Journal of Number Theory 147 (2015) 766–777

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

3-Class field towers of exact length 3

Michael R. Bush [a,*], Daniel C. Mayer [b]

[a] *Department of Mathematics, Washington and Lee University, Lexington, VA 24450, USA*
[b] *Naglergasse 53, 8010 Graz, Austria*

ARTICLE INFO

Article history:
Received 27 December 2013
Received in revised form 4 August 2014
Accepted 4 August 2014
Available online 6 October 2014
Communicated by David Goss

MSC:
primary 11R37
secondary 11R11, 11R29, 20D15, 20F14

Keywords:
p-Class field towers
Principalization of p-classes
Quadratic fields
Transfer map
Relation rank
Inversion automorphism
Schur σ-groups
Central series
Derived series

ABSTRACT

The p-group generation algorithm is used to verify that the Hilbert 3-class field tower has length 3 for certain imaginary quadratic fields K with 3-class group $\mathrm{Cl}_3(K) \cong [3,3]$. Our results provide the first examples of finite p-class towers of length > 2 for an odd prime p.

* Corresponding author.
E-mail addresses: bushm@wlu.edu (M.R. Bush), algebraic.number.theory@algebra.at (D.C. Mayer).
URL: http://www.algebra.at (D.C. Mayer).

http://dx.doi.org/10.1016/j.jnt.2014.08.010
0022-314X/

1. Introduction

In 1925, Schreier and Furtwängler [11, §15.1.1, p. 218] asked whether the ascending tower $K \leq \mathrm{F}^1(K) \leq \mathrm{F}^2(K) \leq \ldots$ of successive Hilbert class fields of an algebraic number field K can be infinite [13, §11.3, p. 46]. In their famous 1964 paper [12], Golod and Shafarevich gave an affirmative answer. They did this by proving that the tower of Hilbert p-class fields $K \leq \mathrm{F}_p^1(K) \leq \mathrm{F}_p^2(K) \leq \ldots$ (which sits inside the tower of Hilbert class fields) is infinite if the base field K has sufficiently large p-class rank $d_p(\mathrm{Cl}(K))$ where p is some prime. They combined this result with a theorem warranting large p-class rank $d_p(\mathrm{Cl}(K))$ whenever sufficiently many primes ramify completely in K with exponents divisible by p, and thus showed that the 2-tower of a quadratic field $K = \mathbb{Q}(\sqrt{D})$ with highly composite radicand D is infinite. For example, taking $D = -2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = -30\,030$ or $D = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9\,699\,690$ one obtains a 2-tower of length $\ell_2(K) = \infty$.

A year earlier, Shafarevich [26] had proved that if p is an odd prime then $r = d$ where $d = \dim_{\mathbb{F}_p}(\mathrm{H}_1(G, \mathbb{F}_p))$ and $r = \dim_{\mathbb{F}_p}(\mathrm{H}_2(G, \mathbb{F}_p))$ are the generator and relation ranks of the p-tower group $G = \mathrm{G}_p^\infty(K) = \mathrm{Gal}(\mathrm{F}_p^\infty(K)|K)$ and K is an imaginary quadratic field. Together with Vinberg's [27,24] general condition $r > \frac{1}{4}d^2$ for a finite p-tower group, this established the bound $d < 4$ for an imaginary quadratic field with finite p-tower, which was improved to $d < 3$ by Koch and Venkov [16] in 1975.

Since the generator rank d of G coincides with the p-class rank $d_p(\mathrm{Cl}(K))$ of K, the inequality $d < 3$ implies that the only imaginary quadratic fields K for which the length $\ell_p(K) \geq 2$ of their p-tower is an open problem (p an odd prime), are those with $d_p(\mathrm{Cl}(K)) = 2$. In the case $p = 3$, such fields were investigated by Scholz and Taussky [25]. They proved that $\ell_3(K) = 2$ if the second 3-class group $\mathrm{G}_3^2(K) = \mathrm{Gal}(\mathrm{F}_3^2(K)|K)$ of K is a metabelian 3-group in Hall's isoclinism family Φ_6, and their proof was confirmed with different techniques by Heider and Schmithals [14] in 1982 and by Brink and Gold [8] in 1987.

No cases of p-towers of finite length $\ell_p(K) > 2$ (p an odd prime) were known up to now and it is the main purpose of the present article to provide the first examples with $\ell_3(K) = 3$. We note that examples of 2-towers of length 3 have appeared previously in [9]. The main approach is to formulate conditions (see Theorem 4.1) that guarantee that the Galois group $\mathrm{G}_3^3(K) = \mathrm{Gal}(\mathrm{F}_3^3(K)|K)$ has derived length 3.

The layout of the paper is as follows. In Section 2, we recall certain properties shared by the Galois groups $G = \mathrm{G}_p^\infty(K) = \mathrm{Gal}(\mathrm{F}_p^\infty(K)|K)$ when K is an imaginary quadratic field. We also introduce the notions of transfer target type and transfer kernel type for the group G and explain how these can be computed arithmetically. In Section 3, we recall how the p-group generation algorithm can be used to enumerate finite p-groups of fixed generator rank d. We also explain how some of the arithmetic data introduced in Section 2 can be used to constrain this enumeration. Finally, in Section 4, we formulate conditions on G which are sufficient to cause an enumeration based search to terminate, allowing