On a Problem of Hasse

By H. Zassenhaus and J. Liang

Abstract. A $p$-adic method to construct explicitly a generating automorphism of the Hilbert classfield over $\mathbb{Q}(\sqrt{-47})$ and to perform Tshirnhausen transformations for generating equations of the real subfield is developed.

I. Let $f(x)$ be a monic polynomial with coefficients in $\mathbb{Z}$, irreducible of degree $n$ over $\mathbb{Q}$, with $\theta$ a real root, let

$$k = \mathbb{Q}(\sqrt{d}), \quad d < 0$$

$$E = \mathbb{Q}(\theta),$$

$$K = E(\sqrt{d})$$

$K$ is normal over $\mathbb{Q}$ and cyclic of degree $n$ over $k$. How to find a generating element of $G(K/k)$, where $G(K/k)$ is the Galois group of $K$ over $k$?

Here we give a $p$-adic method to construct such an automorphism. In the end, we shall give some examples to demonstrate our method.

By a theorem given in [2] there are infinitely many rational prime numbers $p$ which decompose in $k$ into the product of two distinct prime ideals which stay indecomposed in $K$. Those are the ones with decomposition group equal to $G(K/k)$ and not dividing the discriminant of $K$ over $\mathbb{Q}$. Among them there is one which does not even divide the characteristic $b$ of the factor module of $\mathcal{O}_K$ over $\mathcal{O}_F \cdot \mathcal{O}_k$.

(We denote by $\mathcal{O}_F$ the ring of the algebraic integers of the algebraic number field $F$.)

Let $p = p_1p_2$ in $k$, $p_1 \neq p_2$ are prime ideals in $k$ and let $\mathfrak{p}_i = p_i\mathcal{O}_K$, $i = 1, 2$, $\mathfrak{p}_i$ prime ideals in $\mathcal{O}_K$. Since $k$ is imaginary quadratic the two prime ideals $p_1, p_2$ are complex conjugate. The same applies to $\mathfrak{p}_1, \mathfrak{p}_2$.

Then we know there exists an automorphism $\sigma$, namely the Frobenius automorphism in $G$ such that

$$\sigma \xi = \xi^p \mod \mathfrak{p}_1$$

for every $\xi \in \mathcal{O}_K$

and in particular,

$$\sigma \theta = \theta^p \mod \mathfrak{p}_1.$$

Let $\sigma_{1,0}(x) = x^p \mod f(x)$ where $\sigma_{1,0}(x)$ is a polynomial of $\mathbb{Z}[x]$ of degree less than $n$. It follows that $\sigma_{1,0}(\theta) = \theta^p = \sigma \theta \mod \mathfrak{p}_1$.

Since $p$ is unramified in $K$, we have $p$ as $\mathfrak{p}_1$-adic generator of $\mathfrak{p}_1$, i.e. $p \in \mathfrak{p}_1$, but $p \notin \mathfrak{p}_1^2$.

In order to obtain the action of $\sigma$ on $\theta$ modulo powers of $\mathfrak{p}_1$, we proceed as follows: let $\sigma \theta = \sigma_{1,0}(\theta) + p\eta_1(\theta) \mod \mathfrak{p}_1^2$ where $g_1(x)$ is a polynomial of $\mathbb{Z}[x]$ of degree less than $n$.

How to find $g_1$?

We know that

\begin{equation}
(*) \quad f(\sigma_{1,0}(\theta) + p\eta_1(\theta)) = 0 \mod \mathfrak{p}_1^2
\end{equation}

Received November 13, 1968.
and by Taylor-Maclaurin
\[(**)
\begin{equation}
f(\sigma_1,0(\theta) + pg_1(\theta)) \equiv f(\sigma_1,0(\theta)) + pf'(\sigma_1,0(\theta))g_1(\theta) \mod \mathfrak{P}_1^2.
\end{equation}
\]
Since
\[\text{(***)}
\begin{equation}
f(\sigma_1,0(\theta)) \equiv 0 \mod \mathfrak{P}_1
\end{equation}
\]
we can write \(f(\sigma_1,0(x)) \equiv pf_1(x) \mod f\) where \(f_1\) is a polynomial of \(\mathbb{Z}[x]\) of degree less than \(n\).

