



**HAL**  
open science

# Class number in totally imaginary extensions of totally real function fields

Yves Aubry

► **To cite this version:**

Yves Aubry. Class number in totally imaginary extensions of totally real function fields. Lecture Notes Series London Mathematical Society, 1996, Proceedings of the Third International Conference on Finite fields and Applications, pp.23–29. hal-00977316

**HAL Id: hal-00977316**

**<https://hal.science/hal-00977316>**

Submitted on 11 Apr 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Class number in totally imaginary extensions of totally real function fields

Yves Aubry

**Abstract.** *We show that, up to isomorphism, there are only finitely many totally real function fields which have any totally imaginary extension of a given ideal class number.*

## Introduction.

The case of imaginary quadratic extensions of  $\mathbb{F}_q(X)$  with ideal class number one is quite known : we know that there are only four (see [M]). The real quadratic case is completely different since there are infinitely many such fields (see [S]). The regulator in the last case is a hard parameter to deal with. The situation that we are interested in, is totally imaginary extensions of totally real extensions of the rational function field  $\mathbb{F}_q(X)$ . In our situation, the problem of each regulator subsists but we can easily compute the quotient of them : we show that it is essentially the index of units of their rings of integers. After that, we prove the divisibility in the general case of the divisor class numbers in a finite separable extension of function fields. This result, with the Riemann Hypothesis allow us to show the finiteness of the number of such function fields if we fix the ideal class number of the imaginary field.

## 1. Notation.

Let  $q$  be a power of a prime and  $\mathbb{F}_q$  be the finite field with  $q$  elements. Let  $K$  be an algebraic function field of one variable with finite constant field  $\mathbb{F}_q$ . First we give some notation and some well-known results (see for example [R]). Let  $S_\infty(K) = \{P_1, \dots, P_{s_\infty}\}$  be a non empty finite set of places of  $K$  and let  $A$  be the ring of elements of  $K$  whose poles are in  $S_\infty(K)$  (the ring  $A$  is a Dedekind domain). We denote by  $\text{Cl}(A)$  the ideal

class group of  $A$  and by  $h_A$  its order. The number  $h_A$  is finite and is called the ideal class number of  $A$ .

The analogue of Dirichlet theorem states that the unit group  $A^*$  of  $A$  (modulo the constants) is finitely generated of rank  $s_\infty - 1$  where  $s_\infty = \#S_\infty(K)$  :

$$A^*/\mathbb{F}_q^* \simeq \mathbb{Z}^{s_\infty - 1}$$

We consider the following groups  $\mathcal{D}$  = divisors of  $K$ ,  $\mathcal{D}^0$  = divisors of degree zero of  $K$ ,  $\mathcal{P}$  = principal divisors of  $K$ ,  $C = \mathcal{D}/\mathcal{P}$  = the group of divisors classes,  $J = \mathcal{D}^0/\mathcal{P}$  = the divisors classes of degree zero and  $\delta_K$  = greatest common divisor of  $\{\deg P_1, \dots, \deg P_{s_\infty}\}$ .

Recall that we have an isomorphism of  $C/N$  with  $\text{Cl}(A)$  where  $N$  is the subgroup of  $C$  generated by the classes of places in  $S_\infty(K)$ . We remark also that  $J$  is isomorphic to the group of rational points over  $\mathbb{F}_q$  of the Jacobian of the non singular projective curve which has  $K$  as its function field. Thus, the order  $h_K$  of  $J$ , called the divisor class number, is also the numerator of the zeta function of  $K$  evaluated on 1.

Let  $\mathcal{D}_\infty$  be the divisors supported on  $S_\infty(K)$ ,  $\mathcal{D}_\infty^0 = \mathcal{D}_\infty \cap \mathcal{D}^0$ ,  $\mathcal{P}_\infty$  the principal divisors supported on  $S_\infty(K)$  and  $r_A = [\mathcal{D}_\infty^0 : \mathcal{P}_\infty]$ . We have exact sequences

$$0 \longrightarrow \mathbb{F}_q^* \longrightarrow A^* \longrightarrow \mathcal{P}_\infty \longrightarrow 0$$

and

$$0 \longrightarrow \mathcal{D}_\infty^0/\mathcal{P}_\infty \longrightarrow J \longrightarrow \text{Cl}(A) \longrightarrow \mathbb{Z}/\delta_K\mathbb{Z} \longrightarrow 0$$

