Bayerische Kleine AG: The Theorem of Herbrand-Ribet

Organisation:
Paul Jonas Hamacher[1]
Timo Keller[2]

In proving Fermat's Last Theorem, the class number of cyclotomic fields $\mathbf{Q}(\zeta_p)$ and its divisibility by p plays an important role. The theorem of Herbrand is an answer to a refinement of this question. Denote the class group of $\mathbf{Q}(\zeta_p)$ by A and consider A/p as a $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_p))$-module. Under this action, A/p breaks up into eigenspaces $(A/p)_i$. Now Herbrand's theorem states that if for i odd $(A/p)_i$ is nontrivial then the $(p-i)$-th Bernoulli number is divisible by p, so if none of these Bernoulli numbers are divisible by p, one gets a proof of Fermat's Last Theorem. Later, Ribet proved the converse of Herbrand's theorem using modular forms. The main conjecture of Iwasawa theory gives a further generalisation of Herbrand-Ribet: The p-valuation of B_{p-i} is exactly the valuation of p dividing $|(A/p)_i|$.

1. The Theorem of Herbrand-Ribet: Herbrand and Class Field Theory

- State the theorem of Herbrand-Ribet [Wa], Theorem 6.17 and 6.18, p. 101 f.
- Prove Stickelberger's theorem in the case of a full cyclotomic field $\mathbf{Q}(\zeta_p)$ [Wa], Theorem 15.1, § 15.1, p. 332–334.
- Using Stickelberger's theorem and Corollary 5.15, prove the theorem of Herbrand [Wa], § 6.3, p. 100 f.
- Prove the von Staudt-Clausen theorem [Da], Theorem 6.1, p. 17 f.

2. The Theorem of Ribet: Class field theory and Galois representations

- Prove that the converse of Herbrand's theorem, Ribet's theorem, follows via class field theory from the existence of a certain Galois representation [Da], Theorem 1.1–1.3, p. 5–7.
- Sketch the proof that the main conjecture of Iwasawa theory implies the above mentioned refinement of the Herbrand-Ribet theorem [Br], p. 65–68.

In the next sections, we will construct such a Galois representation using modular forms.

3. The Theorem of Ribet: Rounding the circuit

- Illustrate the proof of the Ribet's converse to Herbrand's theorem for $\mathbf{Q}(\zeta_{691})$ as in [Ma], p. 11–16.
- Illustrate the proof of the Ribet's converse to Herbrand's theorem in general as in [Ma], p. 16–20.

4. The Theorem of Ribet: Modular Forms I

- Start proving the existence of the sought-for Galois representation [Da], p. 7–12. You may also consult [Kh], [Sa] or [Br], p. 76 ff.

5. The Theorem of Ribet: Modular Forms II

- Finish the proof [Da], p. 12–16. You may also consult [Kh], [Sa] or [Br], p. 76 ff.

[1] `<Nachname>@ma.tum.de`
[2] `<Vorname>.<Nachname>@mathematik.uni-regensburg.de`

References

[Br] Brown, J. L., *An Introduction to Iwasawa Theory*, http://www.math.clemson.edu/~jimlb/CourseNotes/iwasawa.pdf.

[Da] Dalawat, C. S., *Ribet's modular construction of unramified p-extensions of* $\mathbf{Q}({}_p\mu)$, http://arxiv.org/pdf/0903.2617.

[Kh] Khare, Ch., *Notes on Ribet's Converse to Herbrand*, http://www.bprim.org/cyclotomicfieldbook/ribet1.pdf.

[Ma] Mazur, B., *How can we construct abelian Galois extensions of basic number fields?*, http://www.math.harvard.edu/~mazur/papers/Ribet30.pdf.

[Sa] Saikia, A., *Ribet's Construction of a Suitable Cusp Eigenform*, http://www.iitg.ernet.in/a.saikia/04-ghy-atm-ribet.pdf.

[Wa] Washington, L. C., *Introduction to Cyclotomic Fields*, second edition.[3]

[3] Note the errata http://www2.math.umd.edu/~lcw/cycloerrata.pdf!