From (*), (**), (***) we then obtain
\[g_1(\theta) = -f_1(\theta)/f'(\sigma_1,0(\theta)) \mod \mathfrak{P}_1.\]

Continue this process for higher powers of \(\mathfrak{P}_1\) until we reach an exponent \(2^{r+1}\). The number \(v\) is to be determined later and a bound for the number \(v\) was given in [1].

In the same manner, we should compute \(\sigma \theta\) modulo powers of \(\mathfrak{P}_2\). Noting that \(\mathfrak{P}_1\) and \(\mathfrak{P}_2\) are complex conjugates, but that \(\theta\) is real and that \(\sigma \theta \equiv \theta^p \mod \mathfrak{P}_1\), it follows if \(\tau\) is the automorphism of \(K\) over \(\mathbb{Q}\) such that \(\tau : a + ci \rightarrow a - ci\), \(a, c\) real, then applying \(\tau\) to the above congruence, we have
\[(\tau \sigma \tau^{-1}) \theta \equiv \theta^p \mod \mathfrak{P}_2\]
and \((\tau \sigma \tau^{-1}) \theta \equiv \theta^p \mod \mathfrak{P}_1\) and hence \(\tau \sigma \tau^{-1} \neq \sigma\). On the other hand \(G(K/k)\) is normal in \(\text{Aut } (K/\mathbb{Q}) = \langle \tau, G(K/k) \rangle\) and therefore \((\tau \sigma \tau^{-1}) \theta \equiv (\sigma^j) \theta\) where \(1 < j < n\), so
\[\sigma \theta \equiv h^* (\theta) \mod \mathfrak{P}_2\]
where \(h^* (\theta) \equiv (\sigma^j) \theta \mod \mathfrak{P}_1\).

Again, let \(\sigma_{2,0}(x) \equiv h^* (x) \mod f(x)\) we then have
\[\sigma^j \equiv \sigma_{2,0}(\theta) \mod \mathfrak{P}_2.\]
Proceed from here as before to obtain actions of \(\sigma\) modulo powers of \(\mathfrak{P}_2\) until \(\mathfrak{P}_2^{2^{r+1}}\). We then have the following congruence conditions:
\[\sigma \theta \equiv \sigma_{1,0}(\theta) \mod \mathfrak{P}_1,\]
\[\sigma \theta \equiv \sigma_{1,1}(\theta) \mod \mathfrak{P}_1^2,\]
\[\sigma \theta \equiv \sigma_{1,2}(\theta) \mod \mathfrak{P}_1^3,\]
\[\sigma \theta \equiv \sigma_{1,3}(\theta) \mod \mathfrak{P}_1^{2^{r+1}};\]
\[\sigma \theta \equiv \sigma_{2,0}(\theta) \mod \mathfrak{P}_2,\]
\[\equiv \sigma_{2,1}(\theta) \mod \mathfrak{P}_2^2,\]
\[\equiv \sigma_{2,2}(\theta) \mod \mathfrak{P}_2^3,\]
\[\equiv \sigma_{2,3}(\theta) \mod \mathfrak{P}_2^{2^{r+1}}.\]

Before we go any further, we would like to make the following remark:
By applying the Euclidean algorithm, one can easily obtain the inverse \(h_0 = h_0(\theta)\) of \(f'(\sigma_1,0(\theta))\) modulo \(\mathfrak{P}_1\). In order to find \(h_1\) as solution to \(f'(\sigma_1,0(\theta))h_1 \equiv 1 \mod \mathfrak{P}_1^2\), we proceed as follows:
Since \( h_1 = h_0 \mod \mathfrak{P} \), we may write the polynomial equation \( h_1 = h_0 + pQ_2 \), \( Q_2 \in \mathbb{Z}[x] \), so that \( f'(\sigma_1(\theta)) \cdot (h_0 + pQ_2) = 1 \mod \mathfrak{P}_1^2 \), \( Q_2 = Q_2(\theta) \); let \( f'(\sigma_{11}(\theta))h_0 = 1 + pR_2(\theta) \mod \mathfrak{P}_1^2 \), \( R_2 \in \mathbb{Z}[x] \).

