PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 2, February 1990

GENERATING FUNCTIONS FOR THE NUMBERS OF ABELIAN EXTENSIONS OF A LOCAL FIELD

ARTUR TRAVESA

(Communicated by William Adams)

ABSTRACT. The aim of this paper is to give an explicit formula for the numbers of abelian extensions of a $\mathbf{p}$-adic number field and to study the generating function of these numbers. More precisely, we give the number of abelian extensions with given degree and ramification index, and the number of abelian extensions with given degree of any local field of characteristic zero. Moreover, we give a concrete expression of a generating function for these last numbers.

1. INTRODUCTION

The problem of "counting extensions" has been studied in the local case by M. Krasner in [Kr1] and by J-P. Serre in [Se1]. Krasner gave formulas for the numbers

(1) of all totally ramified extensions with given degree and discriminant;
(2) of all totally ramified extensions with given degree; and
(3) of all extensions with given degree.

Serre re-obtained these numbers by means of a "mass formula" (cf. [Se1], [Tr2]).

We fix our attention on the abelian case. Let K be a local field, fix a separable closure $K^{sep}|K$, and for all pairs (n,e) of positive integers consider the sets

$$\begin{aligned}\Sigma(n;K) &= \{L|K\colon K\subseteq L\subseteq K^{sep} \text{ and } [L\colon K]=n\},\\ \Sigma(n,e;K) &= \{L\in\Sigma(n;K)\colon e(L|K)=e\},\\ \Sigma_{ab}(n;K) &= \{L\in\Sigma(n;K)\colon L|K \text{ abelian}\},\\ \Sigma_{ab}(n,e;K) &= \{L\in\Sigma(n,e;K)\colon L|K \text{ abelian}\},\end{aligned}$$

where $[L\colon K]$ and $e(L|K)$ denote the degree and the ramification index of the extension $L|K$, respectively. Consider also their cardinals $s(n;K)$, $s(n,e;K)$, $a(n;K)$, and $a(n,e;K)$.

Received by the editors May 12, 1989 and, in revised form, June 10, 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11S31, 11S40; Secondary 11Y40, 11M41.

Key words and phrases. Abelian extension, local field, generating function, Dirichlet series.

When K is of characteristic zero, K is a finite extension of the field Q_p of the p-adic numbers; then, $\Sigma(n;K)$ is a finite set (cf. [La1: Chap. II, § 5, Prop. 14]), and therefore $\Sigma(n,e;K)$, $\Sigma_{ab}(n;K)$, and $\Sigma_{ab}(n,e;K)$ are also finite.

We define the generating functions

$$G(K;s)=\sum_{n\geq 1}a(n;K)n^{-s}$$

$$G_{nr}(K;s)=\sum_{n\geq 1}a(n,1;K)n^{-s}$$

$$G_{tr}(K;s)=\sum_{n\geq 1}a(n,n;K)n^{-s}$$

of the numbers of abelian extensions of K, of the numbers of unramified (abelian) extensions of K, and of the numbers of totally ramified abelian extensions of K, respectively.

The aim of this work is to give explicit expressions for these generating functions and, also, for their coefficients. The numbers of extensions are given in Theorem 5, and the generating functions are given in Theorem 6.

2. The tamely ramified case

We begin with the unramified case. Let $n_0=[K:Q_p]$ be the absolute degree, and put q the cardinal of the residual field $\widetilde{K}$ of K; i.e. $q=p^{f_0}$ with $f_0=f(K|Q_p)$ the absolute residual degree. For all $n\geq 1$ K has only one unramified extension of degree n, namely, $K(\zeta)$ where ζ is a primitive (q^n-1)th root of the unity, and it is abelian. So, we have $a(n,1;K)=s(n,1;K)=1$ and, then, $G_{nr}(K;s)=\zeta(s)$ is the Riemann zeta function.

For the tamely ramified case we have:

Proposition 1. *Let n, e be positive integers such that $e\mid n$ and $(p,e)=1$. Then, the following statements are equivalent*:

(1) $\Sigma_{ab}(n,e;K)\neq\varnothing$;
(2) K *contains all primitive eth roots of the unity*;
(3) $e\mid q-1$;
(4) $\Sigma_{ab}(n,e;K)=\Sigma(n,e;K)$;
(5) $a(n,e;K)=e$.

