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 $\mathbf{Q}(\sqrt{-47})$ 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 $\mathbf{Z}$, irreducible of degree n over $\mathbf{Q}$, with θ a real root, let

$$k = \mathbf{Q}(\sqrt{d}) , \qquad d < 0$$
$$E = \mathbf{Q}(\theta) ,$$

$K = E(\sqrt{d})$ and K is normal over $\mathbf{Q}$ 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 $\mathbf{Q}$. Among them there is one which does not even divide the characteristic b of the factor module of $\mathfrak{O}_K$ over $\mathfrak{O}_E \cdot \mathfrak{O}_k$. (We denote by $\mathfrak{O}_F$ the ring of the algebraic integers of the algebraic number field F.)

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

Then we know there exists an automorphism σ, namely the Frobenius automorphism in G such that

$$\sigma\xi \equiv \xi^p \bmod \mathfrak{P}_1 \quad \text{for every } \xi \in \mathfrak{O}_K$$

and in particular,

$$\sigma\theta \equiv \theta^p \bmod \mathfrak{P}_1 .$$

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

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 σ on θ modulo powers of $\mathfrak{P}_1$, we proceed as follows: let $\sigma\theta \equiv \sigma_{1,0}(\theta) + pg_1(\theta) \bmod \mathfrak{P}_1^2$ where $g_1(x)$ is a polynomial of $\mathbf{Z}\,[x]$ of degree less than n.

How to find g_1?

We know that

$$(*) \qquad f(\sigma_{1,0}(\theta) + pg_1(\theta)) \equiv 0 \bmod \mathfrak{P}_1^2$$

Received November 13, 1968.

and by Taylor-Maclaurin

$$(**) \qquad f(\sigma_{1,0}(\theta) + pg_1(\theta)) \equiv f(\sigma_{1,0}(\theta)) + pf'(\sigma_{1,0}(\theta))g_1(\theta) \bmod \mathfrak{P}_1^{\,2}.$$

Since

$$(***) \qquad f(\sigma_{1,0}(\theta)) \equiv 0 \bmod \mathfrak{P}_1$$

we can write $f(\sigma_{1,0}(x)) \equiv pf_1(x) \bmod f$ where f_1 is a polynomial of $\mathbf{Z}[x]$ of degree less than n.

From (*), (**), (***), we then obtain

$$g_1(\theta) = -f_1(\theta)/f'(\sigma_{1,0}(\theta)) \bmod \mathfrak{P}_1 .$$

Continue this process for higher powers of $\mathfrak{P}_1$ until we reach an exponent $2^{\nu+1}$. The number ν is to be determined later and a bound for the number ν 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 θ is real and that $\sigma\theta \equiv \theta^p \bmod \mathfrak{P}_1$, it follows if τ is the automorphism of K over $\mathbf{Q}$ such that $\tau\colon a + ci \rightarrow a - ci$, a, c real, then applying τ to the above congruence, we have

$$(\tau\sigma)\theta \equiv \theta^p \bmod \mathfrak{P}_2$$

and $(\tau\sigma\tau^{-1})\theta \equiv \theta^p \bmod \mathfrak{P}_2$ and hence $\tau\sigma\tau^{-1} \not\equiv \sigma$. On the other hand $G(K/k)$ is normal in Aut $(K/\mathbf{Q}) = \langle \tau, G(K/k) \rangle$ and therefore $(\tau\sigma\tau^{-1})\theta = (\sigma^j)\theta$ where $1 < j < n$, so $\sigma\theta \equiv h^*(\theta) \bmod \mathfrak{P}_2$ where $h^*(\theta) \equiv (\sigma^j)\theta \bmod \mathfrak{P}_1$.

Again, let $\sigma_{2,0}(x) \equiv h^*(x) \bmod f(x)$ we then have

$$\sigma\theta \equiv \sigma_{2,0}(\theta) \bmod \mathfrak{P}_2 .$$

Proceed from here as before to obtain actions of σ modulo powers of $\mathfrak{P}_2$ until $\mathfrak{P}_2^{2^{\nu+1}}$. We then have the following congruence conditions:

$$\begin{aligned}
\sigma\theta &\equiv \sigma_{1,0}(\theta) \bmod \mathfrak{P}_1 ,\\
\sigma\theta &\equiv \sigma_{1,1}(\theta) \bmod \mathfrak{P}_1^{\,2} ,\\
&\ \vdots\\
\sigma\theta &\equiv \sigma_{1,\nu+1}(\theta) \bmod \mathfrak{P}_1^{\,2^{\nu+1}} ;\\
\sigma\theta &\equiv \sigma_{2,0}(\theta) \bmod \mathfrak{P}_2 ,\\
&\equiv \sigma_{2,1}(\theta) \bmod \mathfrak{P}_2^{\,2} ,\\
&\ \vdots\\
&\equiv \sigma_{2,\nu+1}(\theta) \bmod \mathfrak{P}_2^{\,2^{\nu+1}} .
\end{aligned}$$

Before we go any further, we would like to make the following remark:

By applying the Euclidean algorithm, one can easily obtain the inverse $\hat{h}_0 = h_0(\theta)$ of $f'(\sigma_{1,0}(\theta))$ modulo $\mathfrak{P}_1$. In order to find $\hat{h}_1$ as solution to $f'(\sigma_{11}(\theta))\hat{h}_1 \equiv 1 \bmod \mathfrak{P}_1^2$, we proceed as follows:

Since $\hat{h}_1 \equiv \hat{h}_0 \bmod \mathfrak{P}_1$, we may write the polynomial equation $\hat{h}_1 = \hat{h}_0 + pQ_2$, $Q_2 \in \mathbf{Z}[x]$, so that $f'(\sigma_{11}(\theta)) \cdot (\hat{h}_0 + p\hat{Q}_2) \equiv 1 \bmod \mathfrak{P}_1^2$, $\hat{Q}_2 = Q_2(\theta)$; let $f'(\sigma_{11}(\theta))\hat{h}_0 \equiv 1 + pR_2(\theta) \pmod{\mathfrak{P}_1^2}$, $R_2 \in \mathbf{Z}[x]$.

