Iwasawa Theory

It grew out of the work of Kummer and Iwasawa on cyclotomic fields, but, as I hope to explain in these lectures, it seems to be applicable to a large array of problems in arithmetic geometry. Let me also stress that, at least in its present state, it is a p-adic theory, and we always have to choose a prime p to do Iwasawa theory.

It has at least four main ingredients:-

(A). To attack the fundamental problems of arithmetic geometry.

(B). L-functions & their special values (complex and p-adic).

(C). Purely algebraic problems about modules over Iwasawa algebras, including the p-adic representation theory of compact p-adic Lie groups.

(D). As a tool for number-theoretic calculation

Although (C) & (D) are also very important, one can think of the link between (A) & (B) as the heartland of Iwasawa Theory.

Classical examples of links between (A) & (B) are :-

(i). If q is a prime $\equiv 3 \bmod 4$, there are always more quadratic residues than non-residues in $\{1, 2, \ldots, \frac{q-1}{2}\}$ (Dirichlet).

(ii). If N is a positive integer $\equiv 5, 6, 7 \bmod 8$, there always exists a right-angled triangle of area N, all of whose sides have rational length (unproven).

In Iwasawa theory, the link between (A) & (B) are the so-called "Main Conjectures". They seem to hold in vast generality.

1. Cyclotomic Fields.

The theory of cyclotomic fields has always occupied a special place in algebraic number theory. What is true for cyclotomic fields, often first proven by explicit calculations, is often true generally. This is exactly the case for Iwasawa theory.

Let me begin by describing some recent interesting work on class numbers of certain cyclotomic fields.

Notation p - any prime, μ_{p^∞} = group of all p-power roots of unity

Defn. $\mathbb{Q}^{cyc}$ = unique subfield of $\mathbb{Q}(\mu_{p^\infty})$ with Galois group $\mathbb{Z}_p$ over $\mathbb{Q}$.

Defn. B_n = unique subfield of $\mathbb{Q}^{cyc}$ of degree p^n over $\mathbb{Q}$.
h_n = class number of B_n.

easy facts to prove (any fixed p) :-

) $h_n \mid h_m$ if $n \leq m$, (ii) $(h_n, p) = 1$ for all $n \geq 1$.

uestion. Could it be true that $h_n = 1$ for all $n \geq 1$ and all p?

hen $p = 2$, this was conjectured by Weber. It eems that no numerical counter-example s known for any p.

mark. By contrast it still has not been roven today that there exist infinitely many number fields with class number 1.

ecently, there has been some interesting rogress made on Weber's conjecture by ome Japanese mathematicians.

Glder work shows that, when $p=2$, $h_5=1$, and $h_6=1$ on the generalized Riemann hypothesis. It is still unknown whether $h_7=1$.

Theorem (Horie). Assume $p=2$. If l is a prime with $l \equiv 3,5,7,9 \bmod 16$, then $(h_n, l)=1$ for all $n \geq 1$.

Theorem (Fukuda & Komatsu). Assume $p=2$. Let N be the product of all primes $< 11 \cdot 10^7$. Then $(h_n, N)=1$ for all $n \geq 1$.

We now discuss Iwasawa's Main Conjecture for cyclotomic fields, which is the starting point of all subsequent work generalizing it. Assume from now on that $p>2$ (for simplicity).

Defn. $F_\infty = \mathbb{Q}(\mu_{p^\infty})^+ =$ max. real subfield of $\mathbb{Q}(\mu_{p^\infty})$

$$G = \mathrm{Gal}(F_\infty/\mathbb{Q}).$$

We also introduce the Iwasawa algebra of G.

Defn. $\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U]$, where U runs over open subgroups of G.

The ring $\Lambda(G)$ has <u>two</u> interpretations :—

(i). <u>algebraic one</u>. If X is a compact $\mathbb{Z}_p$-module with a continuous G-action, it extends to a $\Lambda(G)$-action.