which give the isomorphism  $\mathcal{P}_\infty \simeq A^*/\mathbb{F}_q^*$  and the relation

$$\delta_K h_K = r_A h_A \tag{1}$$

If  $P$  is a place of  $K$ , we denote by  $v_P$  the valuation associated to  $P$ . Consider the  $s_\infty \times (s_\infty - 1)$  matrix whose  $ij$ 'th entry is  $-\deg P_i v_{P_i}(\varepsilon_j)$  where  $\{\varepsilon_1, \dots, \varepsilon_{d-1}\}$  is a fundamental set of units for  $A^*$ . The regulator  $R_A$  of  $A$  is defined to be the absolute value of the determinant of any  $(s_\infty - 1) \times (s_\infty - 1)$  minor of this matrix. We can easily show that (see [R] and note that "our" regulator is the "q-regulator" of Rosen) :

$$r_A = \frac{\delta_K R_A}{\prod_{i=1}^{s_\infty} \deg P_i} \tag{2}$$

## 2. Finiteness theorem.

Let  $k = \mathbb{F}_q(X)$  and let  $\infty$  be the place at infinity of  $k$ . From now on, all the extensions considered will be contained in a separable closure of  $k$  and will have full constant field  $\mathbb{F}_q$ .

Consider a totally imaginary extension  $L$  of degree  $n$  of a totally real extension  $K$  of degree  $d$  of  $k$ . This means that the place  $\infty$  of  $k$  splits completely in  $K$  and that the infinite places of  $K$  have only one place above each of them in  $L$ . Let  $A$  be the integral closure of  $\mathbb{F}_q[X]$  in  $K$  and  $B$  be the integral closure of  $A$  in  $L$ . Let  $S_\infty(L) = \{\mathfrak{P}_1, \dots, \mathfrak{P}_d\}$  be the places of  $L$  above those of  $S_\infty(K) = \{P_1, \dots, P_d\}$ . Note that the places  $P_i$  are necessarily of degree 1, and that the ring  $A$  is the same that the one defined in 1.

$$\begin{array}{ccccccc}
 & & L & & \mathfrak{P}_1 & \dots & \mathfrak{P}_d \\
 & & | & & & & \\
 B & & & n & & & \\
 & & K & & P_1 & \dots & P_d \\
 & & | & & & & \\
 A & & & d & & & \\
 & & k & & & \infty & \\
 \mathbb{F}_q[X] & & & & & & 
 \end{array}$$

By Dirichlet's theorem the two units groups of  $L$  and  $K$  are of rank  $d - 1$ , and we have :

$$[\mathcal{P}_\infty(L) : \mathcal{P}_\infty(K)] = [B^* : A^*]$$

**Lemma 2.1.** *The index  $Q := [B^* : A^*]$  divides  $n^{d-1}$ .*

**Proof.** We have  $B^* = \mathbb{F}_q^* B_1^*$  where  $B_1^*$  is free on  $d - 1$  generators. Let  $A_1^* = A^* \cap B_1^*$ . Then  $A^* = \mathbb{F}_q^* A_1^*$  and  $A_1^*$  is also free on  $d - 1$  generators. By the elementary divisors theorem, there is a basis  $\{\varepsilon_1, \dots, \varepsilon_{d-1}\}$  of  $B_1^*$  and integers  $m_i$  such that  $\{e_1 = \varepsilon_1^{m_1}, \dots, e_{d-1} = \varepsilon_{d-1}^{m_{d-1}}\}$  is a basis for  $A_1^*$ . If we denote by  $N_{L/K}$  the norm map from  $L$  to  $K$ , then applying  $N_{L/K}$

to each relation  $\varepsilon_i^{m_i} = e_i$  one sees that  $m_i$  divides  $n$  and this concludes the proof.  $\square$

