[P] B. A. Plamenevskij, *Algebras of pseudodifferential operators*, "Nauka", Moscow, (1986) (Russian).

[R] R. Roe, *Elliptic operators, topology and asymptotic methods*, Cambridge Univ. Press, 1988.

[S] B. W. Schultze, *Pseudodifferential operators on manifolds with singularities*, Akad. Verlagsges, Leipzig, North-Holland (in preparation).

Alexander Dynin
Ohio State University

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 21, Number 1, July 1989

*Iwasawa theory of elliptic curves with complex multiplication*, by Ehud de Shalit. Perspectives in Mathematics, vol. 3, Academic Press, Orlando, 1987, ix + 154 pp., $19.50. ISBN 0-12-210255-x

One of the most fascinating aspects of number theory and arithmetic algebraic geometry is the deep and mysterious connection between arithmetic and analysis. One example of this is the formula for the residue of the zeta function of a number field $F$,

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{d}} \tag{1}$$

where $r_1$ (resp. $r_2$) is the number of real (resp. complex) embeddings of $F$, $h$ is the class number of $F$, $R$ is the regulator (a determinant of logarithms of global units) of $F$, $w$ is the number of roots of unity in $F$, and $d$ is the discriminant of $F$.

Another, more modern example deals with elliptic curves. If $E$ is an elliptic curve defined over a number field $F$ (i.e., $E$ is a curve defined by an equation $y^2 = x^3 - ax - b$ with $a, b \in F$ and $4a^3 - 27b^2 \neq 0$), then $E$ has an $L$-function and various arithmetic invariants. The fundamental object of arithmetic interest is the set $E(F)$ of points on $E$ with coordinates in $F$; $E(F)$ has a natural abelian group structure and by the Mordell-Weil theorem this group is finitely generated. The $L$-function is defined by an Euler product over primes $\mathfrak{p}$ of $F$,

$$L(E,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\mathrm{N}\mathfrak{p}^{-s})$$

where $L_{\mathfrak{p}}(T)$ is a polynomial in $T$ of degree at most 2, whose coefficients depend on the reduction of $E$ modulo $\mathfrak{p}$. The conjecture of Birch and Swinnerton-Dyer states that

$$\operatorname{rank}_{\mathbf{Z}} E(F) = \operatorname{ord}_{s=1} L(E,s) \tag{2}$$

and further, if we denote this common value by $r$, the conjecture expresses $\lim_{s\to 1}(s-1)^{-r}L(E,s)$ in terms of other invariants of $E$, with a formula analogous to (1).

Since Birch and Swinnerton-Dyer formulated their conjecture in the late 1950s and early 1960s, many far-reaching generalizations of it have been proposed. Today there is a conjectured arithmetic interpretation of the behavior of the $L$-function of any algebraic variety at integer arguments. Fortunately in this subject the theorems, although not nearly keeping up with the conjectures, have been coming at a good pace.

One of the important tools in studying this connection between arithmetic and analysis is Iwasawa theory, which was begun by Iwasawa in the 1950s. Put most simply, Iwasawa theory is the study of $\mathbf{Z}_p$-extensions of fields. A $\mathbf{Z}_p$-extension of a field $K$ is an abelian extension $F$ of $K$ with $\mathrm{Gal}(F/K) \cong \mathbf{Z}_p$, the ring of $p$-adic integers. Studying these infinite extensions has two major benefits, the first purely algebraic but the second much deeper and having to do with the connection between arithmetic and analysis discussed above.

If $F/K$ is a $\mathbf{Z}_p$-extension, Galois theory shows that for each integer $n \geq 0$ there is a unique intermediate field $K_n$, $K \subset K_n \subset F$, with $\mathrm{Gal}(K_n/K) = \mathbf{Z}/p^n\mathbf{Z}$, and then $F = \bigcup K_n$. Writing $\Gamma = \mathrm{Gal}(F/K)$, if $Y$ is a complete topological $\mathbf{Z}_p$-module on which $\Gamma$ acts continuously, then we can view $Y$ as a module over the Iwasawa algebra

$$\Lambda = \mathbf{Z}_p[[\Gamma]] = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(K_n/K)].$$

