Publ. Math. Debrecen
79/3-4 (2011), 611–621
DOI: 10.5486/PMD.2011.5136

On computing non-Galois cubic global function fields of prescribed discriminant in characteristic > 3

By MICHAEL E. POHST (Berlin)

Dedicated to Professors Kálmán Győry and Attila Pethő

Abstract. We describe how to compute non Galois global cubic function fields of given discriminant. Our method involves ideas from class field theory which help to transfer the task to computations in quadratic extensions. This also leads to an easy method for calculating the number of such fields. Thus we can avoid more complicated computations in case no such fields exist.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with $q = p^\ell$ elements, p a prime bigger than 3 We denote by F the rational function field $\mathbb{F}_q(t)$ and by o_F its maximal order $\mathbb{F}_q[t]$. For given non-zero $\Delta \in o_F$ we want to determine all cubic extensions E of F of discriminant Δ. We note that the extension E/F is Galois – and in that case cyclic – precisely if Δ is a square in o_F. Since this case is straightforward it is treated separately in a different context [3]. Here, we restrict ourselves to non-Galois extensions E/F.

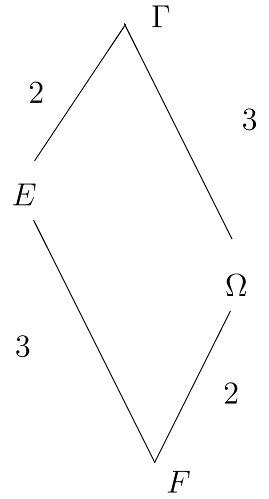
We denote the maximal order of E by o_E and by ω_1, ω_2, ω_3 an integral basis of E. Because of $p > 3$ the extension E/F is separable and the trace bilinear form on E non-degenerate. Then the discriminant of E/F is defined as the determinant Δ of the matrix with entries $Tr(\omega_i\omega_j)$ modulo the square of a unit of o_F, i.e. as

Mathematics Subject Classification: Primary: 11Y50; Secondary: 11D25,11D61.
Key words and phrases: cubic global function fields.

$\Delta(\mathbb{F}_q^\times)^2$. In our case Δ is not a square and we can split it in the form

$$\Delta = df^2 \tag{1}$$

with a square-free element d representing the discriminant of a quadratic extension $\Omega = F(\sqrt{d})$ of F. We note that d, f must be coprime. This will be a consequence of the results of the next section. Let Γ denote the splitting field of E/F. It is a Galois sixth degree extension of F. The corresponding Galois group is isomorphic to the symmetric group $\mathcal{S}_3$. The following diagram illustrates this situation.



Following the precedent of Hasse [4] in the number field case we shall analyze the relations between the arithmetic invariants of the fields E, Ω, Γ by means of class field theory. We note that the function field case is somewhat simpler since our premises guarantee that there is no wild ramification.

2. Prime ideal decomposition and discriminants

According to our assumptions the field Γ is Galois over F, hence it is also Galois over Ω, i.e. Γ is a cyclic extension of Ω. The conductor of that relative extension is an ideal $\mathbf{f}$ in Ω and we shall see in this section that $\mathbf{f} = fo_\Omega$.

Given a prime element $\pi \in o_F$ we deduce its decomposition into prime ideals in E, Ω, Γ from the corresponding Hilbert series. We only need to study the decomposition group G_D and the inertia group G_0. Since we do not have wild ramification the higher ramification groups G_i are trivial for $i \geq 1$. As non-trivial subgroups of the Galois group $\mathcal{S}_3$ we have the alternating group $\mathcal{A}_3$ and three subgroups of order 2, say $\mathcal{T}_1$, $\mathcal{T}_2$, $\mathcal{T}_3$. We assume that $\mathcal{T} = \mathcal{T}_1$ fixes the field E. There are two cases according to (i) $G_0 = \mathcal{E} := \{\mathrm{id}\}$ and (ii) $G_0 \supset G_1 = \mathcal{E}$. We use the notation

- $\mathbf{p}$ for prime ideals of Ω containing π with ramification index $e(\mathbf{p})$ and degree of inertia $f(\mathbf{p})$;
- $\mathbf{P}$ for prime ideals of E containing π with ramification index $e(\mathbf{P})$ and degree of inertia $f(\mathbf{P})$;
- $\bar{\mathbf{P}}$ for prime ideals of Γ containing π with (absolute) ramification index $e(\bar{\mathbf{P}})$ and degree of inertia $f(\bar{\mathbf{P}})$. We note that πo_Γ decomposes into $g_\Gamma = (\mathcal{S}_3 : G_D)$ prime ideals $\bar{\mathbf{P}}$, each of degree of inertia $f(\bar{\mathbf{P}}) = (G_D : G_0)$ and of ramification index $e(\bar{\mathbf{P}}) = (G_0 : \mathcal{E})$.