**Proposition 2.2.** *We have*

$$\frac{R_B}{R_A} = \frac{n^{d-1}}{Q}$$

**Proof.** Consider the basis  $\{\varepsilon_1, \dots, \varepsilon_{d-1}\}$  of the previous proof. Then, we have

$$-\deg P_i v_{P_i}(\varepsilon_j^{m_j}) = \frac{-m_j}{e(\mathfrak{P}_i | P_i)} v_{\mathfrak{P}_i}(\varepsilon_j) = \frac{-m_j}{n} \deg \mathfrak{P}_i v_{\mathfrak{P}_i}(\varepsilon_j)$$

where  $e(\mathfrak{P}_i | P_i)$  is the ramification index of  $\mathfrak{P}_i$  over  $P_i$ . Since the regulator is defined as a  $(d-1) \times (d-1)$ -determinant, we get

$$R_A = \frac{\prod_{i=1}^{d-1} m_i}{n^{d-1}} R_B$$

$\square$

Now, let  $X_K$  be the smooth projective algebraic curve associated to the function field  $K$ . Weil's theorem states that the zeta function of  $X_K$ , defined as

$$Z_K(T) = \exp \left( \sum_{n=1}^{\infty} \#X_K(\mathbb{F}_{q^n}) \frac{T^n}{n} \right)$$

is a rational function  $Z_K(T) = \frac{P_K(T)}{(1-T)(1-qT)}$ . Here,  $P_K(T)$  is a polynomial with integral coefficients of degree  $2g_K$ , where  $g_K$  is the genus of the curve  $X_K$ , which can be described in the following way. Let  $T_\ell(J_K)$  be the Tate module of the Jacobian  $J_K$  of  $X_K$  with respect to any prime number  $\ell$  distinct to the characteristic of  $\mathbb{F}_q$ . Then  $T_\ell(J_K) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$  is a  $\mathbb{Q}_\ell$ -vector space of dimension  $2g_K$  on which the Frobenius morphism induces a linear map. Let  $f_K(T)$  be its characteristic polynomial. Then the numerator of the zeta function is the reciprocal polynomial of  $f_K(T)$ , i.e.  $P_K(T) = T^{2g_K} f_K(1/T)$ .

**Proposition 2.3.** *If  $L/K$  is a finite separable extension of function fields then  $h_K$  divides  $h_L$ .*

**Proof.** Let  $X_L$  be the smooth curve having  $L$  for its function field. Then, we have a finite morphism  $f : X_L \rightarrow X_K$  defined over  $\mathbb{F}_q$  between these

two curves. Let  $f^* : J_K \rightarrow J_L$  be the map induced by  $f$  on the Jacobians of  $X_K$  and  $X_L$ . Then  $f^*$  has finite kernel and sends the  $\ell^n$ -torsion points of  $J_K$  on the  $\ell^n$ -torsion points of  $J_L$ . We deduce from this an injective morphism

$$\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(J_K) \xrightarrow{1 \otimes f^*} \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(J_L),$$

since the tensor product kills the kernel of  $f^*$ . The Frobenius morphism on the  $\mathbb{Q}_\ell$ -vector-space  $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(J_L)$  leaves fixed the subspace  $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(J_K)$ . Hence the characteristic polynomial of the former divides the characteristic polynomial of the latter in  $\mathbb{Q}_\ell[T]$ , hence in  $\mathbb{Z}[T]$  since both  $P_K, P_L \in \mathbb{Z}[T]$  have constant term equals to 1. Since the divisor class number of a function field equal the number of  $\mathbb{F}_q$ -rational points of its jacobian which is equal to the value of the numerator of its zeta function on 1, then  $h_K$  divides  $h_L$ .  $\square$

If we define  $h_L^- = \frac{h_L}{h_K}$  as the relative divisor class number, then we have :

**Proposition 2.4.**

$$h_L^- \geq (\sqrt{q} - 1)^{2(n-1)(g_K-1)+\mathcal{R}}$$

where  $\mathcal{R}$  is the degree of the different of  $L/K$ .

**Proof.** The Riemann Hypothesis for function fields tell us that the inverse roots of the polynomials  $P_K(T)$  and  $P_L(T)$  are algebraic integers  $\omega_i$  of modulus  $\sqrt{q}$ . Thus, we have

$$h_L^- = \prod_{i=1}^{g_L-g_K} (1 - \omega_i)(1 - \bar{\omega}_i) \geq (\sqrt{q} - 1)^{2(g_L-g_K)}$$

By the Riemann-Hurwitz formula, we have  $2g_L - 2 = n(2g_K - 2) + \mathcal{R}$  where  $\mathcal{R}$  is the degree of the different of  $L/K$ , which is the contribution of the ramification in  $L/K$ . So we get the result.  $\square$

**Lemma 2.5.** *Up to isomorphism, there are only finitely many smooth algebraic projective curves defined over  $\mathbb{F}_q$  of bounded genus, where  $q$  is bounded.*