Proof. (1) ⇒ (2) Assume that $L\in\Sigma_{ab}(n,e;K)$, and let $K_0|K$ be the only unramified extension of degree $f=n/e$ of K; then $K_0\subseteq L$ and we can write $L=K_0(\alpha)$ where α^e is a prime element of K_0. If π is a prime element of K we can put $\alpha^e=u\pi$ with u an invertible element of K_0; as $K(\alpha)\subseteq L$, we have $K(\alpha)|K$ abelian. On the other hand, $K_0(u^{1/e})|K$ is unramified, and so, abelian. But $\pi^{1/e}\in K(\alpha,u^{1/e})$, and so $K(\pi^{1/e})|K$ is abelian. This implies that K contains the eth roots of the unity. (2) ⇒ (3) For, then $\widetilde{K}$ contains the eth roots of the unity. (3) ⇒ (4) If $L\in\Sigma(n,e;K)$ then $L=K_0(\alpha)$ as in (1) ⇒ (2). But $\widetilde{K}$ contains the eth roots of the unity, and by Hensel's lemma, so does K; then $K_0(u^{1/e}, \pi^{1/e})|K$ is abelian and $L \subseteq K_0(u^{1/e}, \pi^{1/e})$; so $L|K$ is abelian. (4) $\Rightarrow$ (5) $a(n,e;K) = s(n,e;K) = s(e,e;K_0) = e$ (cf. [Se1]). (5) $\Rightarrow$ (1) is obvious. □

Remarks. (1) Observe that if $e \mid q-1$, then $a(n,e;K) = e$ does not depend on the particular values of n such that $e \mid n$.

(2) Proposition 1 and its proof are also true in the case of a local field of characteristic $p > 0$.

3. The general case

The Lubin–Tate theory (cf. [Ne1: Chap. III, §7]) describes the maximal abelian extension $K^{ab}|K$. Let π be a prime element of K, and let F be a Lubin–Tate module for π. Denote by K_m the field obtained from K by the adjunction of the points of π^m-division of F, and put $K^{(\pi)} = \bigcup_{m \geq 1} K_m$. Then, $K^{ab} = K^{(\pi)} K^{nr}$ where $K^{nr}|K$ is the maximal unramified extension of K. One has that $K_m|K$ is a totally ramified abelian extension such that

$$[K_m : K] = q^{m-1}(q-1), \tag{1}$$

and

$$Gal(K_m|K) \simeq U_K / U_K^{(m)}, \tag{2}$$

the factor group of the units of K by the units of K congruent to 1 mod π^m.

Let n, e be positive integers such that $e \mid n$ and assume that $L \in \Sigma_{ab}(n,e;K)$; then, there exist $N, m \geq 1$, $(p,N) = 1$, and a primitive Nth root of the unity, ζ, such that $L \subseteq K_m(\zeta)$; as $e(K_m(\zeta)|K) = e(K_m|K) = q^{m-1}(q-1)$ we have $e = p^r e'$ with $r \geq 0$ and $e' \mid q-1$. Put $n = p^s n'$, $(p,n') = 1$; the fact that we are dealing with abelian extensions and the decomposition of their Galois groups into direct sum of Sylow's p-subgroups, implies that $a(n,e;K) = a(n',e';K)a(p^s,p^r;K)$. So we can restrict our attention to the case $n = p^s$, $e = p^r$, $0 \leq r \leq s$. The set $\Sigma_{ab}(p^s,p^r;K)$ is finite and so we can select a sufficiently large integer $m \geq 1$ and a certain root of the unity, ζ, such that for all $L \in \Sigma_{ab}(p^s,p^r;K)$ is $L \subseteq K_m(\zeta)$. Moreover L is a subfield of the maximal p-subextension of $K_m(\zeta)$; this subextension is $K'_m(\zeta)$, where K'_m is the maximal p-subextension of K_m and ζ is a $(q^{p^u} - 1)$th root of unity for some integer $u \geq 0$. Looking at the Galois group $Gal(K'_m(\zeta)|K) \simeq Gal(K'_m|K) \times Gal(K(\zeta)|K)$, and because $K(\zeta)|K$ is cyclic, one sees that we can assume $u = s$.

