Kenneth A. Ribet

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


<http://www.numdam.org/item?id=GEA_1975-1976__1__A2_0>
Kummer's criterion states, that an odd prime $p$ is irregular if, and only if, $p$ divides (the numerator of), at least one Bernoulli 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 unramified abelian $p$-extension.

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

$$\chi : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \Delta \overset{\sim}{\rightarrow} F_p^*$$

which arises from the action of $\Delta$ on $\mu_p$. We may then write:

$$C = \bigoplus_{i \mod (p-1)} C(\chi^i)$$

with

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

Actually, though, it is more convenient to rewrite this

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

where

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

and

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

when $k$ is even. If we then put

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

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 $\Delta$. 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 $R_k$ ($k$ even; $2 \leq k \leq p - 1$) 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 $p \mid R_k$ (the same $k$).

This suggests the possibility of proving the following converse.

**CONVERSE.** - If $p \mid R_k$, then $C_k \neq 0$.

To prove it, one performs the following result.

**Construction.** - Suppose $p \mid R_k$. Then, there exists a finite field $F \supseteq F_p$ and a continuous representation

$$\overline{\rho} : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \to \text{GL}(2, F)$$

with the following properties:

1. $\overline{\rho}$ is unramified at all primes $\mathfrak{p} \neq p$.
2. $\overline{\rho}$ is reducible (as an $F$-representation) in such a way that $\overline{\rho}$ may be written matricially in the form

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

3. $\overline{\rho}$ has an image whose order is divisible by $p$,
4. The image in $\text{GL}(2, F)$ 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

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

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 $F_p$-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 $p \mid R_k$, there exists a cusp form $f = \sum_{n \geq 1} a_n q^n$ of weight $k$ on $\text{SL}_2(\mathbb{Z})$ 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 $\mathfrak{p} \mid p$ of the field $K = \mathbb{Q}(a_n, n \geq 1)$ such that for each prime $\mathfrak{p} \neq p$ the number $a_{\mathfrak{p}}$ is a $\mathfrak{p}$-integer satisfying:
A construction of Deligne associates to $f$ a $\mathfrak{p}$-adic representation:

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow G_\mathfrak{p}(2, K_\mathfrak{p})$$

with $K_\mathfrak{p}$ the completion of $K$ at $\mathfrak{p}$. The congruence for the $a_\mathfrak{p}$ (plus an argument in linear algebra) shows, that after a change of basis, $\rho_f$ may be factored:

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow G_\mathfrak{p}(2, \mathcal{O}_\mathfrak{p})$$

(with $\mathcal{O}_\mathfrak{p}$ the integer ring of $K_\mathfrak{p}$) so that the reduction:

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow G_\mathfrak{p}(2, \mathcal{O}_\mathfrak{p}) \rightarrow G_\mathfrak{p}(2, \mathbb{F})$$

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

Therefore, we do something different. SERRE has remarked, that mod $\mathfrak{p}$ 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 $\mathfrak{p}$, over the real cyclotomic field $\mathbb{Q}(\mu_p)^+$, $\overline{\rho}$ 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


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