We then have

\[
1 = f'(\sigma_{11}(\theta))h_0 + pf'(\sigma_{11}(\theta))Q_2
\]

and so,

\[
-pR_2 = pf'(\sigma_{11}(\theta))Q_2 \mod \mathfrak{P}_1^2
\]

or

\[
-R_2 = f'(\sigma_{11}(\theta))Q_2 \mod \mathfrak{P}_1
\]

or

\[
-R_2h_0 = Q_2 \mod \mathfrak{P}_1
\]

continuing in the same manner, we should obtain \( h_2, \ldots, h_{n+1} \).

Now, we are going to apply the Chinese remainder theorem to obtain our final result.

Choose the element \( e_0 \) of \( \mathfrak{S}_p \) subject to the congruences

\[
e_0 = 1 \mod \mathfrak{P}_1, \quad e_0 = 0 \mod \mathfrak{P}_2
\]

and let \( e_1 = 3e_0^2 - 2e_0^3 \); this implies that

\[
e_1 = 1 \mod \mathfrak{P}_1^2, \quad e_1 = 0 \mod \mathfrak{P}_2^2.
\]

Continuing with the construction we arrive at \( e_{n+1} \) of \( \mathfrak{S}_p \) such that

\[
e_{n+1} = 1 \mod \mathfrak{P}_1^{2n+1}, \quad e_{n+1} = 0 \mod \mathfrak{P}_2^{2n+1}.
\]

For \( j = 0, 1, \ldots, n + 1 \) we proceed as follows: set

\[
\Sigma_j(\theta) = e_j\sigma_j(\theta) + (1 - e_j)\sigma_{2j}(\theta).
\]

We may write \( \Sigma_j(\theta) \) as follows:

\[
\Sigma_j(\theta) = (\alpha_{j0} + \beta_{j0}\omega) + (\alpha_{j1} + \beta_{j1}\omega)\theta + \cdots + (\alpha_{j,n-1} + \beta_{j,n-1}\omega)\theta^{n-1},
\]

where \( \alpha_{ji}, \beta_{ji} \in \mathbb{Z}, 0 \leq i \leq n - 1 \) and \( \mathfrak{S}_p = [1, \omega] \).

In view of the fact that \( \mathfrak{S}_k/\mathfrak{S}_x \cdot \mathfrak{S}_k \) has characteristic \( b \) we write

\[
\Sigma_j(\theta) = \{ (\alpha_{j0} + \beta_{j0}\omega) + (\alpha_{j1} + \beta_{j1}\omega)\theta + \cdots + (\alpha_{jn-1} + \beta_{jn-1}\omega)\theta^{n-1} \}/b
\]

and choose \( \alpha'_{ji} \) and \( \beta'_{ji} \) such that

\[
\alpha'_{ji} \equiv \alpha_{ji}b \mod p^{2j}, \quad \beta'_{ji} \equiv \beta_{ji}b \mod p^{2j}
\]

and

\[
-p^{2j/2} < \alpha'_{ji}, \beta'_{ji} \leq p^{2j/2}, 0 \leq i \leq n - 1.
\]

Finally, we set

\[
\Sigma'_j(\theta) = \{ (\alpha'_{j0} + \beta'_{j0}\omega) + (\alpha'_{j1} + \beta'_{j1}\omega)\theta + \cdots + (\alpha'_{j,n} + \beta'_{j,n}\omega)\theta^{n-1} \}/b.
\]

The number \( \nu \) should be chosen as the least nonnegative integer for which we have
(1a) \[ f(\Sigma'(\theta)) = 0. \]

In order to have this condition satisfied, it is necessary to have

(1b) \[ \Sigma'(x) \equiv \Sigma'_{+1}(x) \text{ mod } p^{2r+1} \]

though this congruence may not be sufficient. Therefore it will become necessary to test (1a) even if (1b) is established already.