(ii). <u>analytic one</u>. The elements of $\Lambda(G)$ can be thought of as $\mathbb{Z}_p$-valued measures on G.

These two interpretations are echoed in the formulation of the main conjecture.

<u>p-adic analogue of $S(s)$.</u>

Euler products and Dirichlet series do not seem useful p-adically.

<u>Defn</u>. A <u>pseudo-measure</u> on G is an element μ of the ring of fractions of $\Lambda(G)$ such that $(\sigma - 1)\mu$ is in $\Lambda(G)$ for all σ in G.

$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^\times$ - cyclotomic character

$\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all ζ in μ_{p^∞}.

<u>Note</u>. <u>Even</u> powers of χ give homomorphism from G to $\mathbb{Z}_p^\times$.

Theorem (Kummer, Iwasawa). There exists a unique pseudo-measure S_{F_∞} on G such that

$$\int_G \chi(\sigma)^n \, dS_{F_\infty} = (1 - p^{n-1}) S(1-n)$$

for all even integers $n \geq 2$.

We should think of S_{F_∞} as the p-adic analogue of $S(s)$. But sometimes it is not easy to establish analogous properties for the two functions. For example, if $n = -2, -4, -6, \ldots$ we have

$$(1 - p^{n-1}) S(1-n) \neq 0,$$

but it is still <u>unknown</u> whether

$$\int_G \chi(\sigma)^n \, dS_{F_\infty} \neq 0$$

for all even integers $n \leq -2$.

<u>The arithmetic Iwasawa module</u>.

We first recall some pure algebra.

S^* = set of all non-zero divisors in $\Lambda(G)$.

$\Lambda(G)_{S^*}$ = ring of fractions of $\Lambda(G)$ = localization at S^*.

$\mathcal{M}_t(G)$ = category of all finitely generated torsion $\Lambda(G)$-modules

= category of all f.g. S^*-torsion $\Lambda(G)$-mo

We then have the two associated K-groups :-

$K_0(\mathcal{M}_t(G))$ = Grothendieck group of $\mathcal{M}_t(G)$.

$K_1(\Lambda(G)_{S^*}) = \Lambda(G)_{S^*}^{\times}$.

Theorem. There is a canonical exact sequence

$$K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial} K_0(\mathcal{M}_t(G)) \to 0.$$

Proof. See Bourbaki, Comm. Alg. Chap. 7.
Simplest way is to use the structure theory (Iwasawa, Serre) for torsion modules over $\Lambda(G)$.

Defn. For each M in $\mathcal{M}_t(G)$, a characteristic element for M is any $\xi_M \in K_1(\Lambda(G)_{S^*})$ such that $\partial(\xi_M) = [M]$.

Basic Fact. If $M \in \mathcal{M}_t(G)$, we have

$$\chi(G, M) = \frac{\#(H_0(G, M))}{\#(H_1(G, M))}.$$

We can recover $\chi(G, M)$ from ξ_M.
Similarly for $M(\rho)$, where $\rho \in \mathrm{Hom}(G, \mathbb{C}_p^*)$.

Moral. Knowing Ξ_M does not determine the structure of M. But it does determine the $\chi(G, M(\rho))$ for all $\rho \in \mathrm{Hom}(G, \mathbb{C}_p^\times)$.

Exact formulae of number theory always involve $\chi(G, M(\rho))$, but do not seem to say anything about the structure of the relevant M.

What is the relevant arithmetic M in this situation (for the extension $F_\infty/\mathbb{Q}$, and the Tate motive lurking in the background)?

Defn. J_∞ = maximal abelian p-extension of F_∞ unramified outside p.

