HOMOGENEOUS SPLITTING IN CUBIC NUMBER FIELDS WITH $h_K = 3$

STEVEN CHARLTON

Contents

1. Splitting of p in cubic number fields

Let K be a cubic number field, with class number $h_K = 3$. Then the class group $\mathcal{C}(K)$ is isomorphic to $\mathbb{Z}_3$, where 0 corresponds to the principal ideal class, and 1 and 2 correspond to different non-principal ideal classes. Consider how a prime p in $\mathbb{Z}$ can split in K. Excluding the finite number of primes which ramify, the following are the only possibilities

i) $p\mathcal{O}_K$ is inert, with $f(p\mathcal{O}_K \mid p) = 3$,
ii) $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{q}_1$ with $f(\mathfrak{p}_1 \mid p) = 1$ and $f(\mathfrak{q}_1 \mid p) = 2$, or
iii) $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with $f(\mathfrak{p}_i \mid p) = 1$, so $p\mathcal{O}_K$ splits completely.

Notice that case ii) above can only occur if the field $K/\mathbb{Q}$ is non-Galois since the two primes have different inertial degrees.

Regardless of how the prime (p) splits in K, the factorisation must produce a consistent equation in the class group of K. Case i) is trivial in this regard, because the ideal $p\mathcal{O}_k$ is principal, and there is actually no equation to satisfy. Case ii) is almost as trivial; since $p\mathcal{O}_k$ is principal, we get $[\mathfrak{p}_1] = [\mathfrak{q}_1]^{-1}$ in $\mathcal{C}(K)$. Case iii) is more interesting since the following equations hold in the class group

$$\begin{aligned} 0 &= 0 + 0 + 0 \\ &= 1 + 1 + 1 \\ &= 2 + 2 + 2 \\ &= 0 + 1 + 2\,. \end{aligned}$$

A priori nothing seems to prevent any of the four cases occurring when the prime p splits completely, but curiously the last case appears not to occur in certain number fields.

Definition 1.1 (Homogeneous splitting)**.** Let K be a cubic number field, with class number $h_K = 3$. Let $p \in \mathbb{Z}$ be a prime which does not ramify in K. I shall say K has *homogeneous*

Date: June 29, 2016.

splitting if complete splitting $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ implies $[\mathfrak{p}_1] = [\mathfrak{p}_2] = [\mathfrak{p}_3]$ in $\mathcal{C}(K)$. Otherwise K has *non-homogeneous splitting.*

This write-up stems from the initial curious observation that $\mathbb{Q}(\sqrt[3]{7})$ appears to have homogeneous splitting. This observation appeared whilst investigating the representation of primes by ternary cubic forms, and relating this to the ideal classes in a cubic number field in analogy with the quadratic case. This homogeneous splitting was noted in connection with the splitting of the defining polynomial of the Hilbert class field of $\mathbb{Q}(\sqrt[3]{7})$, specifically the apparent lack of splitting into factors of degree $(1, 1, 1, 3, 3)$ modulo p.

Once the splitting field of the Hilbert class field of $\mathbb{Q}(\sqrt[3]{7})$ is known, homogeneous splitting can be proven easily. There is a condition on the degree of this splitting field which implies homogeneous splitting, and conversely if this condition fails, I can prove non-homogeneous splitting must occur using the Chebotarev density theorem.

2. Hilbert class field of K, and its splitting field

For a field K as above, consider the Hilbert class field H. We know that $h_K = 3$, and $\operatorname{Gal}(H/K) \cong \mathcal{C}(K)$ which means H/K has degree 3 and $H/\mathbb{Q}$ has degree 9.

If $K/\mathbb{Q}$ is Galois, then a standard argument shows that $H/\mathbb{Q}$ is also Galois. H is the maximal unramified Abelian extension of K, and any conjugate of $H/\mathbb{Q}$ is also an unramified Abelian extension of K. Therefore any conjugate of $H/\mathbb{Q}$ is contained in H, and for degree reasons is in fact equal. This means $H/\mathbb{Q}$ is equal to all its conjugates, and so is Galois.