From our construction one can see that \( \Sigma'(\theta) \) is the action of the automorphism \( \sigma \) applied to \( \theta \).

II. The following questions were brought up by Professor H. Hasse. Given three equations:

\[ f_H = x^5 + 10x^3 - 235x^2 + 2610x - 9353 = 0 , \quad \theta_H \text{ the real root} ; \]
\[ f_w = x^5 - x^3 - 2x^2 - 2x - 1 = 0 , \quad \theta_w \text{ the real root} ; \]
\[ f_F = x^5 - x^4 + x^3 + x^2 - 2x + 1 = 0 , \quad \theta_F \text{ the real root} ; \]

\[ k = \mathbb{Q}(\sqrt[5]{-47}) , \quad E = \mathbb{Q}(\theta_H) , \quad K = E(\sqrt[5]{-47}) , \quad \omega = (1 + \sqrt[5]{-47})/2 , \]

\( K \) cyclic of degree 5 over \( k \),

\( G(K/k) \) Galois group of \( K \) over \( k \).

Questions:

(1) How to find a generating element \( \sigma \in G(K/k) \)?

(2) Do \( \theta_H, \theta_w, \theta_F \) generate the same field? And if so, how to express them in terms of each other.

Our method given in Section I has been programmed in ALGOL for the IBM 7094 in order to solve the above question (1).

For the polynomials \( f_w \) and \( f_F \), we have \( d = -47, b = 47, p = 2, \) and

\[ p_1, p_2 \text{ stay prime in } K. \]

We obtained \( \sigma \theta_w \) and \( \sigma \theta_F \) at \( \nu = 3 \). They are as follows:

\[ \sigma \theta_w = \{(54 - 14\omega) + (58 - 22\omega)\theta_w \]
\[ + (55 - 16\omega)\theta_w^2 + (30 - 13\omega)\theta_w^3 + (-56 + 18\omega)\theta_w^4\}/47 \]
\[ \sigma \theta_F = \{(68 + 5\omega) + (-72 + 3\omega)\theta_F + (-21 - 5\omega)\theta_F^2 \]
\[ + (22 + 3\omega)\theta_F^3 + (-44 - 6\omega)\theta_F^4\}/47 . \]

The procedure used to solve the second question is even simpler: in order to express \( \theta_H \), say, in terms of \( \theta_w \), we only have to begin with finding a polynomial \( g_0(\theta_w) \) with coefficients in \( \mathbb{Z}/2 \) of degree less than 5 such that

\[ \theta_H \equiv g_0(\theta_w) \text{ mod } 2 . \]

In our cases we have

\[ \theta_H = \theta_w^2 + \theta_w \mod 2 , \]
\[ \theta_w = \theta_F^4 + 1 \mod 2 . \]
Proceed from here by the same method given in Section I until we arrive at a polynomial $g_\mu(x)$ such that $\theta_H = g_\mu(\theta_W) \mod 2^{22}$ and $f_H(g_\mu(\theta_W)) = 0$. Again, a bound for $\mu$ was given in [1].

We obtain the following results from our ALGOL program:

\[
\begin{align*}
\theta_H &= 5\theta_W^2 - 5\theta_W - 2, \\
\theta_W &= -\theta_F^4 - 2\theta_F + 1.
\end{align*}
\]

The Ohio State University
Department of Mathematics
Columbus, Ohio 43210