Iwasawa theory

Last time we found the relationship between the class group and the Hilbert class field via class field theory. The class group measures the failure of unique factorization and is one of the most important arithmetic invariants of a number field.

Example 1. When trying to solve the Fermat equation

$$x^p + y^p = z^p, \quad p \text{ an odd prime},$$

we factorize it as

$$\prod_i (x + \zeta_p^i y) = z^p$$

and hope to conclude that $x+\zeta_p^i y$ is a pth power. In fact, one can show that the ideals $(x+\zeta_p^i y)$ are mutually coprime, so by unique factorization of prime ideals, we know that $(x + \zeta_p^i y)$ is a p-power of an ideal $\mathfrak{a}$. Now requiring $\mathfrak{a}$ to be a principal ideal suffices to assume that the class group $H(\mathbb{Q}(\zeta_p))$ has no element of p-power order. This is the way Kummer found the following famous criterion.

Theorem 1. If $p \nmid \#H(\mathbb{Q}(\zeta_p))$, then $x^p + y^p = z^p$ has no nontrivial integer solutions.

The primes satisfying this condition are called **regular primes**. Kummer computed the class group for $p < 100$ and showed that there are only three irregular primes $p = 37, 59, 67$ in this range. This is the best result on Fermat's last theorem for a long period.

So understanding the p-part of the class group $H(\mathbb{Q}(\zeta_p))$ is of great arithmetic interest.

Example 2. Let us consider the first irregular prime $p = 37$. The 37-part of the cyclotomic fields $\mathbb{Q}(\zeta_{37^n})$ turns out to be $\mathbb{Z}/37^n\mathbb{Z}$.

Example 3. 691 is also an irregular prime. The 691-part of of the cyclotomic fields $\mathbb{Q}(\zeta_{691^n})$ turns out to be $(\mathbb{Z}/691^n\mathbb{Z})^2$.

You may smell something. We now introduce a general definition and state Iwasawa's class number formula in the more general setting.

Definition 1. Let p be an odd prime. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times \mathbb{Z}_p$. We define $\mathbb{Q}_\infty \subseteq \mathbb{Q}(\zeta_{p^\infty})$ to be the fixed field of $\mathbb{F}_p^\times$ (so $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$). Let K be a number field. We define $K_\infty := K\mathbb{Q}_\infty$. Then $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ and we call K_∞ the **cyclotomic $\mathbb{Z}_p$-extension** of K. We denote by K_n the finite extension of K corresponding to the group $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ and $H_n = H(K_n)$.

Example 4. For $K = \mathbb{Q}(\zeta_p)$, $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$ is the cyclotomic $\mathbb{Z}_p$-extension of K and $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$.

Theorem 2 (Iwasawa's class number formula)**.** There exists constants $\mu, \lambda \geq 0$ and ν such that when n is sufficiently large,

$$\log_p \#H_n = \mu p^n + \lambda n + \nu.$$

Example 5. We have $\mu = 0$, $\lambda = \nu = 1$ for $K = \mathbb{Q}(\zeta_{37})$ and $\mu = 0$, $\lambda = 2$, $\nu = 1$ for $K = \mathbb{Q}(\zeta_{691})$.

In view of the analogy between 3-manifolds and number fields, we obtain the following table.

infinite cyclic covering $X_\infty \to X_K$	Cyclotomic $\mathbb{Z}_p$ extension K_∞/K
homology group $H_1(M_n)$	class group $H_n := H(K_n)[p]$
asymptotic formula on homology groups	asymptotic formula on class groups

Our goal today is to sketch the main ingredients of the proof and see how it is amazingly similar to the case of knots and Alexander polynomials.