If $K/\mathbb{Q}$ is non-Galois, then $H/\mathbb{Q}$ cannot be Galois. If $H/\mathbb{Q}$ were Galois, then $G := \operatorname{Gal}(H/\mathbb{Q}) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ or $\cong \mathbb{Z}_9$ by the classification of groups of order p^2. So $K/\mathbb{Q}$ would correspond to a subgroup of $G = \operatorname{Gal}(H/\mathbb{Q})$ of index 3. Such a subgroup would necessarily be normal, since G is Abelian. But normal subgroups of the Galois group correspond to Galois extensions of the base field, which means $K/\mathbb{Q}$ would be Galois.

Consider now the splitting field S of the Hilbert class field $H/\mathbb{Q}$, which fits into the following field diagram.

$$\begin{tikzcd}
S \arrow[ddd, dash] \arrow[dr, dash] & \\
& H \arrow[d, dash, "h_K = 3"] \\
& K \arrow[dl, dash, "3"] \\
\mathbb{Q} &
\end{tikzcd}$$

Proposition 2.1. *The degree of the splitting field S/H is either $1, 2, 6$ or 18. This corresponds to degrees $9, 18, 54$ or 162 as an extension of $\mathbb{Q}$.*

Proof. The degree of S/H is 1 if and only if $H/\mathbb{Q}$ is Galois, which is if and only if $K/\mathbb{Q}$ itself is Galois. We can therefore assume that $K/\mathbb{Q}$, and $H/\mathbb{Q}$ are non-Galois, and show one of the remaining cases holds.

The splitting field of $K/\mathbb{Q}$ has degree 2 over K and degree 6 over $\mathbb{Q}$. This is a standard result, namely let $f(x)$ is the defining polynomial of K, with roots $\alpha_1, \alpha_2, \alpha_3$. Then K is obtained by attaching α_1, but since K is not Galois, $\alpha_2, \alpha_3 \notin K$. Dividing out $f(x)/(x - \alpha_1)$ gives an irreducible quadratic polynomial over K which has roots α_2, α_3. Attaching α_2 to K gives $\widetilde{K}$ a degree 2 extension of K, a degree 6 extension of $\mathbb{Q}$. And then already $\alpha_3 \in \widetilde{K}$, since $\alpha_2\alpha_3, \alpha_2 \in \widetilde{K}$. So $f(x)$ splits completely in $\widetilde{K}$, and this is the splitting field of K.

Consider the extension H/K, and find some $\alpha_1 \in H \setminus K$. Since H/K is Galois, we get conjugates $\alpha_2 := \alpha_1^\sigma, \alpha_3 := \alpha_1^{\sigma^2}$ in H, where $\mathrm{Gal}(H/K) \cong \mathbb{Z}_3$ is generated by σ.

Let $h(x)$ be the defining polynomial for $H/\mathbb{Q}$, with roots $\alpha_1, \dots, \alpha_9$. Since H/K is Galois, each conjugate H'/K' will also be Galois, where K' is one of the conjugates of $K/\mathbb{Q}$. This means there are 3 conjugates H, H', H'', over K, K', K'' respectively, and we can therefore group the roots such that $\alpha_{1,2,3} \in H$, $\alpha_{4,5,6} \in H'$ and $\alpha_{7,8,9} \in H''$. Consider the polynomial $g(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Since the $\alpha_{1,2,3}$ are conjugates over K, this polynomial is in $K[x]$, and is irreducible here since $\alpha_1 \notin K$. Therefore $g(x)$ is the minimal polynomial for α_1 over K.

Since $h(x)$ is a polynomial over K (in fact $\mathbb{Q}$) with root α_1, and $g(x)$ is the minimal polynomial for α_1 over K, the standard argument using the division algorithm shows $g \mid h$ in $K[x]$. If $g'(x)$ is the minimal polynomial for α_4 over K', and $g''(x)$ for α_7 over K'', we have $g' \mid h$ in $K'[x]$ and $g'' \mid h$ in $K''[x]$ by exactly the same argument.

