Comments

The early works of Iwasawa before around 1950 are mainly devoted to group theory in a wider sense. Groups (finite or infinite) with various additional structures or satisfying certain specific conditions are studied, often ending up with a complete classification. We give brief comments on some of them.

In [3] the structure of a finite group whose lattice of all subgroups satisfies a lattice-theoretic condition is thoroughly studied. (*E. g.* when the lattice is modular the group is called an "M-group".) This was a starting point of early works of M. Suzuki. The structure theorem of finite M-groups is generalized in [6] to the case of infinite M-groups under an assumption that a group under consideration is finite if it satisfies chain conditions. (Later it appeared that this assumption was not satisfied in general.)

A method employed in [1] in order to prove a finite group to be solvable has proved to be very powerful and later, with a generalization by N. Ito, found many applications. (*E. g.* it was used in [3].) [2] is a very short but important paper, in which a new method to prove the simplicity of $PSL_n(K)$ (except the case $n=2$, $K=\boldsymbol{F}_2$, $\boldsymbol{F}_3$) is given. The method depending on the group action on the flag space seems to be suggesting the later development of the theory of BN-pairs.

In [7] Iwasawa considers conditionally complete lattice groups. He proves a conjecture of G. Birkhoff that such a group is always abelian, and gives a complete structure theorem. In [17] he determines the structure of linearly ordered groups, giving a standard construction for all such groups.

In [5] and [10] (in Japanese), of which [11] is a short survey, the correspondences between (continuous) representations of locally compact groups and their suitably defined "group rings" are discussed. [12] gives a basic theory of nilpotent topological groups. (These may be regarded as a preparation for [21].) [18] and [22] deal also with topological groups. In [16], establishing an analogue in the theory of Lie algebras of Artin's splitting groups, he gives a purely algebraic proof of the faithful representability of any finite-dimensional Lie algebra over an arbitrary field, generalizing a theorem of Ado and Cartan in the classical case.

[13]–[15] are concerned with algebraic geometry. In [13] the classical Bezout theorem on intersection numbers is generalized to the

case of an algebraic curve and a hypersurface in a multiple projective space over an arbitrary ground field. A special case of it is used in the theory of algebraic correspondences of two algebraic curves developed in [14], [15].

In [25] in collaboration with T. Tamagawa (a Japanese survey [20]) a new algebraic proof is given for the finiteness of the automorphism group of an algebraic function field of genus greater than one over an algebraically closed field. His book [63] published in 1952 contains a beautiful exposition of the classical theory of algebraic functions (up to the theorem of Abel and Jacobi) from both historical and modern points of view.

However, the most important contribution of Iwasawa in this period is perhaps his work on locally compact groups and (L)-groups ([21], expository surveys [19], [24]) which gave an essential step toward the solution of the fifth problem of Hilbert.

The fifth problem of Hilbert can be formulated as follows: "Is any locally Euclidean topological group a Lie group?" If the answer is affirmative, then it gives a topological characterization of Lie groups among topological groups and, at the same time, opens a way to apply the powerful algebraic and analytic methods in the theory of Lie groups to general locally compact groups.

In the mid 1940's, when Iwasawa started his study, the fifth problem of Hilbert had been solved affirmatively only for compact groups (J. von Neumann, 1933) and for abelian groups (L. Pontrjagin, 1934). He was also informed that it was solved for solvable groups (C. Chevalley, 1941 and A. I. Mal'cev, 1945).

In [21] Iwasawa first makes a detailed study on the structure of solvable topological groups and that of Lie groups (in which appears a decomposition of a real semisimple Lie group, now called an "Iwasawa decomposition"). He establishes among other things an extension theorem for Lie groups, saying that, for a locally compact group G, if there is a closed normal subgroup N such that both N and G/N are Lie groups, then G itself is a Lie group. He then introduces a notion of (L)-groups: A locally compact group G is called an *(L)-group*, if there exists a system of closed normal subgroups $\{N_\alpha\}$ such that (i) G/N_α is a Lie group, and (ii) $\bigcap N_\alpha = e$. If G is connected, this is equivalent to saying that G is a projective limit of Lie groups. He shows that the class of (connected) (L)-groups is closed under the usual group-theoretic operations, *i.e.* taking (connected) subgroups, forming factor groups and group extensions. Compact groups and locally compact abelian groups are (L)-groups and hence, by virtue of the extension theorem, so are also connected locally compact solvable groups. He also gives two (local and global) structure theorems on connected (L)-groups. In particular, he shows that a connected locally compact group G is an (L)-group if and only if it is locally the direct product of a local Lie group and a (small) compact normal subgroup. It follows that, if an (L)-group is locally connected and finite dimensional (*e.g.* if it is locally Euclidean), then it is a Lie group. Thus the fifth problem of Hilbert is solved for all (L)-groups.

