Iwasawa theory

Dominik Bullach

Fermat's last theorem Much of algebraic number theory grew out of attempts to prove *Fermat's last theorem*, which asserts that there are no natural numbers $a, b, c \in \mathbb{N}$ with

$$a^n + b^n = c^n$$

if $n > 2$ is an integer. While this was only proved in full generality by Andrew Wiles in the 1990s, the special case where the exponent n is a 'regular' prime p had already been solved in the 19th century. The prime number p is called regular if it does not divide the cardinality of the class group Cl_K of the cyclotomic field $K \coloneqq \mathbb{Q}(e^{2\pi i/p})$, and so we are led to ask: What can we say about the highest power of p that divides $|\mathrm{Cl}_K|$?

Iwasawa theory Let us first study this question in a family. That is, instead of considering the field K on its own, let us define the tower of cyclotomic fields $K_i \coloneqq \mathbb{Q}(e^{2\pi i/p^i})$ for every $i \in \mathbb{N}$. Writing p^{e_i} for the maximal power of p that divides $|\mathrm{Cl}_{K_i}|$, Iwasawa has then proved that there exist constants $\mu, \lambda, \nu \in \mathbb{Z}$ such that

$$e_i = \mu p^i + \lambda p + \nu \quad \text{for all sufficiently large } i, \tag{1}$$

and later Ferrero and Washington showed that in fact $\mu = 0$. The proof of (1) crucially uses that each class group Cl_{K_i} is naturally endowed with an action of the Galois group $\mathrm{Gal}(K_i/\mathbb{Q})$ so that a limiting process leads to a module A_{K_∞} for the limit algebra $\Lambda \coloneqq \varprojlim_{i\in\mathbb{N}} \mathbb{Z}_p[\mathrm{Gal}(K_i/\mathbb{Q})]$. The latter is called the *Iwasawa algebra* and has nice ring-theoretic properties that lead to the proof of (1) via a structure theory of Λ-modules.

The Iwasawa main conjecture Our question can also be answered using *Kummer's criterion*. This involves the Riemann ζ-function $\zeta(s)$, and states that

$$p \text{ divides } |\mathrm{Cl}_K| \;\Leftrightarrow\; p \text{ divides the numerator of at least one of } \zeta(-1), \zeta(-3), \ldots, \zeta(4-p).$$

For example, it follows from $\zeta(-31) = \frac{37 \cdot 208360028141}{16320}$ that 37 is an irregular prime (and, in fact, the smallest such). This surprising link is a consequence of the *Iwasawa main conjecture* that, in this setting, was proved by Mazur and Wiles. Roughly speaking, the Iwasawa main conjecture asserts that a p-adic object built from the values $\zeta(-n)$ for odd positive integers generates the 'characteristic ideal', an important Λ-structure invariant, of the module A_{K_∞} built from class groups.

Project description Depending on previous knowledge and interests, this project can include the algebraic theory of Iwasawa modules, the proof of Iwasawa's class number formula, p-adic L-functions, or the Iwasawa main conjecture (statement or even parts of the proof).

References Standard textbooks on Iwasawa theory are [NSW08, Chapters V and XI] and [Was97]. Useful survey articles are [Wut14] and [RJW25].

References

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Second. Vol. 323. Fundamental Principles of Mathematical Sciences. Springer-Verlag, Berlin, 2008.

[RJW25] Joaquín Rodrigues Jacinto and Chris Williams. *An introduction to p-adic L-functions*. Essent. Number Theory 4.1 (2025), pp. 101–216.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[Wut14] Christian Wuthrich. "Overview of some Iwasawa theory". In: *Iwasawa theory 2012*. Vol. 7. Contrib. Math. Comput. Sci. Springer, Heidelberg, 2014, pp. 3–34.