Consider now the splitting field $\widetilde{K}$ of K. The splitting field of $H/\mathbb{Q}$, whatever it is, must contain $\widetilde{K}$, so let's start here. Furthermore, $\widetilde{K}$ contains K, K', K''. So in $\widetilde{K}[x]$ the polynomial $h(x)$ of $H/\mathbb{Q}$ splits into three cubic factors as $h(x) = g(x)g'(x)g''(x)$.

We obtain the splitting field of $H/\mathbb{Q}$ by making the factors $g(x)$, $g'(x)$ and $g''(x)$ split completely. And since H/K, H'/K', H''/K'' are Galois, attaching one root of g, g', g'' makes that factor split completely. We must attach first the root α_1 of $g(x)$ to $\widetilde{K}$ get a field $F_1 := \widetilde{K}(\alpha_1)$ containing H, wherein $g(x)$ has split completely. Then $F_1/\mathbb{Q}$ has degree $6 \times 3 = 18$. If this is not the splitting field, one of g', g'' has no split. Say, by reordering the roots, it is g'. Attach α_4 to F_1 to get $F_2 := \widetilde{K}(\alpha_1, \alpha_4)$. Then $F_2/\mathbb{Q}$ has degree $18 \times 3 = 54$. If this is still not the splitting field g'' has not split, so attach α_7 to F_2 to get $F_3 := \widetilde{K}(\alpha_1, \alpha_4, \alpha_7)$. Then $F_3/\mathbb{Q}$ has degree $54 \times 3 = 162$. At this point the polynomial $f(x)$ definitely has split completely, so we have found the splitting field.

If S is the splitting field of $L/\mathbb{Q}$, then by the tower law $[S\colon L][L\colon \mathbb{Q}] = [S\colon \mathbb{Q}]$, so that $[S\colon L] = [S\colon \mathbb{Q}]/9$. If $S = F_1$, then $[S\colon L] = 18/9 = 2$. If $S = F_2$, then $[S\colon L] = 54/9 = 6$. Finally if $S = F_3$, then $[S\colon L] = 162/9 = 18$. This proves the proposition. □

Remark 2.2. It appears generally that $[S\colon L] = 2$, or $[S\colon L] = 6$. If one were to study the situation in the Proposition 2.1 in greater detail, one could presumably establish that once g, g' split, the factor g'' must also split automatically. This would eliminate the case where $[S\colon L] = 18$. But as yet, this would seem to take more effort than I am willing to make.

3. Splitting of p in the Hilbert class field H of K

Now we look at how the prime p can splits in K, and what impact this has on the splitting on the Hilbert class field H. We shall analyse what happens with the factorisation in cases i) to iii), and the subcases of these where the ideals in the factorisation fall into the various different ideal classes in $\mathcal{C}(K)$. Using Dedekind's theorem, we will relate these to the factorisation modulo p of the polynomials $f_K(x)$ defining $K/\mathbb{Q}$, and $f_H(x)$ defining the Hilbert class field $H/\mathbb{Q}$. Recall that the degrees of the irreducible factors of $f_K(x)$ modulo p are the inertial degrees of the prime ideals above p in K.

***p* is inert in *K*:** So $p\mathcal{O}_K$ is prime, with $f(p\mathcal{O}_K \mid p) = 3$. Therefore $f_K(x)$ is irreducible modulo p. The ideal $p\mathcal{O}$ is principal, so splits completely in the Hilbert class field as $p\mathcal{O}_H = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, with $f(\mathfrak{P}_i \mid p\mathcal{O}_H) = 1$. Multiplicativity of f means $f(\mathfrak{P}_i \mid p) = 3$, so $f_H(x)$ factors with degrees $(3, 3, 3)$ modulo p.

$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{q}_1$ in K: We have $f(\mathfrak{p}_1 \mid p) = 1$ and $f(\mathfrak{q}_1 \mid p) = 2$, so modulo p $f_K(x)$ factors with degrees $(1, 2)$. Since $[\mathfrak{p}_1] = [\mathfrak{q}_1]^{-1}$, either both ideals are principal, or both ideals are non-principal.