We list the possible decompositions in a table followed by all necessary explanations.

Hilbert series				decomposition of π in			contribution of π to			
G	G_D	G_0	G_1	Γ	Ω	E	$\mathbf{f}$	$N(\mathbf{f})$	d	Δ
$\mathcal{S}$	$\mathcal{E}$	$\mathcal{E}$	$\mathcal{E}$	$\bar{\mathbf{P}}_1 \dots \bar{\mathbf{P}}_6$	$\mathbf{p}_1\mathbf{p}_2$	$\mathbf{P}_1\mathbf{P}_2\mathbf{P}_3$	–	–	–	–
$\mathcal{S}$	$\mathcal{A}$	$\mathcal{E}$	$\mathcal{E}$	$\bar{\mathbf{P}}_1\bar{\mathbf{P}}_2$	$\mathbf{p}_1\mathbf{p}_2$	$\mathbf{P}$	–	–	–	–
$\mathcal{S}$	$\mathcal{T}$	$\mathcal{E}$	$\mathcal{E}$	$\bar{\mathbf{P}}_1\bar{\mathbf{P}}_2\bar{\mathbf{P}}_3$	$\mathbf{p}$	$\mathbf{P}_1\mathbf{P}_2$	–	–	–	–
$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{E}$	$(\bar{\mathbf{P}}_1\bar{\mathbf{P}}_2)^3$	$\mathbf{p}_1\mathbf{p}_2$	$\mathbf{P}^3$	$\mathbf{p}_1\mathbf{p}_2$	π^2	1	π^2
$\mathcal{S}$	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{E}$	$\bar{\mathbf{P}}^3$	$\mathbf{p}$	$\mathbf{P}^3$	$\mathbf{p}$	π^2	1	π^2
$\mathcal{S}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{E}$	$(\bar{\mathbf{P}}_1\bar{\mathbf{P}}_2\bar{\mathbf{P}}_3)^2$	$\mathbf{p}^2$	$\mathbf{P}_1\mathbf{P}_2^2$	1	1	π	π

The entries in the first 3 lines concern non discriminant divisors (case (i)) those in the last 3 lines regular discriminant divisors (case (ii)). The first column contains the pertinent Hilbert series. There are the following possibilities:

1. $G_D = \mathcal{E}$ is tantamount with $g_\Gamma = 6$ and corresponds to line 1.
2. $G_D = \mathcal{S}_3$ is tantamount with $g_\Gamma = 1$. Since G_0 is a normal subgroup of G_D with cyclic factor group and G_0/G_1 is also cyclic we must have $G_0 = \mathcal{A}_3$. This yields $f(\bar{\mathbf{P}}) = (G_D : G_0) = 2$ and consequently $e(\bar{\mathbf{P}}) = 3$ (see line 5).

3. $G_D = \mathcal{A}_3$ is tantamount with $g_\Gamma = 2$. We get $\mathcal{E}$ and $\mathcal{A}_3$ as candidates for G_0. In the first subcase we have $e(\bar{\mathbf{P}}) = 1$, hence $f(\bar{\mathbf{P}}) = 3$, corresponding to line 2. In the second case we have $e(\bar{\mathbf{P}}) = 3$, hence $f(\bar{\mathbf{P}}) = 1$, corresponding to line 4.
4. $G_D = \mathcal{T}$ is tantamount with $g_\Gamma = 3$. Candidates for G_0 are $\mathcal{E}$ and $\mathcal{T}$. In the first subcase we have $e(\bar{\mathbf{P}}) = 1$, hence $f(\bar{\mathbf{P}}) = 2$, corresponding to line 3. In the second subcase we have $e(\bar{\mathbf{P}}) = 2$ and $f(\bar{\mathbf{P}}) = 1$ (see line 6).