Defn. $X_\infty = \mathrm{Gal}(J_\infty/F_\infty)$

J_∞ is Galois over $\mathbb{Q}$, and we have an exact sequence

$$0 \longrightarrow X_\infty \longrightarrow \mathrm{Gal}(J_\infty/\mathbb{Q}) \longrightarrow G \longrightarrow 0.$$

Since X_∞ is abelian, G acts on X_∞ via inner automorphisms. Thus X_∞ is a compact $\mathbb{Z}_p$-module, with a continuous G-action, and hence is a $\Lambda(G)$-module. It is easy to prove that X_∞ is a f.g. $\Lambda(G)$-module.

Theorem (Iwasawa). X_∞ is $\Lambda(G)$-torsion.

Additional facts about X_∞.

Fact 1. $X_\infty \neq 0$ if and only if p is an irregular prime.

$X_\infty \neq 0$ for $p = 37, 59, 67, 101, 103, \ldots$

Fact 2 (Ferrero-Washington). X_∞ is a free $\mathbb{Z}_p$-module of finite rank.

For $p = 12,613$, X_∞ has rank 4 over $\mathbb{Z}_p$.

Theorem (Iwasawa, Mazur-Wiles). The Main Conjectu

$$\partial(S_{F_\infty}) = [X_\infty] - [\mathbb{Z}_p].$$

I will be discussing the ideas behind the two known proofs in my lectures tomorrow.

A possible vast generalization.

Could this "Main Conjecture" hold in a vastly more general setting in arithmetic geometry? Everything seems to indicate that it should hold in the following general setting.

V - any motive defined over $\mathbb{Q}$ (e.g. V = an elliptic curve or an abelian variety).

$F_\infty/\mathbb{Q}$ - any Galois extension of $\mathbb{Q}$ satisfying:-

(i). $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$ is a p-adic Lie group with no element of order p;

(ii). $F_\infty/\mathbb{Q}$ is unramified outside a finite set of primes of $\mathbb{Q}$.

At present, we only know how to precisely formulate a "main conjecture" if we make two further hypotheses :-

Hypothesis 1. The p-adic Galois representation attached to V is ordinary.

Hypothesis 2. $F_\infty \supset \mathbb{Q}^{cyc}$ = cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

These are often true :

e.g. $V = A$ - an abelian variety, good ordinary reduction at p;

$F_\infty = \mathbb{Q}(A_{p^\infty})$ or $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{m})$ $m > 1$.

But we have no idea at present how to formulate a "main conjecture" when A has supersingular reduction at p and $\dim G > 1$, or when G is a group like $SL_2(\mathbb{Z}_p)$.

Assume Hypothesis 1 and 2.

Joint paper with Fukaya, Kato, Sujatha, and Venjakob formulated a precise "main conjecture". I will discuss it

in more detail in my lecture on Wednesday. Let me just say something now about the non-commutative algebra needed for this.

Defn. $\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U]$, where U runs through all open normal subgroups of G.

We do not know how to define a characteristic element, which will recover the Euler characteristic $\chi(G, M)$ for all torsion $\Lambda(G)$-modules M (good reasons to suppose this is not possible).

But, thanks to Hypothesis 2, G has additional structure :-

$$H = \mathrm{Gal}(F_\infty/\mathbb{Q}^{cyc}),\ \Gamma = \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}),\ G/H = \Gamma \xrightarrow{\sim} \mathbb{Z}_p.$$

Defn. $S = \{f \in \Lambda(G) : \Lambda(G)/\Lambda(G)f$ is a f.g. $\Lambda(H)$-module$\}$

Miracle (Easy to prove). S is an Ore set of non-zero divisors in $\Lambda(G)$.

This seems to be a new type of Ore set (beautifully generalized by Ardakov and Brown).

$S^* = \bigcup_{n \geq 0} t^n S$ - also an Ore set.

Defn. $\mathcal{M}_H(G)$ = category of all f.g. S^*-torsion $\Lambda(G)$-modules.

When $\dim G = 1$, $\mathcal{M}_H(G) = \mathcal{M}_t(G)$, but this no longer holds when $\dim G > 1$.

