Session : Polynomes And NumberTheory

Root-elements and root-subgroups of the Chevalley group $E_6(K)$, for fields K of characteristic two

Abdulkareem Alhuraiji[1]

[1] Department of Mathematics
Public Authority for Applied Education and Training, Kuwait

Abstract

Let K be a field of characteristic two, and A be a 27-dimensional module over K with basis $\{e_x \mid x \in \Omega\}$, where Ω is a quadratic in the generalized quadrangle $(\mathcal{P}, \mathcal{L})$ of type $O_6^-(2)$. Let Δ be a root base of size 6 and $k \in K$, define the root-elements $r_\Delta(k) \in GL(A)$ by

$$e_x^{r_\Delta(K)} = \begin{cases} e_x + ke_x^{\sigma_\Delta} & , \quad x \in \Delta \\ e_x & , \quad \text{otherwise} \end{cases}$$

where σ_Δ is a reflection on a 6-dimensional vector space over $\mathbb{F}_2$, defined by $v^{\sigma_\Delta} = v + (v|s)$, where $s \in V$ with $Q(s) \neq 0$, and Q is a non-degenerate quadratic form on V. If $r_\Delta(k)$ is a roo-element, let $U_\Delta(k) = \{r_\Delta(k) \mid k \in K\}$ be the corresponding root-subgroup and let $\mathbb{E} = \langle U_\Delta(k) \mid \Delta \text{ root-base, } k \in K\rangle$. The purpose of this talk, is to give two new definitions for root-elements and root-subgroups and show that these two notions are equivalent.

Topologies de Grothendieck et Applications

Khadija.AZI, Hinda. Hamraoui

Faculté des Siences Ain Chock , Université Hassan II Casablanca

Abstract

a Grothendieck topology T on a category S and the corresponding shaves. The couple (S,T) is called a site. We give various examples of sites and some applications of Zariski, Etale , Nisnevish and the Arithmetic sites.

On construction of certain Lie algebras embedding of $E_6(K)$ for fields K of characteristic two

Mashhour Bani-Ata[1]

[1] Department of Mathematics
Public Authority for Applied Education and Training, Kuwait

Abstract

The purpose of this talk is to give an elementary construction of Liealgebras of type G_2 in K(K), for fields of characteristic two. This will be achieved by embedding G_2 in $E_6(K)$ where the construction of Lie-algebras of type $E_6(K)$ for fields K of characteristic two, has been given in [2]. The embedding of G_2 in $E_6(K)$ could be achieved by embedding G_2 in the embedding $D_4(K) < F_4(K) < E_6(K)$, .[1].

References

[1] M. Bani-Ata, *On the embedding of Lie algebras D_6 , F_4 in E_6 for fields K of characteristic two*, Preprint.

[2] S. Aldhafeeri and M. Bani-Ata, *On the construction of Lie algebras of type $E_6(K)$ for fields K of characteristic two*, Beitrag Zur Algebra Und Geometrie, **58** (2107), 529-534.

Sub-p-rational fields of the cyclotomic fields

Z. Boughadi[1],and Z. Bouazzaoui[2]

[1]Mathematics department, Moulay Ismail University, Meknes
[2]Mathematics department, Moulay Ismail University, Meknes

Résumé/Abstract

For a non p-rational abelian number field K, we give a one-to-one correspondence between p-rational subfields of K and subgroups of the Galois group of $K/\mathbf{Q}$ satisfying a property related to a special characters set. Then, we give evidence for the validity of a conjecture of Greenberg on the existence of cyclic complex p-rational fields of degree at least 4 and dividing $p-1$.

Références

[1] J. Assim, *Codescente en K-théorie étale et corps de nombres*, Manuscripta Math. 86 (1995) : 499-518.

[2] R. Greenberg, *Galois representations with open image*, Annales mathématiques du Québec, 40 (2016), 83-119.

[3] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Thèse Paris VII (1988).