The initial benefits of Iwasawa theory stem from the fact that $\Lambda$ is a very nice ring, much easier to work with in many ways than its quotients $\mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$. For example, $\Lambda$ is isomorphic to a power series ring $\mathbf{Z}_p[[T]]$. (A noncanonical isomorphism can be obtained by choosing a topological generator of $\Gamma$ and mapping it to the power series $1 + T$.) Thus $\Lambda$ is not only an integral domain, but a unique factorization domain as well. Finitely generated $\Lambda$-modules have a simple structure, at least if we are willing to give up a small amount of information. Namely, we say two $\Lambda$-modules are pseudo-isomorphic if there is a map between them with finite kernel and cokernel. The classification theorem states that any finitely generated $\Lambda$-module is pseudo-isomorphic to a direct sum of cyclic $\Lambda$-modules, $\Lambda^t \oplus \Lambda/f_1\Lambda \oplus \cdots \oplus \Lambda/f_s\Lambda$ where $f_i \in \Lambda$.

Simply using commutative algebra in this way can have very useful results. For example, suppose $F$ is a $\mathbf{Z}_p$-extension of a number field $K$, and let $A_n$ denote the $p$-part of the ideal class group of $K_n$. Using the ideas above applied to the inverse limit $\varprojlim A_n$, Iwasawa proved that there are nonnegative integers $\mu, \lambda$, and $\nu$ such that for all sufficiently large $n$,

$$\#(A_n) = p^{\mu p^n + \lambda n + \nu}. \tag{3}$$

The second application of Iwasawa theory is much more subtle. Number theorists have recognized for a long time that number fields have a great deal in common with function fields of curves over finite fields, and often advances in one of these areas have led to analogous advances in the other. Iwasawa realized that certain special $\mathbf{Z}_p$-extensions and associated $\Lambda$-modules could provide the analogue for number fields of the $p$-part of the Jacobian of a curve over a finite field, in the following sense.

Suppose $C$ is a smooth curve of genus $g$ defined over a finite field $k$ of characteristic different from $p$, and let $J$ be its Jacobian variety. Then $J$ is an abelian variety of dimension $g$, also defined over $k$. If we write $J_{p^\infty}$ for all points of $p$-power order on $J$ over the algebraic closure $\overline{k}$, then as a group $J_{p^\infty} \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{2g}$. The Galois group $\mathrm{Gal}(\overline{k}/k)$ acts on $J_{p^\infty}$, and $\mathrm{Gal}(\overline{k}/k)$ has a canonical generator $\gamma$, the Frobenius automorphism. Weil proved that the characteristic polynomial of $\gamma$ acting on the dual $\hat{J}_{p^\infty} = \mathrm{Hom}(J_{p^\infty}, \mathbf{Q}_p/\mathbf{Z}_p)$ is the polynomial giving the $L$-function of $C$ over $k$.

How can one develop an analogue of this situation starting with a number field $K$ instead of a curve $C$? Iwasawa gave at least a conjectural answer, which we will describe in the special case $K = \mathbf{Q}$, $p > 2$. First, he observed that the extension of scalars from $k$ to $\overline{k}$ (which is obtained by adjoining roots of unity) should correspond to the infinite extension $F = \mathbf{Q}(\boldsymbol{\mu}_{p^\infty})$ formed by adjoining all $p$-power roots of unity to $\mathbf{Q}$. Then $F$ is a $\mathbf{Z}_p$-extension of the field $\mathbf{Q}(\boldsymbol{\mu}_p)$. As for an analogue of $J_{p^\infty}$, by definition

$$J(\overline{k}) = \mathrm{Div}^0(C)/P(C)$$

where $\mathrm{Div}^0(C)$ is the group of divisors of degree 0 on $C$ over $\overline{k}$ and $P(C)$ is the group of principal divisors in $\mathrm{Div}^0(C)$. Thus it is natural to try replacing $J_{p^\infty}$ by the $p$-part of the ideal class group of $F$, that is

$$A_\infty = \varinjlim A_n$$

where as above, $A_n$ is the $p$-part of the ideal class group of the $n$th layer of the $\mathbf{Z}_p$-extension $F/\mathbf{Q}(\boldsymbol{\mu}_p)$. By theorems of Iwasawa and Fererro-Washington, as a group $A_\infty \cong (\mathbf{Q}_p/\mathbf{Z}_p)^\lambda$ where $\lambda$ is the integer from (3).