Next we discuss the ideal decompositions of π in E. Those in Ω are an immediate consequence.

Case (i) (lines 1 to 3)
The prime π is non-ramified and decomposes into g_Γ prime ideals in Γ. $g_\Gamma = 1$ cannot occur since $f(\bar{\mathbf{P}}) = 6$ yields G_D/G_0 cyclic of degree 6. We must therefore have $g_\Gamma \in \{6, 2, 3\}$ (corresponding to lines one to three of the table). $g_\Gamma = 6$ necessarily yields $g_E = 3$ with $f(\mathbf{P}_i) = 1$ for each prime ideal $\mathbf{P}_i$ of E dividing π $(1 \le i \le 3)$. Also, we conclude that for $g_\Gamma = 2$ we must have $g_E = 1$, $f(\mathbf{P}) = 3$. (Namely, for $g_E = 2$ one of the prime ideals $\mathbf{P}_1$, $\mathbf{P}_2$ of E dividing π would have $f(\mathbf{P}_i) = 2$ contradicting $f(\bar{\mathbf{P}}_i) = 3$.) Eventually, for $g_\Gamma = 3$ we could in principal have $g_E \in \{1, 2, 3\}$. $g_E = 1$ cannot occur since $f(\mathbf{P}) = 3$ is in contradiction with $f(\bar{\mathbf{P}}_i) = 2$. $g_E = 2$ yields $\pi o_E = \mathbf{P}_1\mathbf{P}_2$ with degrees $f(\mathbf{P}_i) = i$ $(i = 1, 2)$. The exclusion of $g_E = 3$ is more difficult. (We remark that the reasoning of Hasse in this case is not accurate.) A generating element σ of $\mathcal{T} = \langle\sigma\rangle$ must permute two of the prime ideals $\bar{\mathbf{P}}_i$ lying above π, say $\sigma(\bar{\mathbf{P}}_2) = \bar{\mathbf{P}}_3$ and vice versa. Since σ leaves E invariant the intersections $\bar{\mathbf{P}}_j \cap E$ necessarily coincide for $j = 2, 3$.

Case (ii) (lines 4 to 6)
The prime π is ramified in Γ and decomposes into $g_\Gamma \in \{1, 2, 3\}$ prime ideals. For $g_\Gamma = 2$, hence $e(\bar{\mathbf{P}}_i) = 3$, we get $g_E = 1$ and $e(\mathbf{P}) = 3$. (In case $g_E = 2$ one ramification index would be 2 contradicting $e(\bar{\mathbf{P}}_i) = 3$.) In case $g_\Gamma = 1$ we cannot have $e(\bar{\mathbf{P}}) = 6$; namely, this would imply $(G_0 : G_1) = 6$, hence a cyclic Galois group for Γ/F. Therefore we must have $e(\bar{\mathbf{P}}) = e(\mathbf{P}) = 3$. It remains the possibility $g_\Gamma = 3$ with $e(\bar{\mathbf{P}}_i) = 2$. Then we obtain $g_E = 2$ prime ideals above π in E, one with ramification index 1 the other one with 2. ($g_E = 1$ is clearly impossible. For $g_E = 3$ we had no ramification of π in E, but necessarily in Ω. Since the discriminant of Ω divides the discriminant of E this case is also impossible.)

Next we consider the contributions of primes π to the various occuring discriminants. From class field theory we recall that Γ is the class field for an ideal group H of index 3 in the ray class group of Ω of conductor $\mathbf{f}$. The discriminant Δ

of E is the product of the discriminant d of Ω and f^2 (see (1)). The discriminant $\bar{D}$ of Γ satisfies

$$\bar{D} = d^3 N(\mathbf{f})^2 \tag{2}$$

since $\mathbf{f}^2$ is the relative discriminant of Γ/Ω. The contribution of a ramified prime π to $\bar{D}$ is

$$\nu_\pi(\bar{D}) = g_\Gamma f(\bar{\mathbf{P}})(e(\bar{\mathbf{P}}) - 1) \in \{4, 4, 3\}$$

corresponding to lines 4, 5, 6. Analogously, the contribution of π to $\mathbf{f}$ is found. We remark that $\mathbf{f}$ is the product of those prime ideals of Ω which are contained in ramified prime ideals of Γ. Finally, from (2) we get the contribution of π to Δ.