Recall that the Alexander polynomial is defined via the action of $\Lambda = \mathbb{Z}[G_K^{\mathrm{ab}}] \cong \mathbb{Z}[\mathrm{Gal}(X_\infty/X_K)]$ on $H_1(X_\infty)$. Since $\Lambda \cong \mathbb{Z}[t^{\pm 1}]$ and $\Lambda_{\mathbb{Q}} = \mathbb{Z}[t^{\pm 1}]$ is a PID, we know that

$$H_1(X_\infty) \otimes \mathbb{Q} \cong \bigoplus_i \Lambda_{\mathbb{Q}}/(f_i)$$

as $\Lambda_{\mathbb{Q}}$-modules. Since the presentation matrix is simply the diagonal matrix (f_i), the Alexander polynomial is nothing but the product $\prod_i f_i$ up to $\Lambda_{\mathbb{Q}}^\times$.

What is the arithmetic analogue of Λ acting on $H_n = H(K_n)[p]$? By class field theory, $H_n \cong \mathrm{Gal}(L_n/K_n)$, where L_n is the maximal unramified abelian p-extension of K_n. Write $L_\infty := \bigcup L_n$ and

$$H_\infty := \varprojlim_n H_n = \varprojlim_n \mathrm{Gal}(L_n/K_n) = \mathrm{Gal}(L_\infty/K_\infty).$$

Since $\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$ acts on $H_n \cong \mathrm{Gal}(L_n/K_n)$, we know that $\varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$ acts on H_∞.

Definition 2. We define the **Iwasawa algebra** to be $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] := \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$.

The following theorem tells us that the Iwasawa algebra has a neat description and thus plays a similar role as $\mathbb{Z}[t^{\pm 1}]$.

Theorem 3. Let γ be the topological generator of $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Then $\gamma \mapsto 1 + T$ induces an isomorphism $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[T]]$ of $\mathbb{Z}_p$-algebras.

This is one major reason we want to consider K_∞ and H_∞: the action of the nice algebra $\mathbb{Z}_p[[T]]$ on the class groups cannot be seen at finite levels. Assuming for simplicity that there is only one prime of K ramified in K_∞ and is totally ramified (this is the case for $K = \mathbb{Q}(\zeta_p)$), then we can recover H_n from H_∞ analogously to the knot situation, which is another major reason we would like to consider the infinite tower of fields rather than K itself.

Theorem 4. We have an isomorphism $H_n \cong H_\infty/((1+T)^{p^n} - 1)H_\infty$.

Morally the Iwasawa algebra $\hat{\Lambda} = \mathbb{Z}_p[[T]]$ behaves as the power series ring $\mathbb{C}[[X, Y]]$ and we have the following p-adic version of the Weierstrass preparation theorem.

Theorem 5. Suppose $f(T) \in \hat{\Lambda}$ is non zero. Then $f(T)$ can be uniquely written as

$$f(T) = p^\mu g(T) u(T),$$

where $\mu \geq 0$, $u(T) \in \hat{\Lambda}^\times$ and $g(T)$ is a **Weierstrass polynomial**, namely $g(T) = T^\lambda + c_1 T^{\lambda-1} + \cdots + c_\lambda$ with $c_i \equiv 0 \pmod{p}$. We call μ and λ the **μ-invariant** and **λ-invariant** of $f(T)$.

$\hat{\Lambda} = \mathbb{Z}_p[[T]]$ is not a PID but fortunately the following structure theorem of finitely generated $\hat{\Lambda}$-modules is still valid.

Theorem 6. Let N be a finitely generated $\hat{\Lambda}$-module, then we have an pseudo-isomorphism (i.e., a homomorphism with finite kernel and cokernel)

$$N \sim \hat{\Lambda}^r \bigoplus_i \hat{\Lambda}/(p^{m_i}) \bigoplus_j \hat{\Lambda}/(f_j^{e_j}),$$

where $r, m_i, e_i \geq 0$ and f_i's are irreducible Weierstrass polynomials. The polynomial

$$f := \prod_i p^{m_i} \prod_j f_j^{e_j}$$

is called the **Iwasawa polynomial** of N, well-defined up to $\hat{\Lambda}^\times$. We define the **μ-invariant** and **λ-invariant of** N to be $\mu = \sum_i m_i$ and $\lambda = \sum_j (\deg f_j)^{e_j}$ (the sum of individual μ,λ-invariants).