S^* an Ore set $\Rightarrow$ we can localize & form $\Lambda(G)_{S^*}$.

So we can again form the K-groups

$K_0(\mathcal{M}_H(G))$ = Grothendieck group of $\mathcal{M}_H(G)$.

$K_1(\Lambda(G)_{S^*})$.

Theorem. There is a canonical exact sequence

$$K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial} K_0(\mathcal{M}_H(G)) \to 0.$$

Proof. Standard sequence of algebraic K-theory, and an additional argument is required to prove ∂ is surjective.

Defn. For M in $\mathcal{M}_H(G)$, we define a characteristic element of M to be any $\xi_M \in K_1(\Lambda(G)_{S^*})$ such that $\partial(\xi_M) = [M]$.

G has p-homological dimension $d = \dim G$ as a p-adic Lie group.

$$\chi(G, M) = \prod_{i=0}^{d} \#\left(H_i(G, M)\right)^{(-1)^i}.$$

Again one shows one can recover $\chi(G, M)$ from ξ_M.

In my lecture on Wednesday I will discuss what is the relevant arithmetic $\Lambda(G)$-module for making a precise "Main Conjecture."

Kim's work on rational points on curves.

It has long (the first work was done by Mazur) that classical infinite descent à la Mordell-Weil has a natural interpretation in terms of Iwasawa theory, allowing one to study theoretically, and even computationally, the groups of rational points and the Tate-Shafarevich groups of abelian varieties defined over $\mathbb{Q}$. But our lack of knowledge of the arithmetic Iwasawa modules involved only

allows us to prove fragmentary results so far in the direction of the conjecture of Birch and Swinnerton-Dyer.

Recently, Minhyong Kim has discovered a revolutionary new method for studying rational points on curves of genus > 1 (or integral points on curves of genus 1 or 0). He uses the $\mathbb{Q}_p$-pro-unipotent fundamental group of the curve, where p can be any prime of good reduction. I cannot enter here to any detailed discussion of his method, beyond briefly comment on the specific question in Iwasawa theory which is needed to complete his finiteness proof. What is remarkable is that, via his method, one has to study a much simpler Iwasawa module than in classical descent theory.

A - abelian variety defined over $\mathbb{Q}$ (the Jacobian of our curve of genus >1).

Defn. $F_\infty = \mathbb{Q}(A_{p^\infty})$, $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$.

We will not have to assume A is ordinary at p. Otherwise $F_\infty/\mathbb{Q}$ satisfies all the hypotheses made earlier, including Hypothesis 2 ($F_\infty \supset \mathbb{Q}(\mu_{p^\infty})$ by the Weil pairing)

Defn. L_∞ = maximal abelian p-extension of F_∞, unramified everywhere.

Defn. $W(F_\infty) = \mathrm{Gal}(L_\infty/F_\infty)$.

G acts on the left on $W(F_\infty)$, giving rise to a $\Lambda(G)$-module structure.

Key point. $W(F_\infty)$ is a much smaller module than those arising from classical descent theory on A.

Theorem. $W(F_\infty)$ is a torsion $\Lambda(G)$-module.

Iwasawa's $\mu=0$ conjecture $\Rightarrow$ $W(F_\infty)$ is even S-torsion.

Perhaps $W(F_\infty)$ is always pseudo-null.

So far this has led to a totally new proof of Faltings theorem in the following case :-

Theorem. Let C be a smooth projective curve of genus >1 defined over $\mathbb{Q}$, such that the Jacobian variety of C is isogenous over $\overline{\mathbb{Q}}$ to a product of abelian varieties with complex multiplication. Then $C(\mathbb{Q})$ is finite.

Ex $C: ax^m + by^m = cz^m$
$a, b, c \in \mathbb{Q}$, $abc \neq 0$, $m \geq 4$.

Hopes. It will eventually work for all smooth projective curves of genus >1 defined over number fields, and perhaps yield quantitative results for the rational points.