3. Characterisation by invariants, arithmetic properties

According to Hasse we call the discriminant d of Ω and the ideal group H of index 3 in the ray class group Cl_f of conductor $\mathbf{f}$ the *invariants* of the cubic field E.

The following two lemmata are easily transfered from Hasse's paper [4] to the function field case. For this we denote the non-trivial automorphism of Ω (which maps $\sqrt{d}$ onto $-\sqrt{d}$) by τ.

Lemma 3.1. *For d, H, $\mathbf{f}$, Ω, τ as above the following statements are equivalent:*

1. *d, H are the invariants of a cubic field E.*
2. *$\tau(H) = H$ and for $H \neq \tilde{H} \in Cl_f/H$ we have $\tau(\tilde{H}) = \tilde{H}^{-1}$.*
3. *H contains all elements of F which are coprime to $\mathbf{f}$.*

Lemma 3.2. *The discriminants Δ, d and the conductor $\mathbf{f}$ satisfy*

$$\Delta = dN_{\Omega/F}(\mathbf{f}) = df^2 \quad \textit{and } \mathbf{f} = f o_\Omega.$$

In the number field case the prime numbers dividing f must additionally satisfy certain congruence conditions (see [4]). Most of them are meaningless for the function fields under consideration. However, for prime elements π of o_F dividing the conductor f the multiplicative group $G_\pi = (o_\Omega/\pi o_\Omega)^\times$ contains the subgroup $U_\pi := \langle r(t) + \pi o_\Omega \mid 0 \neq r(t) \in \mathbb{F}_q[t],\ \deg(r) < \deg(\pi)\rangle$. Let H be the invariant subgroup of index 3 in the ray class group Cl_f of Ω. Then we obtain an injective homomorphism

$$\varphi : Cl_f/H = \langle AH\rangle \to G_\pi/U_\pi : \left\{ \begin{array}{rcr} H & \mapsto & U \\ AH & \mapsto & \sqrt{d}U \\ (AH)^{-1} & \mapsto & -\sqrt{d}U \end{array} \right\}.$$

It shows that the order of G_π/U_π is divisible by 3. If π is decomposed in Ω the order of G_π equals $(q^{\deg(\pi)}-1)^2$ that of U_π equals $q^{\deg(\pi)}-1$. If π is inert, however, we get $(G_\pi : 1) = q^{2\deg(\pi)}-1$ and $(G_\pi : U_\pi) = q^{\deg(\pi)}+1$. The next lemma is immediate.

Lemma 3.3. *For* $q \equiv 1 \bmod 3$ *the conductor* f *is a product of distinct primes of* o_F *all of which are decomposed in* Ω.
For $q \equiv 2 \bmod 3$ *a prime* π *of* o_F *can divide* f *if and only if in* Ω *either* π *is decomposed with* $\deg(\pi)$ *even or* π *is inert with* $\deg(\pi)$ *odd.*

4. Number of cubic fields

As already observed by Hasse [4] it is much easier to determine the number $N(\Delta)$ of cubic fields E with prescribed discriminant $\Delta = d\,f^2$, where d is the discriminant of a quadratic field Ω and f the conductor of the cubic extension Γ/Ω (see Section 1). We recall that d is square-free and f a product of distinct primes of F not dividing d and satisfying the conditions of the last lemma. The invariants of E are d and a subgroup H of the ray class group Cl_f of Ω of conductor f. Let I_f denote the group of all fractional ideals of Ω which are coprime to f. Since H is of index 3 in Cl_f the third power of every ideal $\mathbf{a} \in I_f$ belongs to H. We must determine the number of candidates for H, i.e. of those subgroups of index 3 in Cl_f which have the exact conductor f.

Remark 4.1. There are two special cases with $N(\Delta) = 0$:

(i) $f \neq 1$ contains a prime divisor π which does not meet the conditions of the previous lemma.

(ii) f equals 1 and the class number of Ω is not divisible by 3.

