Early Contributions to the Inverse and Embedding Galois Problems

(after N. Vila, A. Arenas, T. Crespo)

•

Pilar Bayer Isant

UB

•

STNB, 29th edition

2015-01-29

Contents

INTRODUCTION

- 1892, D. Hilbert

S_n and A_n are Galois groups over $\mathbb{Q}(T)$

Irreducibility theorem

- 1931, I. Schur

Effective construction of polynomials over $\mathbb{Q}$ realising S_n and A_n for particular values of n.

- 1970, Y. Yamamoto

For every even integer n there are infinitely many polynomials of type $X^n + aX + b \in \mathbb{Z}[X]$ whose Galois group over $\mathbb{Q}$ is isomorphic to S_n.

Galois realisations of solvable groups

- 1954, I. R. Shafarevich

Any solvable group is Galois over any number field.

Strategy: Resolution of successive Galois embedding problems.

Shafarevich, I. R.: Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR. Ser. Mat.* 18 (1954), 525–578. *Amer. Math. Soc. Transl.* 4 (1960), 185–237.

- 1979, J. Neukirch

Simplified proof of Shafarevich's theorem for solvable groups of odd order.

Tools: Use of Galois cohomology

Neukirch, J.: On solvable number fields. *Invent. Math.* 53 (1979), no. 2, 135–164.

Galois realisations of S_n and A_n

- 1983, **E. Nart & N. Vila**

For every even integer $n > 2$ *there are infinitely many polynomials* $X^n + bX^2 + cX + d \in \mathbb{Z}[X]$ *whose Galois group over* $\mathbb{Q}$ *is isomorphic to* A_n.
For every odd integer $n > 3$ *there are infinitely many polynomials* $X^n + aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$ *whose Galois group over* $\mathbb{Q}$ *is isomorphic to* A_n.

Tools: Use of a Furtwängler criterion.

Remark. For the cases n even and $4 \nmid n$, explicit equations for A_n were not known before.

Nart, E.; Vila, N.: Equations with absolute Galois group isomorphic to A_n. *J. Number Theory* 16 (1983), no. 1, 6–13.

□ □ □

CHAPTER I

1987: San Francisco; MSRI, *Galois groups over* $\mathbf{Q}$

From September 1981 to July 1983

Galois embedding problems

K field; $\quad \overline{K}$ separable closure of K

$G_K = \mathrm{Gal}(\overline{K}|K)$ absolute Galois group; $\quad G$ finite group

$K \subseteq L \subseteq \overline{K}$ Galois extension, $L|_G K$

$\varphi : G_K \to \mathrm{Gal}(L|K) \simeq G$

Definition. Given a group extension $\tilde{G} = A \cdot G$, a solution of the Galois embedding problem

$$\tilde{G} \to G \simeq \mathrm{Gal}(L|K)$$

is a field $\tilde{L}$ such that $L \subseteq \tilde{L} \subseteq \overline{K}$ and the diagram

$$\begin{tikzcd} \mathrm{Gal}(\tilde{L}|K) \arrow[r, "\varphi"] \arrow[d, "\wr"] & \mathrm{Gal}(L|K) \arrow[d, "\wr"] \\ \tilde{G} \arrow[r] & G \end{tikzcd}$$

commutes, where φ is given by restriction.

The obstruction to embedding problems

Let $\varepsilon \in H^2(G, A)$ be the element defined by an exact sequence

$$1 \to A \to \widetilde{G} \to G \to 1$$

in which A is an abelian group.

Let $L|_G K$ be a Galois extension defined by a homomorphism

$$\rho : G_K \to \mathrm{Gal}(L|K) \simeq G.$$

Through the inflation map, we obtain an element

$$\rho^* \varepsilon \in H^2(G_K, A).$$

Theorem. **[Hoechsmann, 1968]** *The embedding problem* $\widetilde{G} \to G \simeq \mathrm{Gal}(L|K)$ *is solvable if and only if*

$$\rho^* \varepsilon = 0.$$

Central extensions

An extension $E = N \cdot G$ of a group G is said to be central if it is given by an exact sequence $1 \to N \to E \to G \to 1$ with $N \subseteq Z(E)$. Then N is an abelian group and the action of G in N is trivial.