Let $L_1, \dots, L_t$ be all the subextensions $L_j \subseteq K'_m$ such that $[L_j : K] = p^r$. We have the following

Lemma 2. *For all $L \in \Sigma_{ab}(p^s,p^r;K)$ there exists exactly one index j, $1 \leq j \leq t$, such that $L \subseteq L_j(\zeta)$.*

Proof. The $L_j(\zeta)$ are subextensions of $K'_m(\zeta)$ which contain $K(\zeta)$ and have ramification index $e(L_j(\zeta)|K) = p^r$; in fact, they are the only ones. So $L(\zeta)$ is one of them. □

Consider, now, one of the L_j, $1 \le j \le t$; we put $G_j = Gal(L_j(\zeta)|K(\zeta)) \simeq Gal(L_j|K)$, $G_0 = Gal(L_j(\zeta)|L_j) \simeq Gal(K(\zeta)|K) \simeq Z/p^sZ$, and we identify $Gal(L_j(\zeta)|K)$ with the finite abelian p-group $G = G_0 \oplus G_j$. We shall use the additive notation for all these groups.

We can compute the ramification index $e(L|K)$ for all fields $L \subseteq L_j(\zeta)$. In fact, if $X = Gal(L_j(\zeta)|L)$ we have $e(L|K) = (G_j \colon G_j \cap X)$, because $L_j(\zeta)|K(\zeta)$ is totally ramified and $G_j \cap X = Gal(L_j(\zeta)|L(\zeta))$. So, we have $e(L|K) = p^r$ if and only if $G_j \cap X = (0)$. We summarize this in the following lemma:

Lemma 3. *There exists a one-to-one map between the sets*

$$B_j = \{X \subseteq G_0 \oplus G_j \colon (G_0 \oplus G_j \colon X) = p^s \text{ and } G_j \cap X = (0)\},$$

and,

$$\Sigma_{ab}^{(j)}(p^s, p^r; K) = \{L \in \Sigma_{ab}(p^s, p^r; K) \colon L \subseteq L_j(\zeta)\}. \quad \square$$

But the cardinal of the set B_j does not depend on j. In fact, we shall obtain $\#B_j = p^r$ for all j from the more general result:

Proposition 4. *Let G_1 be a finite abelian p-group of order p^r and let $G_0 \simeq Z/p^sZ$. Put $G = G_0 \oplus G_1$ and define $B = \{X \subseteq G \colon (G \colon X) = p^s$ and $G_1 \cap X = (0)\}$. If $r \le s$ then $\#B = p^r$, otherwise B is the empty set.* $\square$

Corollary. *For $0 \le r \le s$ we have $a(p^s, p^r; K) = p^r t_r$, where t_r is the number of open subgroups of U_K of index p^r.*

Proof. It remains to compute the number t of subfields $L_j \subseteq K'_m$ such that $[L_j \colon K] = p^r$; it is the same than the number of subgroups of $Gal(K'_m|K)$ of index p^r. But this group is isomorphic to the Sylow's p-subgroup of $Gal(K_m|K) \simeq U_K/U_K^{(m)}$, and there is a one-to-one map between the set of all subgroups of index p^r of $U_K/U_K^{(m)}$ and the set of all the open subgroups of index p^r of U_K, for m sufficiently large. $\square$

Observe that $a(p^s, p^r; K)$ does not depend on $s \ge r$. We have, then, the following theorem:

Theorem 5. *Let n, e be positive integers. Write $n = p^s n'$, $e = p^r e'$ with $(p, e'n') = 1$. Then, we have*

$$a(n, e; K) = \begin{cases} e\,t_r, & \text{if } e \mid n \text{ and } e' \mid q-1, \\ 0, & \text{otherwise}; \end{cases} \tag{1}$$

$$a(n; K) = \sigma_1(\gcd(n, q-1)) \sum_{r=0}^{s} p^r t_r, \tag{2}$$

where $\sigma_1(m) = \sum_{d|m} d$ and t_r is the number of open subgroups of index p^r of U_K. $\square$