In general, we know that H is a union of residue classes of Cl_f/J_f for

$$J_f := \{\mathbf{b} \in I_f \mid \mathbf{b} = \mathbf{a}^3 r\gamma,\ \mathbf{a} \in I_f,\ r \in F \text{ coprime to } f,\ \gamma \equiv 1 \bmod f o_\Omega\}. \quad (3)$$

(See also the definition of Z_f below.) In order to obtain a suitable basis of Cl_f/J_f we start to discuss potential generators of principal ideals.

The elements of Ω which are coprime to f form a multiplicative group, say G_f. It contains the subgroup

$$Z_f := \{\alpha^3 r\gamma \mid \alpha,\ \gamma \in G_f,\ r \in F \text{ coprime to } f,\ \gamma \equiv 1 \bmod f o_\Omega\}. \quad (4)$$

(We remark that the occuring congruences are multiplicative.) Following Hasse we determine a basis of the factor group G_f/Z_f. Let $f = \pi_1 \dots \pi_w$. For each prime element π dividing f we fix a prime ideal $\mathbf{p}$ containing π. We compute $\delta \in o_\Omega$ subject to $(o_\Omega/\mathbf{p})^\times = \langle \delta \mathbf{p} \rangle$ By the Chinese Remainder Theorem we calculate an element $\rho \in o_\Omega$ satisfying

$$\rho \equiv \delta \bmod \mathbf{p} \quad \text{and} \quad \rho \equiv 1 \bmod f o_\Omega/\mathbf{p}. \tag{5}$$

We obtain elements $\rho_1, \dots, \rho_w$ which form the desired basis $\mathcal{B}$, i.e. for given $\beta \in G_f$ there exist unique exponents $y_i \in \{0, 1, 2\}$ such that

$$\tilde{\beta} := \prod_{i=1}^{w} \rho_i^{y_i} \tag{6}$$

satisfies $\beta \tilde{\beta}^{-1} \in Z_f$. It is important that the pertinent exponents are easy to compute.

For this we consider the canonical epimorphism

$$\varphi_f : G_f \to (o_\Omega / f o_\Omega)^\times =: o_f^\times .$$

The following lemma is immediate.

Lemma 4.1. *For $\beta \in G_f$ there exist modulo 3 unique exponents $y_1, \dots, y_w$ such that*

$$x := \varphi_f \left(\beta^{-1} \prod_{j=1}^{w} \rho_j^{y_j} \right) \in \varphi_f(Z_f).$$

We therefore need to test for a potential exponent tuple $(y_1, \dots, y_w)$ whether $x \in o_F^\times$ is of the form $\alpha^3 r$ for some $r \in o_F$. This can be done for each prime π dividing f separately using the Chinese Remainder Theorem. Further speed-ups can be obtained from the observation that $r\alpha^3$ equals $(-r)(-\alpha)^3$ thus reducing the number of candidates for r.

Now we are in a situation in which we can easily establish a suitable basis for Cl_f/J_f (compare (3)). We represent the class group Cl in canonical form as a product of cyclic subgroups. For this let I denote the group of fractional ideals of Ω and I_p the subgroup of principal ideals. Then we write $Cl = I/I_p = \prod_{i=1}^{s} U_i$ with cyclic subgroups $U_i = \langle \mathbf{b}_i I_p \rangle$ of order $\# U_i = n_i$ with $n_1 \mid n_2 \mid \dots \mid n_s$. We assume that exactly the last e subgroups U_i have orders n_i which are divisible by 3. Then we choose ideals $\mathbf{a}_1, \dots, \mathbf{a}_e \in I_f$ satisfying

$$\langle \mathbf{a}_i I_p \rangle = \langle \mathbf{b}_{s-e+i} I_p \rangle \quad (1 \le i \le e). \tag{7}$$

Each ideal $\mathbf{b} \in I_f$ can now be written as

$$\mathbf{b} \equiv \prod_{i=1}^{e} \mathbf{a}_i^{x_i} \prod_{j=1}^{w} \rho_j^{y_j} \bmod J_f \tag{8}$$

with modulo 3 uniquely determined exponents x_i, y_j. The exponents y_j, however, must satisfy additional conditions. Those may come from two sources. For each ideal $\mathbf{a}_k$ there exists an exponent m_k such that $\mathbf{a}_k^{m_k}$ is a principal ideal, say $\alpha_k o_\Omega$. We therefore obtain e additional conditions via (compare (6))

$$\alpha_k \equiv \prod_{i=1}^{w} \rho_i^{y_{ki}} \bmod Z_f \quad (1 \le k \le e). \tag{9}$$