We then have

$$\begin{aligned} 1 &\equiv f'(\sigma_{11}(\theta))\hat{h}_0 + pf(\sigma_{11}(\theta))\hat{Q}_2 \\ &\equiv f'(\sigma_{11}(\theta))\hat{h}_0 + pf(\sigma_{10}(\theta))\hat{Q}_2 \bmod \mathfrak{P}_1^2 \end{aligned}$$

and so,

$$-pR_2 \equiv pf'(\sigma_{10}(\theta))\hat{Q}_2 \bmod \mathfrak{P}_1^2$$

or

$$-R_2 \equiv f'(\sigma_{10}(\theta))\hat{Q}_2 \bmod \mathfrak{P}_1$$

or

$$-R_2\hat{h}_0 \equiv \hat{Q}_2 \bmod \mathfrak{P}_1 ;$$

continuing in the same manner, we should obtain $\hat{h}_2, \cdots, \hat{h}_{\nu+1}$.

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

Choose the element e_0 of $\mathfrak{O}_k$ subject to the congruences

$$e_0 \equiv 1 \bmod \mathfrak{p}_1 , \qquad e_0 \equiv 0 \bmod \mathfrak{p}_2$$

and let $e_1 = 3e_0^2 - 2e_0^3$; this implies that

$$e_1 \equiv 1 \bmod \mathfrak{p}_1^2 , \qquad e_1 \equiv 0 \bmod \mathfrak{p}_2^2 .$$

Continuing with the construction we arrive at $e_{\nu+1}$ of $\mathfrak{O}_k$ such that

$$e_{\nu+1} \equiv 1 \bmod \mathfrak{p}_1^{2^{\nu+1}} , \qquad e_{\nu+1} \equiv 0 \bmod \mathfrak{p}_2^{2^{\nu+1}} .$$

For $j = 0, 1, \cdots, \nu + 1$ we proceed as follows: set

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

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 $\alpha_{ji}, \beta_{ji} \in \mathbf{Z}$, $0 \leqq i \leqq n-1$ and $\mathfrak{O}_k = [1, \omega]$.

In view of the fact that $\mathfrak{O}_K/\mathfrak{O}_E \cdot \mathfrak{O}_k$ has characteristic b we write

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

and choose α'_{ji} and β'_{ji} such that

$$\alpha'_{ji} \equiv \alpha_{ji}b \bmod p^{2^j} , \qquad \beta'_{ji} \equiv \beta_{ji}b \bmod p^{2^j}$$

and $-p^{2^j}/2 < \alpha'_{ji}, \beta'_{ji} \leqq p^{2^j}/2$, $0 \leqq i \leqq n - 1$.

Finally, we set

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

The number ν should be chosen as the least nonnegative integer for which we have

(1a) $$f(\Sigma_\nu'(\theta)) = 0 .$$

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

(1b) $$\Sigma_\nu'(x) \equiv \Sigma_{\nu+1}'(x) \bmod p^{2^\nu+1}$$

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 $\Sigma_\nu'(\theta)$ is the action of the automorphism σ applied to θ.

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

$$f_H = x^5 + 10x^3 - 235x^2 + 2610x - 9353 = 0 , \qquad \theta_H \text{ the real root ;}$$
$$f_W = x^5 - x^3 - 2x^2 - 2x - 1 = 0 , \qquad \theta_W \text{ the real root ;}$$
$$f_F = x^5 - x^4 + x^3 + x^2 - 2x + 1 = 0 , \qquad \theta_F \text{ the real root ;}$$
$$k = \mathbf{Q}(\sqrt{-47}) , \quad E = \mathbf{Q}(\theta_H) , \quad K = E(\sqrt{-47}) , \omega = (1 + \sqrt{-47})/2,$$

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 θ_H, θ_W, θ_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

$$(2) = \mathfrak{p}_1\mathfrak{p}_2 = (2, (1 + \sqrt{-47})/2)\ (2, (-1 + \sqrt{-47})/2) \text{ in } k .$$

$\mathfrak{p}_1$, $\mathfrak{p}_2$ 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 θ_H, say, in terms of θ_W, we only have to begin with finding a polynomial $g_0(\theta_W)$ with coefficients in $\mathbf{Z}/2$ of degree less than 5 such that

$$\theta_H \equiv g_0(\theta_W) \bmod 2 .$$

In our cases we have

$$\theta_H \equiv \theta_W^2 + \theta_W \bmod 2 ,$$
$$\theta_W \equiv \theta_F^4 + 1 \bmod 2 .$$

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

We obtain the following results from our ALGOL program:

$$\theta_H = 5\theta_W^2 - 5\theta_W - 2\,,$$

$$\theta_W = -\theta_F^4 - 2\theta_F + 1\,.$$

The Ohio State University
Department of Mathematics
Columbus, Ohio 43210

1. H. Zassenhaus, "On Hensel factorization," *J. Number Theory*, v. 1, 1969. (To appear.)
2. N. Tschebotareff, "Die Bestimmung der Dichtigkeit einer Menge von Primidealen, welche zu einer gegebenen Substitutionsklasse gehören," *Math. Ann.*, v. 95, 1925, p. 191.
3. H. Hasse, "Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante −47," *Acta Arith.*, v. 9, 1964, pp. 419–434. MR **30** #3082.