If $\mathfrak{p}_1$ is principal, then it splits completely in H/K as $\mathfrak{p}_1\mathcal{O}_H = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ with $f(\mathfrak{P}_i \mid \mathfrak{p}_1) = 1$. Since $\mathfrak{q}_1$ is also principal, we get complete splitting in H/K as $\mathfrak{q}_1 = \mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3$ with $f(\mathfrak{Q}_i \mid \mathfrak{q}_1) = 1$. Multiplicativity means $f(\mathfrak{Q}_i \mid p) = 2$ and $f(\mathfrak{P}_i \mid p) = 1$. Therefore $f_H(x)$ factors with degrees $(1, 1, 1, 2, 2, 2)$ modulo p.

If $\mathfrak{p}_1$ is non-principal, it does not split completely in H/K. But since H/K is Galois with prime degree, the only other possibility is that $\mathfrak{p}_1$ is inert. Therefore $\mathfrak{p}_1\mathcal{O}_H$ is prime in L, with $f(\mathfrak{p}_1\mathcal{O}_H \mid \mathfrak{p}_1) = 3$. And $\mathfrak{q}_1\mathcal{O}_H$, similarly, is prime in L with $f(\mathfrak{q}_1\mathcal{O}_H \mid \mathfrak{q}_1) = 3$. Multiplicativity means $f(\mathfrak{p}_1\mathcal{O} \mid p) = 3$ and $f(\mathfrak{q}_1\mathcal{O}_H \mid p) = 6$. Therefore $f_H(x)$ factors with degrees $(3, 6)$ modulo p.

$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in K: So p splits completely in K. We have $f(\mathfrak{p}_i \mid p) = 1$, so $f_K(x)$ factors with degrees $(1, 1, 1)$ modulo p. From the previous discussion there are four cases to consider, where all $\mathfrak{p}_i$ are principal; all $\mathfrak{p}_i$ are non-principal of class 1; all $\mathfrak{p}_i$ are non-principal of class 2; or the $\mathfrak{p}_i$ are of three different classes.

If all $\mathfrak{p}_i$ are principal, then each $\mathfrak{p}_i$ splits completely in H/K as $\mathfrak{p}_i\mathcal{O}_H = \mathfrak{P}_{i,1}\mathfrak{P}_{i,2}\mathfrak{P}_{i,3}$, with $f(\mathfrak{P}_{i,j} \mid \mathfrak{p}_i) = 1$. By multiplicativity $f(\mathfrak{P}_{i,j} \mid p) = 1$. So $f_H(x)$ factors with degrees $(1, 1, 1, 1, 1, 1, 1, 1, 1)$ modulo p.

If all $\mathfrak{p}_i$ are non-principal of either class – we can't distinguish with H(!) – then each $\mathfrak{p}_i$ does not split completely in H/K. Since H/K is Galois with prime degree, they therefore remain inert. So $\mathfrak{p}_i\mathcal{O}_H$ is prime in L with $f(\mathfrak{p}_i\mathcal{O}_H \mid \mathfrak{p}_i) = 3$. By multiplicativity $f(\mathfrak{p}_i\mathcal{O}_H \mid p) = 3$. So $f_H(x)$ factors with degrees $(3, 3, 3)$ modulo p.

If the $\mathfrak{p}_i$ are of three different classes, then say $\mathfrak{p}_1$ is principal, $\mathfrak{p}_2$ is non-principal of class 1, and $\mathfrak{p}_3$ is non-principal of class 2. From the above discussion we know $\mathfrak{p}_1$ splits complete as $\mathfrak{p}_1\mathcal{O}_H = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ with $f(\mathfrak{P}_i \mid p) = 1$. But both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are inert in H, so $\mathfrak{p}_2\mathcal{O}_H$ and $\mathfrak{p}_3\mathcal{O}_H$ are prime with $f(\mathfrak{p}_2\mathcal{O}_H \mid p) = 3$ and $f(\mathfrak{p}_3\mathcal{O}_H \mid p) = 3$. Therefore $f_H(x)$ factors with degrees $(1, 1, 1, 3, 3)$ modulo p.