**Proof.** For elliptic curves, the degree of the equation of the curve is clearly bounded, so we get the result. Now, we can assume  $g > 1$ . Let  $\mathfrak{M}_g$  be the moduli scheme of curves of genus  $g$ . Then  $\mathfrak{M}_g \times \text{Spec}(\mathbb{F}_q)$  is a quasi-projective

variety over  $\mathbb{F}_q$ . Its  $\mathbb{F}_q$ -rational points correspond to  $\overline{\mathbb{F}}_q$ -isomorphism classes of curves of genus  $g$  defined over  $\mathbb{F}_q$ . There are only finitely many rational points over a finite field. If  $C$  is such a curve of genus  $g$  defined over  $\mathbb{F}_q$  the number of  $\mathbb{F}_q$ -isomorphism classes contained in the  $\overline{\mathbb{F}}_q$ -isomorphism class of  $C$  is the size of the group  $H^1(G, \text{Aut}(\overline{C}))$  where  $G = \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$  and  $\overline{C} = C \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ . When  $g > 1$ ,  $\text{Aut}(\overline{C})$  is finite and  $H^1(G, \text{Aut}(\overline{C}))$  is finite as well.  $\square$

Then, we have

**Theorem 2.6.** *Let  $K/k$  be a totally real function field of fixed degree and  $L/K$  a totally imaginary extension of  $K$  of fixed degree  $> 1$ . Let  $B$  be the integral closure of  $\mathbb{F}_q[X]$  in  $L$  and suppose the ideal class number of  $B$  is fixed. Then up to isomorphism, there are only finitely many such extensions  $L/K$ .*

**Proof.** By the relation (1) we have

$$h_B = \frac{r_A}{r_B} \frac{\delta_L}{\delta_K} \frac{h_L}{h_K} h_A$$

Using the relation (2), proposition 2.2 and 2.4. we get

$$h_B \geq h_A \frac{Q}{n^{d-1}} \prod_{i=1}^d \deg \mathfrak{P}_i (\sqrt{q} - 1)^{2(n-1)(g_K-1)+\mathcal{R}}$$

where  $n$  and  $d$  are respectively the degrees of the extensions  $L/K$  and  $K/k$ . The right hand side tends to infinity with  $q$  and  $g_K$  if  $q \geq 5$  and if  $g_K \neq 1$  and  $\mathcal{R} \neq 0$ . Thus, if the ideal class number  $h_B$  of  $B$  is fixed, these quantities are bounded and thus  $g_L$  is bounded too by Riemann-Hurwitz formula. Applying lemma 2.5, we have that there exists, up to isomorphism, only a finite number of such function fields  $K$  and  $L$ .

Furthermore, the condition  $q \geq 5$  can be suppressed since we have the following lower bound

$$h_L^- \geq q^{g_L - g_K - 1} \frac{(q-1)^2}{(q+1)(g_L - g_K + 1)}$$

which can be proved in the same way as Th.2 of [L-M]. Moreover, if  $g_K = 1$  and  $\mathcal{R} = 0$ , we get  $g_L = 1$  and we have a covering of elliptic curves. In this case, the divisor class number  $h_L$  of  $L$  is just the number of rational points over  $\mathbb{F}_q$  of the associated elliptic curve  $X_L$ , which is isogenous

to  $X_K$  so  $h_K = h_L$ . So if  $h_B$  is bounded, using relation (1) we see that  $h_L$  is also bounded and since the Weil's bound gives  $h_L \geq (\sqrt{q} - 1)^2$ , we see finally that  $q$  is bounded too and the lemma 2.5 still gives the result.  $\square$

## References.

- [L-M] G. Lachaud and M. Martin-Deschamps, *Nombre de points des jacobiniennes sur un corps fini*, Acta Arith. LVI (1990), 329-340.
- [M] R. E. MacRae, *On unique factorization in certain rings of algebraic functions*, J. Algebra **17** (1971), 243-261.
- [R] M. Rosen, *The Hilbert class field in function fields*, Expo. Math. **5** (1987), 365-378.
- [S] T. A. Schmidt, *Infinitely many real quadratic fields of class number one*, J. of Number Theory **54**, 203-205 (1995).

Yves Aubry  
Département de Mathématiques  
Université de Caen  
Esplanade de la Paix  
14 032 Caen Cedex - France  
e-mail : aubry@math.unicaen.fr