Also, additional conditions can come from units in $o_\Omega \setminus o_F$. We note that there is at most one additional generator for the full unit group U of Ω, e.g. a fundamental unit ε of Ω. In that case we obtain

$$\varepsilon \equiv \prod_{i=1}^{w} \rho_i^{y_{e+1,i}} \bmod Z_f. \tag{10}$$

In both cases we end up with $\tilde{e} \ge 0$ side conditions ($\tilde{e} \in \{e, e+1\}$).

As generators for Cl_f/J_f we choose the ideals $\mathbf{a}_1, \dots, \mathbf{a}_e$ and the elements $\rho_1, \dots, \rho_w$. They are not independent in case $\tilde{e} > 0$. Every subgroup H we are looking for is defined by a congruence for a linear form

$$L(\mathbf{x}, \mathbf{y}) := \sum_{i=1}^{e} x_i X_i + \sum_{j=1}^{w} y_j Y_j \equiv 0 \bmod 3 \tag{11}$$

i.e. H consists of all ideals coprime to f whose presentations (8) satisfy that congruence. In order that H has conductor f the coefficients Y_j must not vanish. Clearly, the set of different subgroups H is in 1-1-correspondence to modulo 3 non-proportional linear forms in (11) which satisfy the side conditions (13) (see below). We can therefore choose the coefficients according to

$$Y_1 = 1,\ Y_j \in \{1, 2\}\ (j = 2, \dots, w), \quad X_j \in \{0, 1, 2\}\ (j = 1, \dots, e) \tag{12}$$

subject to

$$L(\mathbf{0}, y_{k1}, \dots, y_{kw}) \equiv 0 \bmod 3 \quad (1 \le k \le \tilde{e}). \tag{13}$$

In practise, we generate all linear forms L of (11), (12) whose coefficients satisfy (13). Their number equals $N(\Delta)$.

Remark 4.2. There are two easy cases:

(i) For $f = 1$ there are no additional conditions (13) and we get $N(\Delta) = (3^e - 1)/2$.

(ii) For $\tilde{e} = 0$ there are no additional conditions and we obtain $N(\Delta) = 2^{w-1}$.

We transfer these ideas into an algorithm for computing $N(\Delta)$.

Algorithm 4.1 (Number of non-isomorphic cubic fields of discriminant Δ).
Input A function field $F = \mathbb{F}_q(t)$ and a non-square discriminant $\Delta = df^2 \in o_F$, d quare-free.
Output The number $N := N(\Delta)$ of non-isomorphic cubic extensions E of F of discriminant Δ.
Step 1 For $\gcd(d, f) \neq 1$ or $d = 1$ return $N = 0$.
Else calculate all prime divisors $\pi \in \{\pi_1, \ldots, \pi_w\}$ of f in F. Then compute the quadratic extension $\Omega = F(\sqrt{d})$. If one prime divisor π of f does not satisfy the conditions of Lemma 3.3 return $N = 0$.
Step 2 In Ω compute the class number h, the class group Cl, and ideals $\mathbf{a}_1, \ldots, \mathbf{a}_e$ which are coprime to f and satisfy (7). Also, calculate the unit group U of Ω.
Step 3 (Easy cases) For $f = 1$ return $N = (3^e - 1)/2$.
For $f > 1, e = 0, U = \mathbb{F}_q$ return $N = 2^{w-1}$.
Step 4 ($f > 1$) Compute the elements $\rho_i \in o_\Omega$ according to (5) for $i = 1, \ldots, w$. Compute $\tilde{e}$ and the exponents y_{kj} of conditions (9) and (10) ($1 \leq k \leq \tilde{e}$, $1 \leq j \leq w$).
Step 5 Set $N = 0$. For each potential linear form $L(\mathbf{x}, \mathbf{y})$ of (11), (12) check whether conditions (13) are violated. Each time they are satisfied increase N by 1. Output N.

Remark 4.3. The performance of the last algorithm can be speeded up by several observations. Usually, the computation of the class number of Ω will be faster than that of the class group. The latter will not be needed if the class number is not divisible by 3. The unit group is listed in Step 2 for a better presentation of the algorithm. Actually, it is only needed later.

