GROUPE D'ÉTUDE D'ALGÈBRE

KENNETH A. RIBET

Sur la recherche des p-extensions non ramifiées de $\mathbb{Q}(\mu_p)$

Groupe d'étude d'algèbre, tome 1 (1975-1976), exp. nº 2, p. 1-3
<http://www.numdam.org/item?id=GEA_1975-1976__1__A2_0>

Groupe d'étude d'ALGÈBRE
(Marie-Paule MALLIAVIN)
1re année, 1975/76, n° 2, 3 p.

2 février 1976

SUR LA RECHERCHE DES p-EXTENSIONS NON RAMIFIÉES DE $\mathbb{Q}(\mu_p)$

par Kenneth A. RIBET

English Summary

Kummer's criterion states, that an odd prime p is irregular if, and only if, p divides (the numerator of), at least one Bernouilli number B_k, where k ranges over the even integers between 2 and $p-1$. The irregularity means that h_p is divisible by p, where h_p is the class number of the field $\mathbb{Q}(\mu_p)$ of p-th roots of unity. Alternately, p is irregular when $\mathbb{Q}(\mu_p)$ has an unramifield abelian p-extension.

Let $C\ell$ be the group of ideal classes of $\mathbb{Q}(\mu_p)$, and let C be the group $C\ell/(C\ell)^p$, which for convenience, we write additively. Then, C is an $\mathbb{F}_p$-vector space which is non-zero precisely when p is irregular. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on C through its quotient $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = \Delta$, and on the other hand, all characters of Δ with values in $\mathbb{F}_p$ are obtained, as the power of the fundamental character :

$$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \dashrightarrow \Delta \xrightarrow{\sim} \mathbb{F}_p^*$$

which arises from the action of Δ on μ_p. We may then write :

$$C = \oplus_{i \bmod (p-1)} C(\chi^i)$$

with

$$C(\chi^i) = \{c \in C \ ; \ \sigma c = \chi(\sigma)c \quad \text{for all} \quad \sigma \in \Delta\} .$$

Actually, though, it is more convenient to rewrite this

$$C = C^+ \oplus (\oplus_{k \bmod (p-1), k \text{ even}} C_k) ,$$

where

$$C^+ = \oplus_{i \bmod (p-1), i \text{ even}} C(\chi^i) ,$$

and

$$C_k = C(\chi^{i-k})$$

when k is even. If we then put

$$C^- = \oplus_{i \bmod (p-1), i \text{ even}} C(\chi^i) ,$$

the equation $C = C^+ \oplus C^-$ summarises the decomposition of C into its "plus" and "minus" eigenspaces under the action of the complex conjugation in Δ. It is known, that the non-vanishing of C^+ implies that of C^-, so that p is irregular if, and only if, (at least) one C_k is non-zero. Hence Kummer's criterion may be restated as follows : An odd prime p divides at least one B_k (k even ; $2 \leqslant k \leqslant p-1$) if, and only if, at least, one C_k is non-zero.

Furthermore, the following result is well known in the theory of cyclotomic fields (it is a corollary of the Stickelberger theorem) :

THEOREM. - If $C_k \neq 0$ for a given k, then $p | B_k$ (the same k).

This suggests the possibility of proving the following converse.

CONVERSE. - If $p | B_k$, then $C_k \neq 0$.

To prove it, one performs the following result.

Construction. - Suppose $p | B_k$. Then, there exists a finite field $\underset{\sim}{F} \supset \underset{\sim}{F}_p$ and a continuous representation

$$\bar{\rho} : \mathrm{Gal}(\overline{\underset{\sim}{Q}}/\underset{\sim}{Q}) \dashrightarrow G\ell(2, \underset{\sim}{F})$$

with the following properties :

(i) $\bar{\rho}$ is unramified at all primes $\ell \neq p$.