Permutation polynomials of degree 4 over $\mathbb{F}_q$ of characteristic ≥ 5

Belhout. BOUSALMI[1], and Abdallah. DERBAL[2]

[1,2]Laboratoire d'Equations aux Dérivées Partielles Non linéaires et Histoire des Mathématiques, Ecole Normale Supérieure, B.P. 92, 16308 Vieux Kouba, Alger, Algérie

Résumé/Abstract

Let p be a prime number and let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^n$. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial of $\mathbb{F}_q$ if its associated polynomial mapping $f : x \to f(x)$ from $\mathbb{F}_q$ to itself is a bijection.

The studies of permutation polynomials began with Hermite [2] on the prime fields. Dickson (1896 - 1897) studied permutation polynomials of degree 5 on arbitrary finite fields. Refer that there is a table in the book [5] that classifies permutation polynomials of degree ≤ 5.

In addition to that, there are results in [4] on permutation polynomials of degree 6 and 7 over finite fields $\mathbb{F}_{2^n}$.

Using elementary methods, we present conditions on the coefficients of a polynomial of the degree 4 which are necessary for it to represent a permutation over $\mathbb{F}_q$ where $q = p^n$ and $p \geq 5$. We also give some results on polynomials which are not a permutation polynomial over $\mathbb{F}_q$ and q satisfie some asymptions.

In this paper we prove the following results.

Theorem 1

Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{F}_q[x]$ $(q = p^n, p \geq 5)$. Then f is a permutation polynomial of $\mathbb{F}_q$ implies that $(a^3 + 8c \neq 4ab)$ and $(3a^2 \neq 8b$ or $q \equiv 1 \pmod 3)$

Corollary

Polynomials of the form $f(x) = x^4 + ax^2 + b \in \mathbb{F}_q[x]$ such that q is odd, are not permutation polynomials of $\mathbb{F}_q$.

Theorem 2

Let p a prime number, such that $p \equiv 1 \pmod 3$ and $q = p^n (n \in \mathbb{N}^*)$. All the polynomials of $\mathbb{F}_q[x]$ of the form $ax^{3q^m} + bx^{2q^m} + cx^{q^m} + d$ $(a \neq 0$ and $m \in \mathbb{N}^*)$, are not permutation polynomials of $\mathbb{F}_q$.

Références

[1] C. Hermite, Sur les fonctions de sept lettres, C. R. Acad. Sci-Paris 57 (1863) 750-757.

[2] C.Small, Arithmetic of Finite Fields, CRC Press, 24 avr. 1991 - 240 pages.

[3] J. Li, D.B. Chandler, Q.Xiang, Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, 2010 Elsevier pp 406-419.

[4] L. E. Dickson, The analytic representation of substitutions on a prime power of letters with a discussion of the linear group, Ann. of Math. 11 (1897), 65-120, 161-183.

[5] R. Lidl and H. Niederreiter. Finite Fields. Cambridge University Press, second edition, 1997.

On the 2-class group of some number fields with large degree

Mohamed Mahmoud Chems-Eddin[1], Abdelmalek Azizi[2] and Abdelkader Zekhnini[3]

[1,2,3]Laboratoire Acsa, Université Mohammed Premier, Oujda

Résumé/Abstract

Let d be an odd square-free integer, $m \geq 3$, $\Bbbk := \mathbb{Q}(\sqrt{d}, \sqrt{-1})$, $\mathbb{Q}(\sqrt{-2}, \sqrt{d})$ or $\mathbb{Q}(\sqrt{-2}, \sqrt{-d})$, and $L_{m,d} := \mathbb{Q}(\zeta_{2^m}, \sqrt{d})$. In this paper, we shall determine all the fields $L_{m,d} := \mathbb{Q}(\zeta_{2^m}, \sqrt{d})$, with $m \geq 3$ is an integer, such that the class number of $L_{m,d}$ is odd. Furthermore, using the cyclotomic $\mathbb{Z}_2$-extensions of $\Bbbk$, we compute the rank of the 2-class group of $L_{m,d}$ whenever the divisors of d are congruent 3 or 5 (mod 8).