This discussion can be summarised by the following table

In K	Subcases	f_K degrees	f_H degrees
$p\mathcal{O}_K$ prime	$p\mathcal{O}_K$ principal	(3)	(3,3,3)
$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{q}_1$	$\mathfrak{p}_1$, $\mathfrak{q}_1$ principal	(1,2)	(1,1,1,2,2,2)
	$\mathfrak{p}_1$, $\mathfrak{q}_1$ non-principal	(1,2)	(3,6)
$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_i$ all principal	(1,1,1)	(1,1,1,1,1,1,1,1,1)
	$\mathfrak{p}_i$ all non-principal	(1,1,1)	(3,3,3)
	$\mathfrak{p}_i$ all different classes	(1,1,1)	(1,1,1,3,3)

The upshot of this is that non-homogeneous splitting is detected uniquely by factorisation of $f_H(x)$ modulo p having degrees $(1, 1, 1, 3, 3)$. If this occurs, when we have non-homogeneous splitting, and if it does not occur then we have homogeneous splitting.

The goal of the remaining sections will be to prove the following theorem

Theorem 3.1. *Let K be a cubic number field with $h_K = 3$, and let H/K its Hilbert class field. Let S be the splitting field of $H/\mathbb{Q}$, with $d = [S\colon H]$. Then K has homogeneous splitting if and only if $d \leq 2$.*

4. $[S\colon H] \leq 2$ implies homogeneous splitting

Suppose that $[S\colon H] \leq 2$, and suppose some prime p splits in a non-homogeneous way in K. So $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with $\mathfrak{p}_1$ principal, and $\mathfrak{p}_2, \mathfrak{p}_3$ non-principal, say. Then let $\mathfrak{P}_1$ be a prime in H above the principal prime $\mathfrak{p}_1$. From the discussion previously, we know $f(\mathfrak{P}_1 \mid p) = 1$. The prime in H above $\mathfrak{p}_2$ is $\mathfrak{p}\mathcal{O}_H$, since $\mathfrak{p}_2$ is inert, and $f(\mathfrak{p}_2\mathcal{O}_H \mid p) = 3$.

Let $\mathfrak{R}_1$ be a prime above $\mathfrak{P}_1$ in S. It is not clear how $\mathfrak{P}_1$ behaves in S/H, but regardless we have $f(\mathfrak{R}_1 \mid \mathfrak{P}_1) \leq [S\colon K] \leq 2$. Let $\mathfrak{R}_2$ be a prime above $\mathfrak{p}_2\mathcal{O}_H$ in S. Again it is not clear how $\mathfrak{p}\mathcal{O}_H$ behaves in S/H, but we do have $f(\mathfrak{R}_2 \mid \mathfrak{p}_2\mathcal{O}_H) \geq 1$.

This information fits into the following field diagram.

$$\begin{tikzcd}
S \text{ with } \mathfrak{R}_1 \text{ above } \mathfrak{P}_1, \text{ and } \supset \mathfrak{R}_2 \text{ above } \mathfrak{p}_2\mathcal{O}_H \arrow[dr, dash, "\leq 2"] \arrow[ddd, dash, "\leq 18"'] & \\
& H \text{ with } \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 = \mathfrak{p}_1\mathcal{O}_H, \text{ and } \supset \mathfrak{p}_2\mathcal{O}_H \arrow[d, dash, "h_K = 3"] \\
& K \text{ with } \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = p\mathcal{O}_K \arrow[dl, dash, "3"] \\
\mathbb{Q} \supset (p) &
\end{tikzcd}$$

By multiplicativity we have $f(\mathfrak{R}_1 \mid p) \leq 1 \times 2 = 2$, and $f(\mathfrak{R}_2 \mid p) \geq 3 \times 1 = 3$. But this is not possible in the Galois extension $S/\mathbb{Q}$, every prime above p must have the same inertial degree. This proves that the splitting of p in K must be homogeneous.