A group G is said to be perfect if $[G, G] = G$. In particular, non-abelian simple groups are perfect.

Perfect groups admit universal central extensions $\widetilde{G} = A \cdot G$; they are central extensions such that for any central extension $E = N \cdot G$ there is a unique homomorphism $h : \widetilde{G} \to E$ making commutative the diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d] & \widetilde{G} \arrow[r, "\pi"] \arrow[d, "h"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N \arrow[r] & E \arrow[r] & G \arrow[r] & 1.
\end{tikzcd}$$

Galois realisations of central extensions of perfect groups

Lemma. **[Vila]** *Let $L|_G K$ be a Galois extension with G a perfect group. Let $\widetilde{G}$ be its universal central extension. If the embedding problem*

$$\widetilde{G} \to G \simeq \mathrm{Gal}(L|K)$$

admits a solution, then any embedding problem defined by a central extension $E = N \cdot G$ will be solvable.

Proof. (sketch) The proof makes use of an Ikeda's lemma [1960] on the existence of *proper* solutions.

Remark. The lemma motivated to consider the realisation of central extensions of simple groups as Galois groups. The easiest cases being those of A_n, $n \neq 6, 7$:

$$1 \to C_2 \to \widetilde{A}_n \to A_n \to 1.$$

Theorem. [Nart & Vila] *Let K be a number field and R its ring of integers. Let $F(X) = X^n + aX^2 + bX + c \in R[X]$, $ac \neq 0$, be a polynomial satisfying the following conditions:*

(i) *$F(X)$ is irreducible and primitive.*

(ii) $b^2(n-1)^2 = 4acn(n-2)$.

(iii) *$(-1)^{n/2}c$ is a square.*

(iv) *If $u = -b(n-1)/2(n-2)a$, there exists a prime ideal $\mathfrak{p}$ of R such that*

$$c(n-1) \notin \mathfrak{p}, \quad F(u) \in \mathfrak{p}, \quad \text{and } 3 \nmid v_{\mathfrak{p}}(F(u)).$$

Then, if n is even and $n > 2$, the Galois group of $F(X)$ over K is isomorphic to A_n.

The local obstruction at infinity for the Nart-Vila equations

Proposition. **[Vila]** *Let $f(X) \in \mathbf{Q}[X]$ be an irreducible polynomial of degree n whose Galois group is isomorphic to A_n and let r_1 be the number of its real roots. Then*

1. $n \equiv r_1 \pmod 4$.

2. *The local obstruction at ∞ of the embedding problem $\tilde{A}_n \to A_n \simeq$* $\mathrm{Gal}_{\mathbf{Q}}(\mathrm{f})$ *is zero if and only if*

$$n \equiv r_1 \pmod 8.$$

Corollary. *The obstruction at ∞ of Nart-Vila equations for A_n is trivial if and only if $n \equiv 0$ or $2 \pmod 8$.*

Serre's formula

Suppose that $n \neq 6, 7$. The exact sequence $1 \to C_2 \to \widetilde{A}_n \to A_n \to 1$ defines an element $a_n \in H^2(A_n, C_2)$. For any $G \subseteq A_n$, let $\varepsilon \in H^2(G, C_2)$ be the element obtained by restriction

$$\mathrm{res} : H^2(A_n, C_2) \to H^2(G, C_2), \quad a_n \mapsto \varepsilon,$$

and denote by $\widetilde{G}$ the corresponding extension of groups. Let $E|K$ be an extension of degree n, $L|_G K$ its Galois closure and $\rho : G_K \to \mathrm{Gal}(L|K) \simeq G$. Through the inflation map, we obtain now an element

$$\rho^*\varepsilon \in H^2(G_K, C_2) \simeq \mathrm{Br}_2(K).$$

Theorem. [Serre, 1984] *Let Q_E be the n-ary quadratic form*

$$X \to \mathrm{Tr}_{E|K}(X^2).$$

Then the obstruction to the embedding problem $\widetilde{G} \to G \simeq \mathrm{Gal}(L|K)$ is given by

$$\rho^*\varepsilon = w(Q_E),$$

where w denotes the Hasse-Witt invariant of Q_E.