As a by-product, he gives some important results on locally compact groups in general, for instance, the unique existence of the maximal solvable closed normal subgroup (called the "radical"). At the end of [21] he mentions the following conjecture:

(C_1) Any connected locally compact group is an (L)-group.

This has a close connection with the following conjecture of Chevalley:

(C_2) A connected locally compact group with no small subgroup is a Lie group.

(C_2') A connected locally compact group with no small normal subgroup is a Lie group.

Actually, Iwasawa shows that (C_1) and (C_2') are equivalent. Of course, (C_2') trivially implies (C_2). [A little later, but independently, A. M. Gleason introduced also a notion of "generalized Lie groups" which was similar to that of (L)-groups and obtained some of the above results of Iwasawa.]

After Iwasawa a number of mathematicians such as Gleason, Montgomery, Zippin, Kuranishi, Yamabe, *etc.* continued the study on these conjectures. In 1952, Gleason confirmed the conjecture (C_2) for finite-dimensional groups, which led to a general solution of the fifth problem by Montgomery and Zippin. In 1953, H. Yamabe (Ann. of Math. 58) proved that (C_2) implies (C_2') and gave a proof of (C_2), whence follows that all the above conjectures are true. Since the Hilbert conjecture was known to be true for (L)-groups, it was proved once again and thus all basic questions about the relation between locally compact groups and Lie groups were completely settled.

There is another indirect, but no less important consequence. It is clear that from a very early stage of his study, Iwasawa was among the few number-theorists (like Artin, Chevalley and Weil) who recognized that the theory of locally compact groups would provide very powerful tools in number theory. Perhaps the first appearance of such applications was [23] and [26]. In the latter, a simple characterization of the adele rings of a number field and of an algebraic function field by their properties as topological rings is given. The techniques in totally disconnected groups, especially pro-p-groups, are indispensable in his later works in number theory. (Ichiro Satake)

{The above comments on [1], [2], [3] and [6] are due to a communication with M. Suzuki, to whom the commentator wishes to express his hearty thanks.}

From the early 1950's onwards, all of Iwasawa's published papers are devoted to algebraic number theory. Their influence has been enormous over the last 20 years, having pioneered a method which now appears widely applicable, and they have earned him a place amongst the select few who have made major advances in a subject which is one of the oldest, most highly developed, and beautiful in all of mathematics. The evolution of methods and ideas in these papers, as well as the elegance and precision of their style, can only be fully appreciated by reading the original papers themselves. However, it is hoped that the following brief comments, which concentrate on those aspects of Iwasawa's work which appear most important today, will serve as a rough guide to the mathematician who wishes to embark on reading the original papers. I have also briefly indicated where important progress has been made on the problems raised by Iwasawa. The references are to the list of Iwasawa's publications given in this volume.

The note [23] at the 1950 International Congress indicates that Iwasawa had independently of Tate discovered the adelic approach to Hecke's L-functions and their functional equation. However, the dominant theme of Iwasawa's work in algebraic number theory is his revolutionary idea that previously inaccessible information about the arithmetic of a number field F (by a number field, we mean a finite extension of the rational field $\boldsymbol{Q}$) can be obtained by investigating certain infinite towers of number fields lying above F. The archetypal example (see his comments in the introduction of [37]), to which he returns repeatedly as his ideas evolve, is the classical theory of cyclotomic fields. For each integer $m>1$, let μ_m denote the group of m-th roots of unity in some algebraic closure of $\boldsymbol{Q}$. Let p be a prime number, and define

$$(1) \qquad P=\boldsymbol{Q}(\mu_{2p}), \quad P_n=\boldsymbol{Q}(\mu_{2p^{n+1}}), \quad P_\infty=\bigcup_{n\geq 0} P_n.$$