Finally, and most importantly, what should be the analogue of Weil's theorem in this situation? Both

$$\Gamma = \mathrm{Gal}(F/\mathbf{Q}(\boldsymbol{\mu}_p)) \cong \mathbf{Z}_p \quad \text{and} \quad \Delta = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_p)/\mathbf{Q})$$

act on $A_\infty$. For any character $\chi$ of $\Delta$ into $\mathbf{Z}_p^\times$, we define

$$A_\infty^\chi = \{a \in A_\infty : a^\delta = \chi(\delta)a \text{ for all } \delta \in \Delta\}.$$

For every $\chi$, $\hat{A}_\infty^\chi = \mathrm{Hom}(A_\infty^\chi, \mathbf{Q}_p/\mathbf{Z}_p)$ is a finitely generated torsion $\Lambda$-module, so the classification theorem referred to above shows that $\hat{A}_\infty^\chi$ is pseudo-isomorphic to a module of the form $\bigoplus \Lambda/f_i\Lambda$. We define a *characteristic power series* of $\hat{A}_\infty^\chi$ to be any generator of the ideal $(\prod f_i)\Lambda$. Iwasawa's proposed analogue of Weil's theorem is the following, which became known as Iwasawa's Main Conjecture. It was proved only recently, by Mazur and Wiles [**MW**].

THEOREM. *If $\chi$ is an odd character of* $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_p)/\mathbf{Q})$, *then the p-adic L-function $L_\chi$ is a characteristic power series of $\hat{A}_\infty^\chi$.*

Here $L_\chi$ is the element of $\Lambda$ which interpolates special values of Dirichlet $L$-functions in the following sense: for every charactery $\kappa$ of finite order of $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})/\mathbf{Q}(\boldsymbol{\mu}_p))$,

$$\kappa(L_\chi) = L(\kappa\chi^{-1}, 0).$$

This $p$-adic $L$-function was first constructed by Kubota and Leopoldt. Iwasawa gave a new construction using $\mathbf{Z}_p$-extensions. This theorem can be viewed as a refinement of (1); it has very deep consequences for the arithmetic of cyclotomic fields.

The book by de Shalit is not concerned with ideal class groups of cyclotomic fields, but rather with the arithmetic of elliptic curves with complex multiplication. As mentioned above, the fundamental conjecture of Birch and Swinnerton-Dyer relates the arithmetic of an elliptic curve with the behavior at $s = 1$ of its $L$-function. In the mid-1970s, Coates and Wiles observed that there is a generalization of the 'cyclotomic' Iwasawa theory that can be used to attack this conjecture. This generalization, which we will now describe, is the subject of de Shalit's book. Fix an elliptic curve $E$ with complex multiplication by an imaginary quadratic field $K$, and suppose for simplicity that $E$ is defined over $K$. Fix an odd rational prime $p$ which splits into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$ in $K$, such that $E$ has good reduction at $\mathfrak{p}$. Instead of the extension of $K$ generated by all $p$-power roots of unity, we will consider the field $K_\infty = K(E_{\mathfrak{p}^\infty})$, the extension of $K$ generated by all $\mathfrak{p}$-power torsion points on $E$. It is not hard to show that $\Gamma = \mathrm{Gal}(K_\infty/K(E_\mathfrak{p}))$ is isomorphic to $\mathbf{Z}_p$, and $\Delta = \mathrm{Gal}(K(E_\mathfrak{p})/K)$ is cyclic of degree $p - 1$.

The Iwasawa module to consider in this setting turns out to be the Selmer group $S_\infty$ of $E$ over $K_\infty$ relative to powers of $\mathfrak{p}$. For the definition see for example Chapter IV of de Shalit's book; the important property of $S_\infty$ is that it sits in an exact sequence

$$0 \to E(K_\infty) \otimes K_\mathfrak{p}/\mathcal{O}_\mathfrak{p} \to S_\infty \to Ш_{\mathfrak{p}^\infty} \to 0$$

where $K_\mathfrak{p}$ is the completion of $K$ at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ is its ring of integers, and $Ш_{\mathfrak{p}^\infty}$ is the $\mathfrak{p}$-primary part of the Tate-Shafarevich group of $E$ over $K_\infty$. From this exact sequence it is clear that knowledge of $S_\infty$ as a $\mathrm{Gal}(K_\infty/K)$-module contains a great deal of information about the points on $E$ and the Tate-Shafarevich groups of $E$ over all extensions of $K$ in $K_\infty$. As in the cyclotomic situation, for any character $\chi$ of $\Delta$ into $\mathbf{Z}_p^\times$, we define

$$S_\infty^\chi = \{s \in S_\infty : s^\delta = \chi(\delta)s \text{ for all } \delta \in \Delta\}.$$