Using the finiteness of the class group H_n and a Nakayama lemma argument, one can show that H_∞ is a finitely generated torsion $\hat{\Lambda}$-module. So the Iwasawa polynomial, μ-invariant and λ-invariant of H_∞ are all well defined due to the previous structure theorem. Now we can restate Theorem 2 more precisely.

Theorem 2. Let μ and λ be the μ-invariant and λ-invariant of H_∞. Then there exists a constant ν such that when n is sufficiently large,

$$\log_p \# H_n = \mu p^n + \lambda n + \nu.$$

Sketch of the Proof. Suppose $H_\infty \sim \hat{\Lambda}/(p^{m_i}) \bigoplus_j \hat{\Lambda}/(f_j^{e_j})$. By Theorem 4 we need to compute $\#N/((1+T)^{p^n}-1)N$ for $N = \hat{\Lambda}/(p^m)$ or $N = \hat{\Lambda}/(g)$ for g a Weierstrass polynomial. The first case contributes p^{mp^n} and the second case contributes $\prod_{\zeta^{p^n}=1} |g(\zeta-1)|_p^{-1}$. The latter one is dominated by the leading term since g is a Weierstrass polynomial and becomes $n \deg g + c$ for some constant c when n is sufficiently large. □

Remark. One can further show that $\mu = 0$ for K any abelian extension of $\mathbb{Q}$. Moreover when $K = \mathbb{Q}(\zeta_p)$, the formula $\# H_n = \prod |f(\zeta-1)_p^{-1}|$ is true for any $n \geq 1$, where $f(T)$ is the Iwasawa polynomial of H_∞.

Remark. The Iwasawa polynomial is harder to compute compared to Alexander polynomial by hand, since we do not have a nice arithmetic analogue of the Wirtinger representation and also the ring $\mathbb{Z}_p$ is much larger than $\mathbb{Z}$. Computer algorithms have been developed for the computation.

Remark. When is p an irregular prime, i.e., when does $H(\mathbb{Q}(\zeta_p))$ has nontrivial p-part? Miraculously Kummer proved that it happens exactly when p appears in one of the numerators of the Riemann zeta values $\zeta(-1), \zeta(-3), \zeta(-5), \ldots$! For example,

$$\zeta(-11) = \frac{691}{32760}$$

and

$$\zeta(-31) = \frac{37 \cdot 683 \cdot 305062827}{2^6 \cdot 3 \cdot 5 \cdot 17}$$

shows that 691 and 37 are irregular. The connection between Iwasawa polynomials and Riemann zeta functions can be made rigorously and is the content of the Iwasawa main conjecture. This conjecture is much deeper and was first proved by Mazur-Wiles in 1984 and reproved by Rubin in 1994 using Euler system. It not so surprising that Wiles' proof of Fermat's last theorem used ideas from Iwasawa theory in an essential way.

We end the lectures by the following summary.

infinite cyclic covering $X_\infty \to X_K$	Cyclotomic $\mathbb{Z}_p$ extension K_∞/K
homology group $H_1(M_n)$	class group $H_n := H(K_n)$
asymptotic formula on homology groups	asymptotic formula on class groups
$\Lambda = \mathbb{Z}[G_K^{\mathrm{ab}}] \cong \mathbb{Z}[t^{\pm 1}]$	$\hat{\Lambda} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[T]]$
$H_1(M_n) \cong H_1(X_\infty)/(t^n - 1)H_1(X_\infty)$	$H_n \cong H_\infty/((1+T)^{p^n} - 1)H_\infty$
Alexander polynomial	Iwasawa polynomial
$\#H_1(M_n) = \prod \lvert\Delta(\zeta)\rvert$	$\#H_n = \prod \lvert f(\zeta - 1)\rvert_p^{-1}$

There are many more beautiful stories to tell and discover. Now — it's your turn!