5. Examples

In the last section we illustrate our methods by two examples.

5.1. Example 1. We want to determine all cubic extensions of $F = \mathbb{F}_7(t)$ of discriminant $\Delta = t^2(1-t)$. We immediately get $d = 1 - t$, $f = t$, and $\Omega = F(\sqrt{1-t})$. We calculate $o_\Omega = o_F + \sqrt{1-t}o_F$. The class number of Ω is 1. The prime element f of o_F decomposes: $t = (1+\sqrt{1-t}\,)(1-\sqrt{1-t}\,) =: \alpha\tau(\alpha)$. Since the unit group of o_Ω coincides with $\mathbb{F}_7^\times$ we have $N(\Delta) = 1$ according to Remark 4.2. From the theory we know that Γ is a cyclic cubic Kummer extension of Ω of relative discriminant f^2. By the Dedekind criterion (see [3]) we conclude that

$$\Gamma = \Omega(\sqrt[3]{\alpha^2\tau(\alpha)}\,) = \Omega(\sqrt[3]{f\alpha}\,).$$

Let $\rho \in \Gamma$ with $\rho^3 = f\alpha$. The element $\lambda := \rho + \tau(\rho)$ is invariant under τ and must therefore generate E. The minimal polynomial $m_\lambda(T)$ of λ is easily calculated from the conjugates of λ. If ζ denotes a third root of unity in $\mathbb{F}_7$ those conjugates are: $\rho+\tau(\rho)$, $\zeta\rho+\zeta^2\tau(\rho)$, $\zeta^2\rho+\zeta\tau(\rho)$. We obtain

$$m_\lambda(T) = T^3 - 3\rho\tau(\rho)T + f(\alpha+\tau(\alpha)) = T^3 - 3fT + 2f$$

of discriminant $-108t^2(1-t)$. (We note that -3 is a square in $\mathbb{F}_7$.)

5.2. Example 2. We want to determine all cubic extensions of $F = \mathbb{F}_{11}(t)$ of discriminant $\Delta = 6t^4 + 4t$. We immediately get $d = \Delta$, $f = 1$, and $\Omega = F(\sqrt{\Delta}\,)$. We calculate $o_\Omega = o_F + \sqrt{\Delta}o_F$. The class number of Ω is 12, the class group is cyclic. According to Remark 4.2 there exists exactly one cubic extension E.

The class field theoretical computations yield the following polynomial a root of which generates E:

$$\begin{aligned} y^3 \quad & +(8t^{11}+9t^8+5t^5+7t^2)\,y^2 \\ & +(3t^{22}+6t^{16}+2t^{13}+6t^{10}+3t^7+4t^4)\,y \\ & +10t^{33}+3t^{30}+2t^{27}+7t^{24}+7t^{21}+9t^{18}+5t^{15}+5t^{12}+8t^9 \ . \end{aligned}$$

Fot these calculations we used KANT [2] and Magma [1] in an interactive way.

References

[1] W. Bosma and J. Cannon, Discovering mathematics with Magma. Reducing the abstract to the concrete, Algorithms and Computation in Mathematics, Vol. 19, *Berlin, Springer*, 2006.

[2] M. Daberkow, C.Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, KANT V4, *J. Symbolic Comput.* **24** (1997), 267–283, `http://www.math.tu-berlin.de/~kant/`.

[3] C. Fieker, I. Gaál and M. Pohst, On computing integral points of a Mordell curve over rational function fields in characteristic > 3 (*to appear*).

[4] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Z.* **31** (1930), 565–582.

[5] L. J. Mordell, Diophantine equations, Pure and Applied Mathematics, Vol. 30, *Academic Press, London – New York*, 1969.

[6] M.Pohst and H.Zassenhaus, Algorithmic algebraic number theory, Encyclopedia of Mathematics and its Applications, Vol. 30, *Cambridge University Press*, 1989.

MICHAEL E. POHST
TECHNISCHE UNIVERSTÄT BERLIN
INSTITUT FÜR MATHEMATIK
STRASSE DES 17. JUNI 136
10623 BERLIN
GERMANY

E-mail: pohst@math.tu-berlin.de

(Received February 8, 2011; revised April 8, 2011)