First results

Theorem. **[Vila]** *Suppose that $n > 6$ is an even integer. Let L be the splitting field over K of a polynomial $F(X)$, as above. Then the embedding problem $\widetilde{A}_n \to \mathrm{Gal}(L|K) \simeq A_n$ is solvable if and only if*

$$\begin{array}{ll} n \equiv 0 \pmod 8, & \text{or} \\ n \equiv 2 \pmod 8 & \textit{and } n \textit{ is a sum of two squares.} \end{array}$$

Corollary. *Any central extension of A_n, $n > 6$, occurs as Galois group over $\mathbf{Q}$ if $n \equiv 0 \pmod 8$ or $n \equiv 2 \pmod 8$ and n is a sum of two squares.*

In these cases:

$$\mathrm{Tr}_{E|K}(X^2) \sim \begin{cases} nX_1^2 - (n-2)aX_2^2 + X_3X_4 + \cdots + X_{n-1}X_n, & \text{if } n \text{ is even,} \\ \\ nX_1^2 + X_2^2 + X_3X_4 + \cdots + X_{n-1}X_n, & \text{if } n \text{ is odd.} \end{cases}$$

How to achieve more values of n

1. Find new irreducible polynomials $f(X) \in \mathbf{Q}[X]$, of degree n, with Galois group isomorphic to A_n and with a "computable" trace form and good behaviour at infinity.

2. Compute $w(\mathrm{Tr}_{E|\mathbf{Q}})$, where $E = \mathbf{Q}(\theta)$, θ a root of $f(X)$.

3. Impose conditions on $f(X)$ in order that $w(\mathrm{Tr}_{E|\mathbf{Q}}) = 1$.

Remark. (1) was solved with techniques used by Hurwitz and worked out by Matzat. Afterwards, they gave rise to the so called Thompson *rigidity methods*.

The starting point was Riemann existence theorem.

Hurwitz presentations

Definition. Let G be a finite group and $t_i \in G$, $1 \leq i \leq r$. We say that $(t_1, \ldots, t_r)$ is a *Hurwitz r-presentation* of G if $\{t_1, \ldots, t_r\}$ generate G and $t_1 \cdots t_r = 1$.

$H_r(G)$ set of Hurwitz r-presentations

Given $(t_1, \ldots, t_r) \in H_r(G)$, let $H(t_1, \ldots, t_r)$ be the set of $(s_1, \ldots, s_r) \in H_r(G)$ such that the subgroups $\langle s_i \rangle$ and $\langle t_i \rangle$ are conjugate in G.

$h(t_1, \ldots, t_r) := \# H(t_1, \ldots, t_r)/\mathrm{Aut}(G)$ Hurwitz number

Definition. A finite group is *complete* if its center is trivial and any automorphism is inner. Ex.: S_n is a complete group.

Proposition. *Any finite complete group having a Hurwitz presentation with Hurwitz number equal to* 1 *is Galois over* $\mathbf{Q}(T)$.

New S_n and A_n-equations over $\mathbf{Q}(T)$

Theorem. [Vila] *Let n, k be positive integers,* $\gcd(n,k) = 1$, $k \leq n$.

(a) *Let* $s_1 = (n, n-1, \ldots, 3, 2, 1)$, $s_2 = (1, 2, \ldots, k)(k+1, \ldots, n)$, $s_3 = (1, k+1)$. *Then* $(s_1, s_2, s_3) \in H_3(S_n)$ *and* $h(s_1, s_2, s_3) = 1$.

(b) *For* $n \geq 5$, *the polynomial* $G_k(X,T) = X^{n-k}\left(X - \frac{n}{n-k}\right)^k - \left(\frac{-k}{n-k}\right)^k T$ *has Galois group over* $\mathbf{Q}(T)$ *isomorphic to* S_n.