(ii) $\bar{\rho}$ is reductible (as an $\underset{\sim}{F}$-representation) in such a way that $\bar{\rho}$ may be written matricially in the form

$$\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$$

(iii) $\bar{\rho}$ has an image whose order is divisible by p,

(iv) The image in $G\ell(2, \underset{\sim}{F})$ of any decomposition group for p has order prime to p.

The construction gives the required result, because of functorial properties of the Artin symbol and the matrix conjugaison formula

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & ad^{-1}x \\ 0 & 1 \end{pmatrix}.$$

John COATES has remarked that the three properties (i), (ii), (iii) together imply property (iv) under the assumption $C^+ = 0$. This assumption, equivalent to the statement that p is "properly irregular", implies as well the above converse. Further, if $C^+ = 0$, then all non-zero C_k have $\underset{\sim}{F}_p$-dimension 1.

The aim of the seminar was to suggest a proof of the converse by means of modular forms. Here, we give a quick sketch of the basic idea of the proof, which will appear else where.

The first key was suggested by SERRE [3]. Namely, if $p | B_k$, there exists a cusp form $f = \sum_{n \geqslant 1} a_n q^n$ of weight k on $S\ell_2(\underset{\sim}{Z})$ which is a normalized eigenform for all Hecke operators $T(n)$, and which resembles an Eisenstein series in the following sense : there exists a prime ideal $\wp | p$ of the field $K = \underset{\sim}{Q}(a_n, n \geqslant 1)$ such that for eachprime $\ell \neq p$ the number a_ℓ is a $\wp$-integer satisfying :

$$a_\ell \equiv 1 + \ell^{k-1} \mod \wp \ .$$

A construction of Deligne associates to f a $\wp$-adic representation :

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \dashrightarrow G\ell(2 \ , K_\wp)$$

with $K_\wp$ the completion of K at $\wp$. The congruence for the a_ℓ (plus an argument in linear algebra) shows, that after a change of basis, ρ_f may be factored :

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \dashrightarrow G\ell(2 \ , O_\wp)$$

(with $O_\wp$ the integer ring of $K_\wp$) so, that the reduction :

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \dashrightarrow G\ell(2 \ , O_\wp) \longrightarrow G\ell(2 \ , \mathbb{F})$$

of ρ_f mod $\wp$ has the properties (i), (ii), (iii). Unfortunately, it seems impossible to prove (iv), because little is known about the properties at p of the representation ρ_f .

Therefore, we do something different. SERRE has remarked, that mod p representations obtained from forms of weight k may often be seen on the Jacobian J attached to cusp forms of weight 2 on $\Gamma_0(p)$. This induces us to construct such a form with a congruence property like that above (the construction may be done by essentially bare-handed techniques). Given such a form, we obtain a representation $\overline{\rho}$ which again satisfies (i) , (ii), and (iii), but which has the following additional property (deduced from results of DELIGNE and RAPOPORT [1]) : locally at p , over the real cyclotomic field $\overline{\mathbb{Q}}(\mu_p)^+$, $\overline{\rho}$ is the representation attached to a finite flat commutative group scheme, killed by p , over the integer ring of a p-adic field whose absolute ramification index is less than $p - 1$. However, such group-schemes have been studied by RAYNAUD [2]. Using his results, we deduce that property (iv) for the new $\overline{\rho}$ is satisfied as well.

REFERENCES

[1] DELIGNE (P.) and RAPOPORT (M.). - Les schémas de modules de courbes elliptiques "Modular functions of one variable, II, Proceding International summer school [1972. Antwerpen]", p. 143-316. - Berlin, Springer-Verlag, 1973 (Lecture Notes in Mathematics, 349).

[2] RAYNAUD (M.). - Schémas en groupes de type (p , ... , p), Bull. Soc. math. France, t. 112, 1974, p. 241-280.

[3] SERRE (J.-P.). - Une interprétation des congruences relatives à la fonction τ de Ramanujan, Séminaire Delange-Pisot-Poitou : théorie des nombres, 9e année, 1967/68, n° 14, 17 p.

Kenneth A. RIBET
Princeton University
PRINCETON, N. J. 08540
(Etats-Unis)