5. $[S\colon H] > 2$ implies non-homogeneous splitting

This direction is a little more delicate, at the moment. It relies on the classification of transitive groups of degree 9, and the Chevotarev density theorem. With more work in Proposition 2.1, one could presumably even determine the exact structure of the Galois group in the case where $[S\colon K] = 1, 2,$ or 6. But again this is more effort than I want to expend.

Recall the Chebotarev density theorem, phrased in terms of the splitting of a polynomial modulo p goes as follows.

Theorem 5.1 (Chebotarev density theorem). *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial with $\deg(f) = n$. Let $E = \mathbb{Q}(\alpha)$ where α is a root of $f(x)$, and let F be the normal closure of E. Let $P = (n_1, \ldots, n_r)$ be a partition of n. Let $\mathcal{S}$ be the set of unramified primes, and $\mathcal{S}_P$ be the set of unramified primes p for which $f(x)$ factors modulo p into irreducibles of degree $(n_1, \ldots, n_r)$. Let $G = \mathrm{Gal}(F/\mathbb{Q})$ be the Galois group of E, viewed as a subgroup of the symmetric group Σ_n. And let G_P be the set of elements of G with cycle type $(n_1, \ldots, n_r)$. Then the density $\delta(\mathcal{S}_P)$ of $\mathcal{S}_P$ satisfies*

$$\lim_{N\to\infty} \frac{\#\{\, p \in \mathcal{S}_p \mid p \leq N \,\}}{\#\{\, p \in \mathcal{S} \mid p \leq N \,\}} =: \delta(\mathcal{S}_p) = \frac{\#G_P}{\#G} \,.$$

In particular, if $\#G_P > 0$, then $\mathcal{S}_P \neq \emptyset$, and there exists some prime p for which $f(x)$ factors modulo p with degrees $P = (n_1, \ldots, n_r)$, and in fact infinitely many.

Recall from Proposition 2.1, if $[S\colon H] > 2$, then $[S\colon H] = 6$ or 18. Which then corresponds to $[S\colon \mathbb{Q}] = 54$ or 162. The Galois group of $H/\mathbb{Q}$ then corresponds to a transitive group of degree 9 of order 54 or 162. (Here 9 corresponds to the degree of $H/\mathbb{Q}$, and of the polynomial $f_H(x)$. The order 54 or 162 is the degree of the splitting field $S/\mathbb{Q}$.) When $[S\colon H] \leq 2$, we get $[S\colon \mathbb{Q}] = 9$ or 18 giving transitive groups groups of degree 9 and order 9 or 18.

Butler and McKay [BM83] classify the transitive groups of degree up to 11 (and in particular degree 9). Those groups relevant to us are summarised in the following table by limiting the groups to those of degree 9 and order 54 or 162. Those of order 9 and 18 are also included for completeness to illustrate how homogeneous splitting in the previous section also follows from Chebotarev (at least for all but finitely many primes).

Group G	Name	Order $\#G$	$\#G_{(1,1,1,3,3)}$
9T1	$C(9) = 9$	9	0
9T2	$E(9) = 3 \boxtimes 3$	9	0
9T3	$D(9) = 9 : 2$	18	0
9T4	$S(3) \boxtimes 3$	18	0
9T5	$S(3)[\frac{1}{2}]S(3) = 3^2 : 2$	18	0
9T10	$[3^2]S(3)_6$	54	6
9T11	$E(9) : 6 = \frac{1}{2}[3^2 : 2]S(3)$	54	6
9T12	$[3^2]S(3)$	54	6
9T13	$E(9) : D_6 = [3^2 : 2]3 = [\frac{1}{2}S(3)^2]3$	54	6
9T20	$[3^3]S(3) = 3 \wr S(3)$	162	12
9T21	$\frac{1}{2}[3^3 : 2]S(3)$	162	12
9T22	$[3^3 : 2]3$	162	12

From this table we can see that groups of order 54 or 162 always have $\#G_{(1,1,1,3,3)} > 0$. From Chebotarev, this means that there exist some prime p for which $f_H(x)$ factors modulo p into degrees $(1, 1, 1, 3, 3)$. By the analysis of the prime decomposition in K, and H from section 3, this type of splitting occurs only for non-homogeneous splitting of p. Therefore if $[S\colon H] > 2$, the field K has non-homogeneous splitting.

