MR1336749 (96e:11142) 11R33 (11G05 11G07)
Bayad, Abdelmejid (D-AGSB-MI)

Structure galoisienne d'anneaux d'entiers et courbes elliptiques sans multiplication complexe. (French. English summary) [Galois structure of rings of integers and elliptic curves without complex multiplication]

J. Number Theory **52** (1995), *no. 2,* 267–279.

The subject of this paper is the (integral) Galois module structure of an extension $M = K(E[l])/K$ given by adjoining the l-torsion points of the elliptic curve E. In contrast with the majority of existing work, the author assumes neither good reduction nor complex multiplication. On the other hand, a rather strict condition is imposed (namely, $E(K)[l] \neq 0$), and the base field is taken to be $F = K(\zeta_l)$ instead of K. The author defines (with notation which is a trifle awkward) a class of cases ("class A") by postulating the existence of $a \in K(E[l])$ with a specific decomposition into primes, governed by the prime factors of the discriminant of E/K. The main theorem is then as follows: If one has such a case, then O_M is free over the associated order in $F[\mathrm{Gal}(L/F)]$. The proof uses that M/F is l-Kummerian and proceeds by looking at ramification. It seems that it will be, in general, not easy to decide whether a given situation is "class A".

There is also a section on elliptic resolvents; these give arithmetic generators of L/F. Much more is shown, using previous work of W. Bley and the author: the decomposition of the principal ideal generated by the elliptic resolvent is given in terms of a quadratic Stickelberger element. The reviewer feels that this should have some impact on the proof of the main result, via some connection with the "class A" property. This does not seem to be the author's approach, however; the main result is proved just by assuming class A. It would be interesting to see whether the Stickelberger theory can perhaps be exploited in favorable cases in order to get rid of that latter assumption.

Reviewed by *Cornelius Greither*