4. The generating functions

Let us forget for a moment the convergence questions. We have just seen that, if $e \mid n$, $a(n,e;K) = a(e,e;K)$; this implies that

$$a(n;K) = \sum_{e|n} a(n,e;K) = \sum_{e|n} a(n/e,1;K)a(e,e;K).$$

This equality says us that the arithmetic function $n \longmapsto a(n;K)$ is the Dirichlet convolution of the functions $n \longmapsto a(n,1;K)$ and $n \longmapsto a(n,n;K)$. So the series $G(K;s)$ is the ordinary product of the series $G_{nr}(K;s)$ and $G_{tr}(K;s)$ (cf. [Ap1: Chap. 11, §4, Thm. 11.5]). Moreover, the arithmetical function $a(n,n;K)$ is multiplicative and so, we can write the Euler product, extended over all the prime numbers ℓ,

$$G_{tr}(K;s) = \prod_{\ell} B_{\ell}(K;s),$$

where

$$B_{\ell}(K;s) = \sum_{r\geq 0} a(\ell^r,\ell^r;K)\ell^{-rs}.$$

Assume, now, that $\ell \neq p$. From Proposition 1 we have that $B_{\ell}(K;s)$ is a finite sum; in fact, if $a(\ell^r,\ell^r;K) \neq 0$ then ℓ^r must divide $q-1$; in particular, we have $B_{\ell}(K;s) = 1$ for all ℓ not dividing $p(q-1)$. Moreover one can compute easily the product

$$\prod_{\ell\neq p} B_{\ell}(K;s) = \sigma_{1-s}(q-1),$$

where $\sigma_{1-s}(m) = \sum_{d|m} d^{1-s}$.

From the equalities

$$\begin{aligned} G(K;s) &= G_{nr}(K;s)G_{tr}(K;s) \\ &= \zeta(s)\sigma_{1-s}(q-1)B_p(K;s) \end{aligned}$$

we need only to prove the convergence and to sum the series

$$\begin{aligned} B_p(K;s) &= \sum_{r\geq 0} a(p^r,p^r;K)p^{-rs} \\ &= \sum_{r\geq 0} t_r p^{r(1-s)} \end{aligned}$$

in some semiplane.

The structure theorem of the units of K (cf. [Ha1: Chap. 15, §5]) says us that if $\mu \geq 0$ is the greatest integer such that K contains all the primitive p^{μ}th roots of the unity, then

$$U_K \simeq Z/p^{\mu}Z \times Z/(q-1)Z \times Z_p^{n_0},$$

Z_p being the ring of the p-adic integers. Observe that this group is the product of a finite abelian group and an abelian profinite p-group.

So, let A be a finite abelian group and put $G = A \times Z_p^{n_0}$. For all integers $r \geq 0$ put $t_r(A, n_0)$ the number of all open subgroups of G of index p^r, and define the generating function

$$g(A, n_0; T) = \sum_{r \geq 0} t_r(A, n_0) T^r$$

of these numbers.

Remark. Observe that if we put $A = Z/p^\mu Z \times Z/(q-1)Z$, we obtain that

$$B_p(K; s) = g(A, n_0; p^{1-s});$$

so the problem related to $B_p(K; s)$ is reduced to a group problem.

We state here the result concerning $G(K; s)$.

Theorem 6. *Let K be a finite extension of Q_p of degree n_0 and let $\mu \geq 0$ be the greatest integer such that K contains the primitive p^μth roots of the unity. Then, we have*

(1) *$G(K; s)$ is convergent in some semiplane and extends meromorphically to all the plane with simple poles at $s = 2, 3, \dots, n_0$ and a double pole at $s = 1$.*

(2) *The extension has the expression*

$$G(K; s) = \zeta(s)\sigma_{1-s}(q-1)\frac{1 - p^{(n_0+1-s)(\mu+1)}}{1 - p^{(n_0+1-s)}} Z(G_{F_p}(1, n_0); p^{1-s}),$$

where $\zeta(s)$ is the Riemann zeta function and

$$Z(G_{F_p}(1, n_0); T) = \prod_{h=1}^{n_0} (1 - p^{h-1} T)^{-1}$$

is the zeta function of the Grassmannian defined by all the lines of an $(n_0 + 1)$-dimensional vector space over F_p.

The result will follow from a more general result that we shall prove in the next paragraph.