Références

[1] A. Azizi, M. M. Chems-eddin and A. Zekhnini, *On rank of the 2-class group of some imaginary triquadratic number fields*, submitted(2019), arXiv :1905.01225

[2] M. M. Chems-eddin, A. Azizi and A. Zekhnini, *On the 2-class group of some number fields with large degree*, submitted(2019), arXiv :1911.11198.

[3] A. Mouhib, A. Movahhedi, *Cyclicity of the unramified Iwasawa module*, Manuscripta Math , 135 (2011) : 91-106.

[4] T. Fukuda, *Remarks on Z_p-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci , 70(1994) : 264-266.

On The Diophantine Equation $x^2 + 7^k = y^n$

A. EL ACHAB,

Université Cadi Ayyad, Faculté des Sciences, Marrakech

Abstract

In this paper, we give all the solutions of the Diophantine equation $x^2 + 7^k = y^n$, in nonnegative integers $k,\ x,\ y,\ n \geq 3$ with x and y coprime, except for the case when $k.x$ is odd .

Keywords : Exponential equations, Primitive divisors of Lucas

Références

[1] S. A. Arif and F. S. A. Muriefah, The diophantine equation $x^2 + 3^m = y^n$, *Internat. J. Math. Math. Sci.*, **21** (1998), 619–620.

[2] S. A. Arif and F. S. A. Muriefah, On the Diophantine equation $x^2 + q^{2k+1} = y^n$, *J. Number Theory*, **95** (2002), no. 1, 95–100.

[3] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte), *J. Reine Angew. Math.*, **539** (2001), 75–122.

[4] A. Bérczes and I. Pink, On the Diophantine equation $x^2 + p^{2k} = y^n$, *Arch. Math.*, **91** (2008), 505–517.

[5] A. Bérczes and I. Pink, On the Diophantine equation $x^2 + d^{2\ell+1} = y^n$, *Glasg. Math. J.*, **54** (2012), no. 2, 415–428.

[6] F. Luca, On a Diophantine equation, *Bull. Austral. Math. Soc.*, **61** (2000), no. 2, 241–246.

[7] F. Luca, Sz. Tengely and A. Togbe, On the Diophantine equation $x^2 + C = 4y^n$, *Ann. Sci. Math. Quebec*, **33** (2009), no. 2, 171–184.

[8] V. A. Lebesgue, Sur l'impossibilitg en nombres entiers de liquation $x^m = y^2 + 1$, *Nouvelles Annales des Math.*, **9** (1850), p. 178.

Sur la divisibilité par les puissances de 2 du nombre de classes de certains corps quartiques cycliques réels

Mohammed Tamimi

Université Mohammed Premier
Faculté des sciences d'Oujda
Maroc
med.tamimi@gmail.com

Travail en commun avec : A. Azizi and A. Zekhnini.

Étant donné un corps de nombres quartique cyclique réel $\mathbb{K} = \mathbb{Q}(\sqrt{n\epsilon_0\sqrt{l}})$, où n et l sont deux entiers non nuls positifs libres de carrés et ϵ_0 l'unité fondamentale du sous-corps quadratique réel $k = \mathbb{Q}(\sqrt{l})$. Le travail porte sur la divisibilité par les puissances de 2 du nombre de classes de certains corps quartiques cycliques réels $\mathbb{K}$.

Mots clefs : Corps cycliques quartiques réels, groupe de classes, le rang du 2-groupe de classes, groupe de classe d'ordre impair, divisibilité par 2 du nombre de classes.

Références

[1] Brown E, Parry Ch J. *The 2-class group of certain biquadratic number fields*. Journal fur die reine und angewandte Mathematik, volume 295, (1977) 61-71.

[2] Gras M N. *Table numérique du nombre de classes et des unités d'extensions cycliques réelles de degré 4 de* $\mathbb{Q}$. Publ. Math. Fac. Sciences Bensançon, Théorie des Nombres (1977-78).

[3] Parry Ch J. *Pure quartic number fields whose class numbers are even*. Journal reine angew Math, Volume 264,(1975) 102-112.

[4] Ch. J. Parry, *A genus theory for quartic fields,* J. reine angew. Math. 314 (1980), 40?71.