(c) *For* $n \geq 5$ *and* $k \leq n/2$, *the polynomial*

$$F_{n,k}(X,T) = \begin{cases} X^n - A(nX - k(n-k))^k, & \text{if } n \text{ is odd,} \\ X^n + k^{n-2k}B^{n-k-1}(nX + Bk(n-k))^k, & \text{if } n \text{ is even,} \end{cases}$$

where $A = k^{n-2k}(1 - (-1)^{(n-1)/2}nT^2)$, $B = (-1)^{n/2}k(n-k)T^2 + 1$ *has Galois group over* $\mathbf{Q}(T)$, *and over* $\mathbf{Q}(i,T)$, *isomorphic to* A_n.

The computation of the Hasse-Witt invariant

$K = \mathbf{Q}(T)$ or $K = \mathbf{Q}(i,T)$; $n \neq 6, 7$; $k \leq (n+1)/3$ odd
$F_{n,k}(X,T) = X^n + A(bX+c)^k$; $E_{n,k} = K(\theta)$; $L_{n,k}|K$ splitting field

Theorem. [Vila]

(a) $\mathrm{Tr}_{E_{n,k}|K}(X^2) \simeq$

$$\begin{cases} nX_1^2 + (-1)^{(n-2)/2}X_2^2 + X_3X_4 + \cdots + X_{n-1}X_n, & \text{if } n \text{ is even,} \\ nX_1^2 + nCX_2^2 + (-1)^{(n+1)/2}CX_3^2 + X_4X_5 + \cdots + X_{n-1}X_n, & \text{if } n \text{ is odd,} \end{cases}$$

where $C = k(n-k)(1-(-1)^{(n-1)/2}nT^2)$.

(b) $w(E_{n,k}|\mathbf{Q}) =$

$$\begin{cases} (n, (-1)^{n/2}) \otimes (-1,-1)^{n(n-2)/8}, & \text{if } n \text{ is even,} \\ (-(n-k)k, (-1)^{(n-1)/2n}) \otimes (-1,-1)^{(n+1)(n-1)/8}, & \text{if } n \text{ is odd.} \end{cases}$$

(c) $w(E_{n,k}|\mathbf{Q}(i)) = \begin{cases} 1, & \textit{if } n \textit{ is even,} \\ (-(n-k), n) = 1, & \textit{if } n \textit{ is odd and } k \textit{ is a square.} \end{cases}$

Galois realisations over $\mathbf{Q}(i)$

Corollary. *Let $L_{n,k}$ be the splitting field of the polynomial $F_{n,k}(X,T)$ over $\mathbf{Q}(i,T)$. Then the embedding problem*

$$\widetilde{A}_n \to A_n \simeq \mathrm{Gal}(L_{n,k}|\mathbf{Q}(i,T))$$

is solvable for any even value of n, or for any odd value of n and k a square ($n \neq 6, 7$).

Corollary. *Any central extension of the alternating group A_n occurs infinitely often as Galois group over $\mathbf{Q}(i)$, for any value of $n \neq 6, 7$.*

Galois realisations over $\mathbb{Q}$

Definition. A positive integer n, $n \not\equiv 0 \pmod 4$ or $n \not\equiv 7 \pmod 8$, satisfies the *property* (N) if there exists a decomposition of n into a sum of three squares $n = x^2 + y^2 + z^2$ such that $\gcd(x, n) = 1$ and $x^2 \leq (n+1)/3$.

Theorem. **[Vila]** *The embedding problem $\widetilde{A}_n \to A_n \simeq \mathrm{Gal}(L_{n,k}|\mathbf{Q}(T))$ is solvable for the following values n and k:*

(a) $n \equiv 0 \pmod 8$, $k > 0$,
(b) $n \equiv 1 \pmod 8$, k *a square,*
(c) $n \equiv 2 \pmod 8$, *and n being a sum of two squares,* $k > 0$,
(d) $n \equiv 3 \pmod 8$, n *satisfying* (N), *and* $k = x^2$.
If $n \equiv 4, 5, 6, 7 \pmod 8$, *the previous embedding problem is not solvable for any value of* k.