Since the time of Kummer, number-theorists have studied the field $F=P$, but it was Iwasawa who discovered the importance of the infinite tower P_n $(n=1, 2, \cdots)$ above P. However, from his first paper [35] on these questions, he clearly saw that many aspects of his theory were not special to the cyclotomic theory. Thus, more generally, he considered infinite towers of the form

$$F=F_0\subset F_1\subset\cdots\subset F_n\subset\cdots,\quad F_\infty=\bigcup_{n\geq 0}F_n, \tag{2}$$

where, for all $n\geq 0$, F_n is a cyclic extension of F of degree p^n. Initially [35], he called such towers Γ-extensions of F, but subsequently [52] introduced the now standard terminology of $\boldsymbol{Z}_p$-extensions (indeed, F_∞ is then an infinite Galois extension of F whose Galois group is topologically isomorphic to the additive group of the p-adic integers $\boldsymbol{Z}_p$). Class field theory shows that such $\boldsymbol{Z}_p$-extensions abound in nature (every F admits at least $1+r_2(F)$ independent $\boldsymbol{Z}_p$-extensions, with equality if the units of F are p-adically independent; here $r_2(F)$ denotes the number of pairs of conjugate embeddings of F in $\boldsymbol{C}$). In what follows, we write Γ for the Galois group of F_∞ over F, and Γ_n for the subgroup of Γ which fixes F_n.

The first major group of papers on $\boldsymbol{Z}_p$-extensions are [35], [36], [37]. They are algebraic in nature, in the sense that the methods used in them do not involve special values of zeta and L-functions attached to F. The paper [35] lays the groundwork for the algebraic theory of $\boldsymbol{Z}_p$-extensions, and implicitly (but not quite explicitly) introduces what we now call the Iwasawa algebra of Γ, namely

$$R=\varprojlim_n \boldsymbol{Z}_p[\Gamma/\Gamma_n], \tag{3}$$

where $\boldsymbol{Z}_p[\Gamma/\Gamma_n]$ denotes the group ring with coefficients in $\boldsymbol{Z}_p$ of the cyclic group Γ/Γ_n of order p^n. Let $\Lambda=\boldsymbol{Z}_p[[T]]$ be the ring of formal power series in an indeterminate T with coefficients in $\boldsymbol{Z}_p$. The arguments given in [35] about the classification of compact R-modules were simplified by Serre (Sem. Bourbaki, 174, 1958–59), who pointed out that R is topologically isomorphic as a ring to Λ, whence Iwasawa's results could be obtained from the known classification theory of finitely generated Λ-modules. Compact R-modules arise naturally in the theory of $\boldsymbol{Z}_p$-extensions as follows. If N_∞ is any abelian p-extension of F_∞, which is Galois over the base field F, then the Galois group $G(N_\infty/F_\infty)$ is a compact $\boldsymbol{Z}_p$-module (because it is a projective limit of finite abelian p-groups) on which Γ acts continuously via inner automorphisms (if $x\in G(N_\infty/F_\infty)$ and $g\in\Gamma$, define $g(x)=\tilde{g}x\tilde{g}^{-1}$, where $\tilde{g}$ is any lifting of g to the Galois group of N_∞ over F_∞). This action then extends by linearity and continuity to a continuous action of R on $G(N_\infty/F_\infty)$. The main arithmetic result of [35] asserts that, if we take N_∞ to be the maximal unramified abelian p-extension L_∞ of F_∞, then $G(L_\infty/F_\infty)$ is a finitely generated torsion module over R. Let A_n be the p-primary subgroup of the ideal class group of F_n. By identifying A_n with certain quotients of the R-module $G(L_\infty/F_\infty)$, Iwasawa deduces his asymptotic formula for the order of A_n, namely that there exist integers $\lambda\geq 0$, $\mu\geq 0$, ν such that, for all sufficiently large n,

(4) $$\#(A_n)=p^{\lambda n+\mu p^n+\nu}.$$

These results are valid for all base fields F, and all $\boldsymbol{Z}_p$-extensions over F. Paper [37] returns to the classical situation (1), and is largely concerned with the study of the R-module $G(M_\infty/P_\infty)$, where M_∞ denotes the maximal abelian p-extension of F_∞, which is unramified outside p. Today, [37] should be read in conjunction with § 1–9 of [52], since many of its results are extended there to the cyclotomic $\boldsymbol{Z}_p$-extension of an arbitrary base field F (by the cyclotomic $\boldsymbol{Z}_p$-extension of F, we mean the compositum with F of the unique $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}$ contained in P_∞).