5. The group problem

Let A be a finite abelian p-group. Put $G_1 = A \times Z_p^{n_0 - 1}$, $G_2 = Z_p$, $G = G_1 \oplus G_2$ and define the set $S_r(A, n_0)$ of all the open subgroups of G of index p^r. If $X \in S_r(A, n_0)$, then $p^r G \subseteq X$ and $G/p^r G$ is a finite abelian p-group. So we have a one-to-one map between $S_r(A, n_0)$ and $S_r(G/p^r G, 0)$, and, then, $t_r(A, n_0) = t_r(G/p^r G, 0)$.

If we put $G_1' = G_1/p^r G_1$, $G_2' = G_2/p^r G_2 \simeq Z/p^r Z$ we have $G/p^r G \simeq G_1' \oplus G_2'$. Moreover, if $X' \in S_r(G_1' \oplus G_2', 0)$ we have $(G_1' \colon G_1' \cap X') = p^h$ for some h, $0 \leq h \leq r$. So, we can write the cardinal $t_r(A, n_0)$ as the sum, for $0 \leq h \leq r$, of the cardinals of the sets

$$\{X' \subseteq G_1' \oplus G_2' \colon (G_1' \oplus G_2' \colon X') = p^r \text{ and } (G_1' \colon G_1' \cap X') = p^h\}.$$

Now, this set is the disjoint union, for all subgroups $B \subseteq G_1'$ such that $(G_1' \colon B) = p^h$, of the sets

$$\{X' \subseteq G_1' \oplus G_2' \colon (G_1' \oplus G_2' \colon X') = p^r \text{ and } G_1' \cap X' = B\},$$

and each one of them is equipotent, by passing to the quotient, $X'' = X'/B$, with the set

$$\{X'' \subseteq G_1'' \oplus G_2' \colon (G_1'' \oplus G_2' \colon X'') = p^r \text{ and } G_1'' \cap X'' = (0)\},$$

where $G_1'' = G_1'/B$. As $G_2' \simeq Z/p^rZ$, and G_1'' is a finite abelian p-group with order p^h, we can apply Proposition 4: its cardinal equals p^h. So, we have the formula

$$\begin{aligned} t_r(A, n_0) &= \sum_{h=0}^{r} \sum_{\substack{B \subseteq G_1/p^rG_1 \\ (G_1/p^rG_1 \colon B) = p^h}} p^h \\ (*) \qquad &= \sum_{h=0}^{r} p^h t_h(G_1/p^rG_1, 0) \\ &= \sum_{h=0}^{r} p^h t_h(A, n_0 - 1), \end{aligned}$$

because $t_h(A, n_0 - 1) = t_h(G_1/p^hG_1, 0) = t_h(G_1/p^rG_1, 0)$.

Theorem 7. *With the above notations we have*:

(1) *The series* $g(A, n_0; T)$ *has a positive radius of convergence*;
(2) $g(A, 0; T)$ *is a polynomial in* T *with positive integer coefficients*;
(3) $g(A, n_0; T) = g(A, 0; p^{n_0}T)Z(G_{F_p}(1, n_0); T)$;
(4) $g(A, n_0; T)$ *has poles only at* $T = p^{-j}$ *for* $j = 0, 1, 2, \dots, n_0 - 1$, *and they are simple.*

Proof. We have, from the above formula, that $t_r(A, n_0) = O(p^{rn_0})$ (induction over n_0). So the radius of convergence of $g(A, n_0; T)$ is at least equal to p^{-n_0}. Moreover,

$$\begin{aligned} g(A, n_0; T) &= \sum_{r \geq 0} \left(\sum_{h=0}^{r} p^h t_h(A, n_0 - 1) \right) T^r \\ &= \sum_{i \geq 0} T^i \sum_{j \geq 0} t_j(A, n_0 - 1)(pT)^j \\ &= \frac{1}{1 - T} g(A, n_0 - 1; pT). \end{aligned}$$

Now, induction over n_0 implies that

$$g(A, n_0; T) = g(A, 0; p^{n_0}T) \prod_{h=1}^{n_0} (1 - p^{h-1}T)^{-1};$$

and the last product is $Z(G_{F_p}(1, n_0); T)$.

Moreover A is finite, so $g(A, 0; T)$ is a polynomial in T of degree r (if A is of order p^r) and with positive integer coefficients. The question concerning poles is clear if one notes that the polynomial $g(A, 0; p^{n_0}T)$ has no positive real zeroes. □

Remarks. (1) It is not difficult to prove that if C is the number of all subgroups of A, then one has that $t_r(A, n_0) \leq C2^{n_0}p^{n_0 r}$.

