New number fields with known p-class tower

Daniel C. Mayer

Denote by p a prime, by K a number field with p-class group $\mathrm{Cl}_p(K) \simeq (p,p)$, by $L_1,\ldots,L_{p+1}$ the unramified cyclic extensions of degree p of K, by $\varkappa(K)$ the p-capitulation type of K in $L_1,\ldots,L_{p+1}$, and by $\ell_p(K)$, resp. $G = \mathrm{Gal}(\mathrm{F}_p^\infty(K)|K)$, the length, resp. the group, of the p-class tower of K.

In the first two theorems, let $p=3$, and let $K=\mathbb{Q}(\sqrt{d})$, $d>0$, be a real quadratic field.

Theorem 1. (Mayer) Suppose that $\mathrm{Cl}_3(L_1) \simeq (27,9)$, and $\mathrm{Cl}_3(L_j) \simeq (9,3)$ for $2 \le j \le 4$. Assume that $\varkappa(K)$ neither contains a total capitulation nor a 2-cycle. If there exists an unramified cyclic cubic extension M of some L_j, $2 \le j \le 4$, with $\mathrm{Cl}_3(M) \simeq (27,3)$, resp. $\mathrm{Cl}_3(M) \simeq (9,3)$, then $\ell_3(K)=3$, $G \simeq \langle 729,54\rangle - \#2;2|4|6$ (e.g. $d = 342\,664$), resp. $\ell_3(K)=2$, $G \simeq \langle 2\,187,302|304|306\rangle$ (e.g. $d=4\,760\,877$).

Theorem 2. (Mayer) Suppose that $\mathrm{Cl}_3(L_j) \simeq (3,3,3)$ for $1 \le j \le 3$, and $\mathrm{Cl}_3(L_4) \simeq (9,3)$. Let $\tau^{(1)}(L_j) = [\tau_0(L_j);\tau_1(L_j)]$ be the IPAD (index-p abelianization data) of L_j for $1 \le j \le 4$. (See [1].)

If $\tau^{(1)}(L_1) = [1^3;(21^2,(1^3)^3,(1^2)^9)]$, $\tau^{(1)}(L_2) = [1^3;(21^2,(21)^{12})]$, $\tau^{(1)}(L_3) = [1^3;((21^2)^4,(2^2)^9)]$, and $\tau^{(1)}(L_4) = [21;(21^2,(21)^3)]$, then $G \simeq \langle 2\,187,273\rangle$ (e.g. $d=957\,013$).

If $\tau^{(1)}(L_1) = [1^3;(21^2,(1^3)^3,(1^2)^9)]$, $\tau^{(1)}(L_j) = [1^3;(21^2,(21)^{12})]$ for $2 \le j \le 3$, and $\tau^{(1)}(L_4) = [21;(21^2,(31)^3)]$, then $G \simeq \langle 2\,187,271|272\rangle$ (e.g. $d=2\,023\,845$).

If $\tau^{(1)}(L_1) = [1^3;((21^2)^4,(1^2)^9)]$, $\tau^{(1)}(L_j) = [1^3;(21^2,(21)^{12})]$ for $2 \le j \le 3$, and $\tau^{(1)}(L_4) = [21;(21^2,(21)^3)]$, then $G \simeq \langle 2\,187,270\rangle$ (e.g. $d=2\,303\,112$). In each of the three cases, $\ell_3(K)=3$.

In the next two theorems, let $p=5$.

Theorem 3. (Kishi, Mayer) Let $K=\mathbb{Q}((\zeta-\zeta^{-1})\sqrt{d})$ be a cyclic quartic field with $\zeta=\exp(\frac{1}{5}2\pi i)$ and $d>0$, $\gcd(d,5)=1$. If $\varkappa(K)$ is a 4-cycle (e.g. $d=457$), resp. the identity permutation (e.g. $d=581$), then $\ell_5(K)=2$, and $G \simeq \langle 3\,125,11\rangle$, resp. $G \simeq \langle 3\,125,14\rangle$.

Theorem 4. (Ayadi, Oumazouz, Mayer) Let K be a cyclic quintic field with conductor f divisible by two primes p,q which are mutual quintic

residues, and let γ be generator of a non-trivial primitive ambiguous principal ideal of K with norm $N_{K|\mathbb{Q}}(\gamma) = p^e q^u$. If $e = 0$ or $u = 0$, then $\ell_5(K) = 2$ (e.g. $f = 5\,921 = 31 \cdot 191$).

Reference. [1] D. C. Mayer, *Index-p abelianization data of p-class tower groups*, Adv. Pure Math. **5** (2015), no. 5, 286–313, DOI 10.4236/apm.2015.55029, Special Issue on Number Theory and Cryptography, April 2015.