A second theme that recurs throughout Iwasawa's work is the search for analogies between $\boldsymbol{Z}_p$-extensions of number fields and the constant field extensions of curves over finite fields. Since the analogue of the invariant μ appearing in (4) is 0 in the function field case, he already begins to investigate in [33] whether μ is always 0 for the $\boldsymbol{Z}_p$-extension P_∞/P. Subsequently, this has been proven for the cyclotomic $\boldsymbol{Z}_p$-extension of any abelian extension F of $\boldsymbol{Q}$ (Ferrero-Washington, Ann. Math. 109 (1979), 377–395, Sinnott, Invent. Math. 75 (1984), 273–282), but remains an open question for the cyclotomic $\boldsymbol{Z}_p$-extension of an arbitrary base field F. On the other hand, Iwasawa later constructed [53] examples of (non-cyclotomic) $\boldsymbol{Z}_p$-extensions F_∞/F where the μ-invariant is positive.

The next group of papers to consider are [38], [39], [41], [42], [45], [46], [47] and [48], of which [41] and [48] are the central ones. They are all concerned with the classical case (1) (although [48] deals with all Dirichlet characters), and are analytic in the sense that the deepest results in them depend ultimately on the special values of the Riemann zeta and Dirichlet L-functions. In my view, they are the most significant of all, since they lead inexorably to the main conjecture, via a remarkable series of related results. Taking p odd, let U_n be the group of units in the completion of P_n at the unique prime above p, which are $\equiv 1$ and have norm 1 to $\boldsymbol{Q}_p$. Let C_n be the classical group of cyclotomic units of P_n, which are also $\equiv 1$ modulo the unique prime above p. Write Δ for the Galois group of P over $\boldsymbol{Q}$. The principal result of [41] is the complete determination as both a Δ-module and an R-module of

(5) $$Y_\infty=\varprojlim_n (U_n/\overline{C}_n)^+,$$

where $\overline{C}_n$ denotes the closure of C_n in the p-adic topology, the $+$ denotes the elements fixed by complex conjugation, and the projective limit is taken with respect to the norm maps. The arguments used are very ingenious, and depend on the explicit reciprocity law of Artin-Hasse (today a simpler proof can be given using a suitable generalization to $\varprojlim U_n$ of Kummer's notion of the higher logarithmic derivatives of an element of U_0, cf. Chap. 13 of the book *Cyclotomic Fields* by Washington). The determination involves certain twisted versions of the classical Stickelberger ideals for the extensions $P_n/\boldsymbol{Q}$ $(n=0, 1, \cdots)$, but the startling significance of this only emerges in [48]. Let χ be the character of the Galois group $G(P_\infty/\boldsymbol{Q})$ with values in the units of $\boldsymbol{Z}_p$, which is given by the action on $\mu_{p^\infty}=\bigcup_{n\geq 1}\mu_{p^n}$. Noting that $G(P_\infty/\boldsymbol{Q})=\Delta\times\Gamma$, we define

$$\omega=\chi\,|\,\Delta,\quad \rho=\chi\,|\,\Gamma.$$

Since the values of ρ lie in the units $\equiv 1 \bmod p$, ρ^s is defined for all s in $\boldsymbol{Z}_p$ and extends by linearity and continuity to a $\boldsymbol{Z}_p$-algebra homomorphism

$$\rho^s\colon R\longrightarrow \boldsymbol{Z}_p. \tag{6}$$

Let ϕ be any p-adic character of Δ with $\phi(-1)=-1$, and suppose for simplicity that $\phi\neq\omega$. Then Iwasawa shows in [48] that natural elements in the Stickelberger ideals for $G(P_n/\boldsymbol{Q})$ define an element L_ϕ of R which satisfies the remarkable interpolation property that