Remark 5.2. In all the cases I have explicitly calculated so far, the splitting field has degree $[S\colon H] = 1, 2$ or 6. And the structure of the Galois group depends only on $[S\colon H]$, as follows.

$[S\colon H]$	$\mathrm{Gal}(H/\mathbb{Q})$	Name
1	9T2	$E(9) = 3 \boxtimes 3$
2	9T4	$S(3) \boxtimes 3$
6	9T12	$[3^2]S(3)$

With more effort in Proposition 2.1, this could probably be proven explicitly.

Remark 5.3. One question really remains. Given a cubic number field K with $h_K = 3$, how can one determine whether $[S\colon H] = 2$ or 6 from the arithmetic of K itself?

6. Tighter bound on the degree of the splitting field S of H

In Proposition 2.1, we established that the degree of the splitting field S of the Hilbert class field H of the pure cubic field $K = \mathbb{Q}(\sqrt[3]{n})$ of class number $h_K = 3$ satisfies $[S\colon H] = 1, 2, 6, 18$. Moreover we observed that in calculations the case $[S\colon H] = 18$ never occurs. We will give a proof of this now, by appealing to certain facts about the class number of the normal closure of $\mathbb{Q}(\sqrt[3]{n})$.

Theorem 2 in [Rei05] establishes the following result about the class number h_L of the normal closure $L = \overline{K} = \mathbb{Q}(\sqrt[3]{n}, \zeta_3)$ of K in terms of the class number h_K of $K = \mathbb{Q}(\sqrt[3]{n})$ itself.

Theorem 6.1 (Theorem 2 in [Rei05])**.** *Consider the pure cubic field $K = \mathbb{Q}(\sqrt[3]{n})$. Then the class number h_L of the normal closure $L = \overline{K} = \mathbb{Q}(\sqrt[3]{n}, \zeta_3)$ of K is either h_K^2 or $\frac{1}{3}h_K^2$.*

Recall also from class field theory that the Hilbert class field is 'compatible' with field extensions in the following sense. If $E \subset F$ is a field extension, then $H(E) \subset H(F)$, where $H(E)$ is the Hilbert class field of E. So if E is a non-Galois field over $\mathbb{Q}$, with splitting field F, we get that the splitting field of $H(E)$ is contained in $H(F)$. This is because $H(F)$ is a Galois field over $\mathbb{Q}$, containing $H(E)$, and the splitting field of $H(E)$ is the smallest such field.

We can therefore assemble $K, \overline{K}$ and their Hilbert class fields into the following diagram.

$$\begin{tikzcd}
 & & H(\overline{K}) \\
 & S \arrow[ur, dash, "\geq 1"'] & \overline{K} = \mathbb{Q}(\sqrt[3]{n}, \zeta_3) \arrow[u, dash, "h_{\overline{K}} \leq 9"'] \\
H(K) \arrow[ur, dash, "\therefore\ \leq 6"'] & & \\
K = \mathbb{Q}(\sqrt[3]{n}) \arrow[u, dash, "h_k = 3"'] \arrow[uurr, dash, "2"'] & & \\
\mathbb{Q} \arrow[u, dash, "3"'] & &
\end{tikzcd}$$

We know that $h_{\overline{K}} = \frac{1}{3}h_K^2$ or h_K^2, both of which are ≤ 9. Therefore $[H(\overline{K})\colon K] \leq 18$. And $[H(\overline{K})\colon S] \geq 1$, almost by definition. So using the tower law, we establish that

$$[S\colon H(K)] = \frac{[H(\overline{K})\colon K]}{[H(\overline{K})\colon S][H(K)\colon K]} \leq \frac{18}{1 \cdot 3} = 6\,.$$

References

[BM83] Gregory Butler and John McKay. "The transitive groups of degree up to eleven". In: *Communications in Algebra* 11.8 (1983), pp. 863–911.

[Rei05] Nils Reich. "On units and class numbers of pure cubic fields". In: *Mathematika* 52.1-2 (2005), pp. 87–91.