(2) Assume that $A = Z/p^\mu Z$. Then

$$g(A, 0; T) = (1 - T^{\mu+1})/(1 - T),$$

because $t_r(A, 0) = 1$ for $0 \leq r \leq \mu$, and $t_r(A, 0) = 0$ for $r > \mu$.

6. Final remarks

We can obtain the numbers $a(n, e; K)$ and $a(n; K)$ explicitly. In fact, by the formulas in Theorem 5 we need only to give the numbers $t_r(Z/p^\mu Z, n_0)$ for all $r \geq 0$. This can be done in two different ways: by induction using the formula $(*)$, or by expanding the generating function

$$g(Z/p^\mu Z, 0; p^{n_0}T) \prod_{h=1}^{n_0} (1 - p^{h-1}T)^{-1}$$

into a power series in T. This leads to the following proposition:

Proposition 8. *One has that*

$$\begin{aligned} t_r(Z/p^\mu Z, n_0) &= \begin{bmatrix} n_0 + r \\ r \end{bmatrix}_p - p^{n_0(\mu+1)} \begin{bmatrix} n_0 + r - (\mu+1) \\ r - (\mu+1) \end{bmatrix}_p \\ &= \sum_{\overline{M}=r} p^{\sum_{i\geq 1} M_{i+1}(N_i - M_i)} \prod_{i \geq 1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p, \end{aligned}$$

where the last sum is extended over all the partitions $\overline{M}$: $M_1 + \cdots + M_r = r$ *such that* $M_1 \geq \cdots \geq M_r \geq 0$, $M_i \leq N_i$, $i \geq 1$ *and* $N_1 = \cdots = N_\mu = n_0 + 1$, $N_i = n_0$, *for* $i > \mu$; *and where the symbol*

$$\begin{bmatrix} N + M \\ M \end{bmatrix}_p = \prod_{j=1}^{M} \frac{p^{N+j} - 1}{p^j - 1}$$

is the value at p *of the generating polynomial of the Betti numbers* $\beta_{2i}(G_{F_p}(M, N))$ *of the Grassmannian manifold of the* M*-dimensional subspaces of a* $(N + M)$*-dimensional vector space over* F_p.

A proof of this proposition can be found in [Tr1].

Acknowledgment

I am very grateful to Prof. Dr. P. Bayer for all the time that she has devoted to directing the work that has led me to preparing this paper, and also for her valuable suggestions and advice.

REFERENCES

[Ap1] T. M. Apostol, *Introduction to analytic number theory*, UTM Springer-Verlag, New York, 1976.

[Ha1] H. Hasse, *Number theory*, GMW 229 Springer-Verlag, Berlin-Heidelberg, 1970.

[Kr1] M. Krasner, *Nombre des extensions d'un degré donné d'un corps p-adique*, C.R. Acad. Sc. Paris **254** (1962), 3470–3472; C. R. Acad. Sc. Paris **255** (1962), 224–226, 1682–1684, 2342–2344, 3095–3097, See also Les tendances géométriques en algèbre et théorie des nombres. Colloques internationaux du C.N.R.S. **143** (1966), pp. 143–169..

[La1] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Massachusetts, 1970.

[Ne1] J. Neukirch, *Class field theory*, GMW 280 Springer-Verlag, Berlin-Heidelberg, 1986.

[Se1] J.-P. Serre, *Une formule de masse pour les extensions totallement ramifiées de degré donné d'un corps local*, C. R. Acad. Sc. Paris **286** (1978), 1031–1036.

[Tr1] A. Travesa, *Nombres d'extensions abelianes i les seves funcions generatrius*, Doctoral Thesis, Universitat de Barcelona, 1987.

[Tr2] ——, *Sobre el número de extensiones de grado dado de un cuerpo local*, Actas de las X Jornadas Hispano-Lusas de Matemáticas, Sección I: Álgebra y Fundamentos, Murcia, 1985, pp. 235–243.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA, FACULTAT DE MATEMÀTIQUES, UNIVERSITAT DE BARCELONA, GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA, CATALUNYA, SPAIN