$$\rho^m(L_\phi)=\zeta(m)(1-p^{-m}),$$

for all integers $m<0$ such that $\chi^m\,|\,\Delta=\phi$; here $\zeta(s)$ denotes the Riemann zeta function, and we recall that its values at the odd negative integers are non-zero rational numbers. In particular, $\rho^s(L_\phi)$, for s ranging over $\boldsymbol{Z}_p$, is essentially the Kubota-Leopoldt p-adic L-function of the character $\omega\phi^{-1}$ of Δ. Thus, combining the results of [41] and [48], one obtains a complete determination of the module Y_∞ in terms of the Kubota-Leopoldt p-adic L-functions. In itself, this is a deep generalization of results going back to Kummer, but it is not the ultimate goal since Y_∞ cannot naturally be identified with the Galois group over P_∞ of some abelian p-extension of P_∞. Let L_∞ be the maximal unramified abelian p-extension of P_∞, and put $X_\infty=G(L_\infty/P_\infty)$. Now Δ also operates on X_∞ via inner automorphisms, and X_∞ can be decomposed $X_\infty=\bigoplus X_\infty^{(\psi)}$, where ψ runs over the p-adic characters of Δ, and $X_\infty^{(\psi)}$ denotes the submodule on which Δ acts via ψ. If A and B are two R-modules, $A\sim B$ will mean that there is an R-homomorphism from A to B with finite kernel and cokernel. Take $\psi=\phi$, where ϕ as above is any odd character of Δ distinct from ω. Iwasawa points out that the results of [48], together with the classical Stickelberger theorem, imply that L_ϕ annihilates the module $X_\infty^{(\phi)}$, and that if p satisfies Vandiver's conjecture (*i.e.* p does not divide the class number of the maximal real subfield of P), then

(7) $$X_\infty^{(\phi)} \sim R/(L_\phi).$$

It is now an obvious step to pass to the formulation of the main conjecture, which avoids the seemingly inaccessible Vandiver conjecture. The algebraic arguments of [35] show that there exists a pseudo-isomorphism

(8) $$X_\infty^{(\phi)} \sim R/(f_{1,\phi}) \oplus \cdots \oplus R/(f_{r_\phi,\phi}).$$

The main conjecture asserts that, up to a unit in R, the product of the elements $f_{i,\phi}$ $(1 \leq i \leq r_\phi)$ appearing in (8) is equal to L_ϕ. But it says nothing at all about the integer r_ϕ occurring in (8). Iwasawa probably correctly sensed that it needed ideas from outside the theory of cyclotomic fields to prove the main conjecture. Indeed, after a beautiful initial breakthrough by Ribet (Invent. Math. 34 (1976), 151–162), it was proven in the great paper of Mazur and Wiles (Invent. Math. 76 (1984), 179–330), using methods from modular forms*). Subsequently, Wiles has even established an analogue of the main conjecture for the field obtained by adjoining all p-power roots of unity to an arbitrary totally real number field. Finally, while we have stressed the importance of this group of papers for the discovery of the main conjecture, there is much else of interest in them. For example, [46] establishes a general formula for the Hilbert norm residue symbol in the completion of P_n at the unique prime above p, which does much to explain what lies behind the explicit formulae of Artin and Hasse (for a generalization to Lubin-Tate formal groups, see Wiles, Ann. Math. 107 (1978), 235–254).

Most of the subsequent papers contain further developments of the theory of Z_p-extensions, and, for brevity, we only mention two specifically, which both pursue aspects of the parallels between the cyclotomic Z_p-extensions of number fields and curves over finite fields. The latter part of [52] gives the detailed construction of a skew-symmetric bilinear form, which is analogous to the Weil pairing on the Tate module of the Jacobian of a curve over a finite field (see Wingberg, Comp. Math. 55 (1985), 333–381 for an alternative description of this bilinear form). Paper [58] elaborates work of Kida on an analogue for the λ-invariant appearing in (4) of the classical Riemann-Hurwitz formula for the genus change in a covering of compact Riemann surfaces. Finally, the paper [56] takes up again the question of possible generalizations of the classical Stickelberger theorem on annihilators of ideal class groups.

(John Coates)

*) Since these comments were written, V. Kolyvagin (extending earlier work of himself and F. Thaine) has found a remarkable new proof on the main conjecture, which uses only classical methods from cyclotomic fields, together with Iwasawa's work (notably his determination of Y_∞).