Canad. Math. Bull. Vol. **45** (1), 2002 pp. 86–88

On Cyclic Fields of Odd Prime Degree p with Infinite Hilbert p-Class Field Towers

Frank Gerth III

Abstract. Let k be a cyclic extension of odd prime degree p of the field of rational numbers. If t denotes the number of primes that ramify in k, it is known that the Hilbert p-class field tower of k is infinite if $t > 3 + 2\sqrt{p}$. For each $t > 2 + \sqrt{p}$, this paper shows that a positive proportion of such fields k have infinite Hilbert p-class field towers.

Let p be an odd prime number, and let k be a cyclic extension of degree p over the field of rational numbers $\mathbb{Q}$. Let C_k be the p-class group of k (*i.e.*, the Sylow p-subgroup of the ideal class group of k). Let k_1 be the Hilbert p-class field of k. So k_1 is the maximal abelian unramified extension of k whose Galois group is a p-group. From class field theory, $C_k \cong \mathrm{Gal}(k_1/k)$. For $i \geq 2$, let k_i be the Hilbert p-class field of k_{i-1}. Then

$$k \subset k_1 \subset k_2 \subset \cdots \subset k_i \subset \cdots$$

is the Hilbert p-class field tower of k. If $k_i \neq k_{i-1}$ for each i, then the Hilbert p-class field tower of k is said to be *infinite*.

Let r_k be the rank of the p-class group of k. So

$$r_k = \operatorname{rank} C_k = \dim_{\mathbb{F}_p}(C_k/C_k^p). \tag{1}$$

Here $\mathbb{F}_p$ is the finite field with p elements, $C_k^p = \{a^p : a \in C_k\}$, and we are viewing the elementary abelian p-group C_k/C_k^p as a vector space over $\mathbb{F}_p$. It is known (*cf.* [1], p. 233) that the Hilbert p-class field tower of k is infinite if

$$r_k > 2 + 2\sqrt{p}. \tag{2}$$

Now let $G = \mathrm{Gal}(k/\mathbb{Q})$, and let σ be a generator of the cyclic group G. Then C_k is a module over the group ring $\mathbb{Z}[G]$. Since the norm map from the p-class group of k to the p-class group of $\mathbb{Q}$ is the trivial map, then $C_k^{1+\sigma+\cdots+\sigma^{p-1}} = \{1\}$. So we may view C_k as a module over $\mathbb{Z}[G]/(1+\sigma+\cdots+\sigma^{p-1})\mathbb{Z}[G]$. Note that

$$\mathbb{Z}[G]/(1+\sigma+\cdots+\sigma^{p-1})\mathbb{Z}[G] \cong \mathbb{Z}[\zeta]$$

where ζ is a primitive p-th root of unity. (The map $\mathbb{Z}[G] \to \mathbb{Z}[\zeta]$ induced by $\sigma \mapsto \zeta$ is a surjective homomorphism with kernel $(1+\sigma+\cdots+\sigma^{p-1})\mathbb{Z}[G]$.) Since the ideal

Received by the editors July 20, 2000.
AMS subject classification: 11R29, 11R37, 11R45.

$(1-\zeta)^{p-1}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta]$, then $C_k^{(1-\sigma)^{p-1}} = C_k^p$, where $C_k^{(1-\sigma)^i} = \{a^{(1-\sigma)^i} : a \in C_k\}$ for $i \geq 0$. Then

$$r_k = \operatorname{rank}(C_k/C_k^p) = \operatorname{rank}(C_k/C_k^{(1-\sigma)^{p-1}}) = \sum_{i=1}^{p-1} \operatorname{rank}(C_k^{(1-\sigma)^{i-1}}/C_k^{(1-\sigma)^i}). \tag{3}$$