For every $\chi$, the dual $\hat{S}_\infty^\chi = \mathrm{Hom}(S_\infty^\chi, \mathbf{Q}_p/\mathbf{Z}_p)$ is a finitely generated torsion $\Lambda$-module, so it makes sense to ask for a characteristic power series of $\hat{S}_\infty^\chi$. The work of Coates and Wiles led to the following analogue of Iwasawa's Main Conjecture; to state it we must extend scalars to $\mathcal{I}$, the ring of integers of the completion of the maximal unramified extension of $\mathbf{Q}_p$.

MAIN CONJECTURE. *If $L_\chi(E) \in \mathcal{I}[[\Gamma]]$ denotes the $\mathfrak{p}$-adic L-function associated to E and $\chi$, and $f_\chi$ is a characteristic power series of $\hat{S}_\infty^\chi$, then $L_\chi(E)\mathcal{I}[[\Gamma]] = f_\chi\mathcal{I}[[\Gamma]]$.*

Here $L_\chi(E)$ is the element of $\mathcal{I}[[\Gamma]]$ satisfying the interpolation formulas

$$\Omega_\mathfrak{p}^{-1}\kappa(L_\chi(E)) = (1 - \psi\chi^{-1}\kappa^{-1}(\mathfrak{p})/p)\Omega^{-1}L(\overline{\psi}\chi\kappa, 1)$$

for every character $\kappa$ of finite order of $K(E_{\mathfrak{p}^\infty})/K(E_\mathfrak{p})$, where $\Omega \in \mathbf{C}^\times$ is a period of $E$, $\Omega_\mathfrak{p} \in \mathcal{I}^\times$ is a $\mathfrak{p}$-adic period attached to $E$, and $\psi$ is the

Hecke character attached to $E$. The $L$-function of $E$ is given by

$$L(E,s) = L(\psi,s)L(\overline{\psi},s).$$

Coates and Wiles, although not able to prove this conjecture, were able to use their ideas to prove the following theorem, an important initial step in the direction of (2).

THEOREM. *Suppose $E$ is defined over $K$ and has complex multiplication by $K$. If $E(K)$ is infinite then $L(E,1) = 0$.*

In this theorem, as in all other work on this Main Conjecture, the crucial link between arithmetic and analysis is provided by elliptic units. Elliptic units are global units in abelian extensions of $K$, defined by analytic formulae. As global units they are related to properties of abelian extensions of$K$, and thereby to the arithmetic of $E$; being defined analytically they are related to special values of Hecke $L$-functions.

The book by de Shalit provides, for the first time, a comprehensive survey of this entire field. The first two chapters are concerned with the construction and properties of both one-variable and two-variable $\mathfrak{p}$-adic $L$-functions attached to Hecke characters of $K$. These functions were originally constructed by Manin and Vishik and by Katz, but de Shalit follows the different approach of Coates and Wiles, which is more useful for arithmetic applications. The Coates-Wiles construction uses formal groups and elliptic units, thereby relating the $\mathfrak{p}$-adic $L$-functions with arithmetic from the start. The third chapter discusses the Main Conjecture and gives some evidence for it. The fourth and final chapter uses the results of the previous chapters to prove the theorem of Coates and Wiles stated above, and a partial converse due to Greenberg.

By combining and in many cases going beyond the existing literature, this book makes an excellent reference for researchers in the area. As a textbook, or a source for learning the subject, it will be useful more for those already familiar with the classical cyclotomic Iwasawa theory; others might find it easier to learn the cyclotomic case first, for example from the texts of Lang [L] or Washington [W], or Iwasawa's survey article [I]. However, the book is largely self-contained and could be read by any mathematically-sophisticated reader with some general knowledge of number theory. It is well written and organized, and as up-to-date as any book can be in such a rapidly changing field.

## REFERENCES

[I] K. Iwasawa, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[L] S. Lang, *Cyclotomic fields*, Graduate Texts in Math., vol. 59, Springer-Verlag, Berlin, Heidelberg, New York, 1978.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[W] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., vol. 83, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

KARL RUBIN
COLUMBIA UNIVERISTY