local fields and idele groups with an emphasis on their topological and analytical properties. In particular, the classical theorems known as Finiteness of Class Number and Dirichlet's Unit Theorem are corollaries to the compactness and discreteness of certain groups associated with the idele group J_F . Chapter four is a build-up to the statements of the main theorems of class field theory. It starts with a study of the cyclotomic fields which are at the heart of the development of class field theory. The fifth chapter contains proofs. The book concludes with a forty page history of class field theory and a lengthy bibliography. Zeta functions and L-series are mentioned but not used.

The theory of numbers was first published in Japanese, in 1969. It is a thoroughly reworked and thoroughly polished production that started in the 1950s with a series of seminars on number theory held each Sunday in the home of S. Iyanaga. Main contributors to the volume are S. Iyanaga, Tannaka, Tamagawa, Satake, Hattori, Shimizu, and Fujisaki. The translation is by K. Iyanaga. In spite of the multiple authorship, there is an integrity to the volume and there are no abrupt changes in style from chapter to chapter. The only exception is the historical appendix which, in contrast to the rest of the volume, is vivid and descriptive. The general philosophy seems to be to develop each machine as a separate unit, somewhat more fully than is required, and then put it into storage until it is needed. Some authors have a way of phrasing things so that their mathematics generates its own motivation as it is being developed. Here the motivation has to come from the appendix. Because of this, and because of the throughness of exposition, some readers will be discouraged. The book assumes "some basic knowledge of algebra, such as contained in . . . van der Waerden's Algebra I, II, and a knowledge of Galois theory...knowledge concerning the locally compact topological

groups is summarized ...". From a logical point of view, then, the book starts from scratch. In actual fact, however, you should either have some familiarity with algebraic numbers, cohomology and locally compact groups, or be in the presence of someone who does. If not, start with Lang. Otherwise there is a chance that you will get bogged down in the machinery. On the other hand, if you are ready for the book, and if you master it, you will have a complete understanding of class field theory in the modern medium and will be ready to approach difficult and active areas of research like the arithmetic theory of algebraic groups, modern analytic number theory, and nonabelian class field theory. If you are looking for a cohomological development of class field theory in introductory book form, then the only feasible alternative to Iyanaga is Cassels-Fröhlich. There everything is done in 203 pp. Iyanaga takes 400. Some readers will find Cassels-Fröhlich sketchy, others will find Iyanaga ponderous. While the definitive text in the modern medium remains to be written, and writing it will require enormous effort, even a touch of genius, the authors of The theory of numbers are to be thanked and congratulated for successfully completing a big task and for enriching the literature with a coherent account of class field theory in the modern spirit. Needless to say, The theory of numbers should be in the possession of anyone interested in algebraic number theory.

REFERENCES

- 1. E. Artin, Algebraic numbers and algebraic functions, Gordon and Breach, New York, 1967. MR 38 #5742.
 - 2. E. Artin and J. Tate, Class field theory, Benjamin, New York, 1968. MR 36 #6383.
- 3. J. W. S. Cassels and A. Fröhlich, Algebraic number theory, Academic Press, London, 1967. MR 35 #6500.
 - 4. L. J. Goldstein, Analytic number theory, Prentice Hall, Englewood Cliffs, N. J., 1971.
- 5. H. Hasse, Vorlesungen über Klassenkörpertheorie, Physica-Verlag, Würzburg, 1967. MR 36 #3752.
 - 6. G. J. Janusz, Algebraic number fields, Academic Press, New York, 1973.
 - 7. S. Lang, Algebraic number theory, Addison-Wesley, Reading, Mass., 1970. MR 44 #181.
 - 8. J. P. Serre, Corps locaux, Hermann, Paris, 1962. MR 27 #133.
 - 9. A. Weil, Basic number theory, Springer-Verlag, New York, 1967. MR 38 #3244.

O. T. O'MEARA

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 1, January 1978
© American Mathematical Society 1978

Stability of fluid motions. I, II, by Daniel D. Joseph, Springer Tracts in Natural Philosophy, vol. 28, Springer-Verlag, New York, 1976, xiii + 282 pp., \$39.80, and xiv + 274 pp., \$39.80.

The distinction between laminar flow and turbulent flow of a fluid is, in the first place, a matter of everyday experience. Broadly speaking, laminar flow is regular and smooth, while turbulent flow is characterized by the irregularity and random nature of the motion. Although the division between these two types of flow is not always sharp, and although a precise definition of turbulence is difficult to formulate, there is sufficient experimental evidence to indicate that the classification of fluid motions into two states, laminar and turbulent, is a very good approximation to real behaviour, at least in so far as