Let t denote the number of primes that ramify in $k/\mathbb{Q}$. From genus theory it is known that

$$\operatorname{rank}(C_k/C_k^{1-\sigma}) = t-1. \tag{4}$$

From Inequality 2 and Equations 3 and 4, we see that the Hilbert p-class field tower of k is infinite if $t > 3 + 2\sqrt{p}$. We shall consider cases where $t > 2 + \sqrt{p}$. Let

$$s_k = \operatorname{rank}(C_k^{1-\sigma}/C_k^{(1-\sigma)^2}). \tag{5}$$

Then from Equations 3, 4, and 5,

$$r_k \geq t - 1 + s_k. \tag{6}$$

For each positive integer t and each positive real number x, we define

$$A_t = \{\text{cyclic extensions } k \text{ of } \mathbb{Q} \text{ of degree } p \text{ with exactly } t \text{ ramified primes}\}$$
$$A_{t;x} = \{k \in A_t : \text{ the conductor of } k \text{ is } \leq x\}$$
$$A_{t;x}^* = \{k \in A_{t;x} : \text{ Hilbert } p\text{-class field tower of } k \text{ is infinite}\}.$$

Next we define a density

$$d_t^* = \liminf_{x\to\infty} \frac{|A_{t;x}^*|}{|A_{t;x}|} \tag{7}$$

where $|A|$ denotes the cardinality of a set A. Since $A_{t;x}^* = A_{t;x}$ for $t > 3 + 2\sqrt{p}$, we know that $d_t^* = 1$ for $t > 3 + 2\sqrt{p}$. Our main result is the following theorem.

Theorem *Let d_t^* be defined by Equation 7. Then $d_t^* = 1$ for $t > 3+2\sqrt{p}$. Furthermore, $d_t^* > 0$ for $t > 2+\sqrt{p}$. In other words, for each integer $t > 2+\sqrt{p}$, a positive proportion of the cyclic extensions of $\mathbb{Q}$ of odd prime degree p with exactly t ramified primes have infinite Hilbert p-class field towers.*

Proof With s_k defined by Equation 5, we define for nonnegative integers s

$$A_{t,s;x} = \{k \in A_{t;x} : s_k = s\}$$

and

$$d_{t,s} = \lim_{x\to\infty} \frac{|A_{t,s;x}|}{|A_{t;x}|}. \tag{8}$$

From Equation 3 in [2],

$$d_{t,s} = \Big[\prod_{i=1}^{t-1-s}\Big(1-\frac{1}{p^{t+1-i}}\Big)\Big]\cdot\frac{1}{p^{ts}}\cdot\sum_{\substack{i_1+\cdots+i_{t-1-s}\le s\\ \text{each } i_j\ge 0}}\Big(\prod_{j=1}^{t-1-s}p^{ji_j}\Big) \tag{9}$$

for $0 \le s \le t-2$. When $s = t-1$, $d_{t,t-1} = p^{-t(t-1)}$. Now if $t > 2+\sqrt{p}$ and $s_k = t-1$, then from Inequality 6, $r_k > 2 + 2\sqrt{p}$. Hence from Inequality 2, the Hilbert p-class field tower of k is infinite. So for $t > 2+\sqrt{p}$,

$$d_t^* \ge d_{t,t-1} = p^{-t(t-1)} > 0,$$

which completes the proof of the theorem.

We now consider the special case $p = 3$, and we shall use Equation 9 to give somewhat more detailed results in this case. From Inequality 2, a cyclic cubic field k has an infinite Hilbert 3-class field tower if $r_k \ge 6$. So if $t \ge 7$, then $d_t^* = 1$. From the Theorem, $d_t^* > 0$ for $t \ge 4$. For cyclic cubic fields with exactly four ramified primes,

$$d_4^* \ge d_{4,3} = 3^{-12}.$$

For cyclic cubic fields with exactly five ramified primes,

$$d_5^* \ge d_{5,2} + d_{5,3} + d_{5,4} > .002.$$

For cyclic cubic fields with exactly six ramified primes,

$$d_6^* \ge d_{6,1} + d_{6,2} + d_{6,3} + d_{6,4} + d_{6,5} > .159.$$

References

[1] J. Cassels and A. Fröhlich, *Algebraic Number Theory*. Academic Press, London, New York, 1986.
[2] F. Gerth, *Densities for ranks of certain parts of p-class groups*. Proc. Amer. Math. Soc. **99**(1987), 1–8.

Department of Mathematics
The University of Texas at Austin
Austin, Texas 78712-1082
U.S.A.
e-mail: gerth@math.utexas.edu