Class Field Towers

Matthew Warren

Small note going through chapter IX of ANT - Cassels and Frohlich because I found it interseting.

When writing my part III essay, I was mulling over some results that held in $\mathbb{Q}$, because we can take gcds in $\mathbb{Z}$, and was wondering how to generalise to K a number field. Of course, we can take gcds in any UFD (ie. a UFD is a gcd-domain) so I wondered if we could *embed* a number field K into a field with class number 1.

Turns out that in the classic text Algebraic Number Theory edited by Cassels and Fröhlich, there was a chapter dedicated to this question. This is just me outlining these results to myself.

Question: Let K be a number field, can we embed K into a finite extension L with $h_L = 1$?

Well, a natural seeming course of action is to take the Hilbert class field F of K - that is, the maximal unramified extension of K, or equivalently, the ray class field of the ideal class group! - because the degree $[F : K]$ is equal to h_K. Hence if we were to repeatedly do this to get a tower

$$K \subset K_1 \subset K_2 \subset \dots$$

of Hilbert class fields, then if this stabilises in finitely many iterations we have a solution.

Follow-up question: Does the converse hold? If this sequence does not stabilise, can there still be a solution to our embedding problem?

Note that if K_∞ is the union of the field in our tower, then the tower stabilises if and only if K_∞ has finite degree over K.

Proposition 1 There exists a finite extension L/K with $h_L = 1$ if and only if the Hilbert class field tower stabilises.

Proof. We have remarked that $\Longleftarrow$ is obvious. For the converse, suppose that such an L exists. We want to show that $K_i \subset L$ for all $i \geq 0$ (where $K = K_0$), which can be done by induction as follows. Indeed, K_i/K_{i-1} is unramified with abelian Galois group G, thus LK_i/L is also an unramified abelian extension and therefore contained in the Hilbert class field of L. But L is its own Hilbert class field, because $h_L = 1$, so we deduce that $K_i \subset LK_i \subset L$, as required.

Therefore, if L exists then $K_\infty \subset L$, meaning K_∞ has finite degree over K, and so the class field tower stabilises. □

Ok, so we've rephrased the question, and notice that if there exists a solution, then K_∞ is the smallest such solution. Now we *further* rephrase the question as follows:

Let p be a prime, a p-extension of K is a Galois extension L/K such that $\mathrm{Gal}(L/K)$ is a p-group. Then we consider a new tower!
Let $K_i^{(p)}$ be the maximal p-extension of $K_{i-1}^{(p)}$ contained in its Hilbert class field. Note that there is a unique such maximal p-extension because abelian groups have unique Sylow p-subgroups. We shall call $K_1^{(p)}$ the Hilbert p-class of K, so we have a Hilbert p-class tower

$$K \subset K_1^{(p)} \subset K_2^{(p)} \subset \dots$$

Claim: $K_i^{(p)} \subset K_i$

Proof. We shall induct on i, noting that the case for $i = 1$ is trivial. Let l_i be the Hilbert class field of $K_i^{(p)}$, and assume that that $K_i^{(p)} \subset K_i$.
We have $l_i K_i / K_i$ is an unramified Abelian extension of K_i and hence contained in K_{i+1}. But by its definition $K_{i+1}^{(p)} \subset l_i$, hence we have

$$K_{i+1}^{(p)} \subset l_i \subset l_i K_i \subset K_{i+1}.$$

□

Now, setting $K_\infty^{(p)}$ as the union of our p-class tower, we have that if $K_\infty^{(p)}$ has infinite degree over K, then $K_\infty^{(p)} \subset K_\infty$ implies that K_∞ must also be of infinite degree. Hence to disprove the existence of L/K finite such that $h_L = 1$, we only need to look at the Hilbert p-class tower.

This leads to the main result of the chapter, which proves that the Hilbert class field tower may be infinite. Given a group G, let G/p be the maximal abelian quotient with exponent p. We can then regard this as an $\mathbb{F}_p$ vector space and define $d^{(p)}G := \dim_{\mathbb{F}_p}(G/p)$. Notice that we have G^{ab} the maximal Abelian quotient, and if this is finitely generated we may use the structure theorem to say

$$G^{\mathrm{ab}} \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{d_t\mathbb{Z}} \oplus \mathbb{Z}^r$$

for some $d_1, d_2, \dots, d_t$ prime powers and $r \geq 0$. Then $d^{(p)}G$ is simply the number of factors in the finite part with order a power of p, plus the rank r.
The main theorem is due to Golod and Shafarevich:

Theorem 2 There exists a function $\gamma(n)$ such that $d^{(p)}Cl_K < \gamma(n)$ for any K with $n = [K : \mathbb{Q}]$ and a finite p-class field tower.

In fact we can show

$$d^{(p)}Cl_K < 2 + 2\sqrt{r_K + \delta_K^{(p)}} \tag{1}$$

where r_K is the number of infinite primes of K, and

$$\delta_K^{(p)} = \begin{cases} 1 & \text{if } K \text{ contains all } p\text{th roots of unity,} \\ 0 & \text{otherwise.} \end{cases}$$

Now, suppose that $K/\mathbb{Q}$ is Galois for simplicity, then given some finite prime q in $\mathbb{Z}$, let $e_K(q)$ be the common ramification index $e(\mathfrak{q}/q)$ of all primes lying over q. Then let $t_K^{(p)}$ be the number of ramified q such that $p \mid e_K(q)$. (Note; the results will also hold for non-Galois extensions with some minor modifications)

Theorem 3 There exists a function $c(n)$ such that $d^{(p)}Cl_K \geq t_K^{(p)} - c(n)$, where $n = [K : \mathbb{Q}]$.

In particular, we can show

$$d^{(p)}Cl_K \geq t_K^{(p)} - \left(\frac{r_K - 1}{p - 1} + \operatorname{ord}_p(n)\delta_K^{(p)}\right). \tag{2}$$

These theorems are both somewhat lengthy to prove - I may write this up from my notes later. For now, we just consider that combining these results gives

Corollary 4 If K an number field of degree n, and

$$t_K^{(p)} \geq \gamma(n) + c(n)$$

then the p-class field tower of K is infinite!

This just amounts to noting that if K had finite p-class field tower, then we'd have by combining our inequalities above that $\gamma(n) > t_K^{(p)} - c(n)$.

Cool, this gives us the necessary ingredients to construct a field with no solution to the embedding problem. Indeed, consider the case of quadratic extensions with $p = 2$, then $K/\mathbb{Q}$ is Galois automatically, $\delta_K^{(2)} = 1$, and

$$r_K = \begin{cases} 1 & K \text{ imaginary,} \\ 2 & K \text{ real.} \end{cases}$$

So, consider $K = \mathbb{Q}(\sqrt{-q_1 q_2 ... q_m})$ with q_i distinct primes. We have that $t_K^{(p)}$ is just equal to the number of ramified primes - which will be m (or $m+1$ if 2 is not included in our list, and we have $-\prod q_i \equiv 1 \mod 4$)- and then we can use the inequalities (1) and (2) do determine that K has an infinite 2-class field tower if

$$\begin{aligned} m &\geq 2 + 2\sqrt{r_K + \delta_K^{(p)}} + \left(\frac{r_K - 1}{p - 1} + \operatorname{ord}_p(n)\delta_K^{(p)}\right) \\ &= 2 + 2\sqrt{2} + 1 \\ &= 5.8284271\ldots \end{aligned}$$

Hence, taking $m = 6$ we have a solution!