Corollary. *Any central extension of A_n occurs infinitely often as Galois group over $\mathbf{Q}$ if*
$n \equiv 0, 1 \pmod 8$,
$n \equiv 2 \pmod 8$, *and n is a sum of two squares,*
$n \equiv 3 \pmod 8$, *and n satisfies* (N).

Remarks

• Vila presented her results at the 1983 *Journées Arithmétiques*, held at Noordwijkerhout.

• The above articles caught the attention of [Conner; Perlis, 1984], [Serre, 1984; 1988; 1989; 1992], [Schacher; Sonn, 1986], [Feit, 1986; 1989], [Matzat, 1987; 1988; 1991], [Sonn, 1988; 1989; 1991], [Conner; Yui, 1988], [Karpilovski, 1989], [Mestre, 1990; 1994], [Turull, 1992], [Volklein, 1992], [E. Bayer, 1994], [Swallow, 1994], and [Epkenhans, 1994; 1997].

• Mestre [1990] succeeded in proving that $\widetilde{A}_n$ occurs as Galois group over $\mathbf{Q}(T)$ for any value of n. For that, Mestre combined some of the above techniques with ideas due to Henniart, Oesterlé, and Serre.

A question of Serre

If $G = \mathrm{Gal}(L|K) \subseteq A_n$, $w(Q_E) = 0$, and $\widetilde{G} = \mathrm{Gal}(\widetilde{L}|K) \subseteq \widetilde{A}_n$, how can $\widetilde{L} = L(\sqrt{u})$ be effectively constructed?

$\square\ \square\ \square$

CHAPTER II

1991: UB

From May 1983 to July 1985

The property (N)

Definition. A positive integer n, $n \not\equiv 0 \pmod 4$ or $n \not\equiv 7 \pmod 8$, satisfies the property (N) if there exists a decomposition of n into a sum of three squares $n = x^2 + y^2 + z^2$ such that $\gcd(x, n) = 1$ and $x^2 \le (n+1)/3$.

- Is this property always satisfied?

il se peut que ce soit très difficile Serre, 1983

- P. Llorente checked that any positive integer $n \le 600\,000$, $n \equiv 3 \pmod 8$, satisfies the property (N).
- Gauss, 1800: n admits a primitive representation as a sum of three squares if and only if $n \not\equiv 0, 4, 7 \pmod 8$.
- Catalan. If $n = 3^u$, the three summands can be chosen to be coprime to 3.

- Arenas: Constructed special families of integers fulfilling the property (N).

The level of an integer: first results

Definition. Given a positive integer $n \neq 4^a(8b+7)$, the level $\ell(n)$ is the maximum value ℓ such that n can be written as a sum of three squares, $n = x_1^2 + x_2^2 + x_3^2$, with ℓ summands coprime to n.

Corollary. *If $n \equiv 3 \pmod 8$ is a positive integer such that $\ell(n) = 3$, then any central extension of the alternating group A_n is Galois over $\mathbf{Q}$.*

Theorem. [Arenas] *Let $n = mt > 1$ be an integer, with $m = 2^{\alpha_0} p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\alpha_i \geq 0$, $p_i \equiv 1 \pmod 4$, $t = q_1^{\beta_1} \dots q_s^{\beta_s}$, $q_j \equiv 3 \pmod 4$, $\beta_j \geq 0$.*

(a) *If $n \equiv 0 \pmod 2$ or $n \equiv 0 \pmod 5$, then $\ell(n) \leq 2$.*
(b) *If $n = m$, $\alpha_0 = 0$, then $\ell(n) \geq 2$.*
(c) *If $n = 2^{\alpha_0} 5^{\alpha_1} p_1^{\alpha_2} \dots p_r^{\alpha_r}$, $\alpha_0 + \alpha_1 > 0$, $\alpha_0 \leq 1$, then $\ell(n) = 2$.*
(d) *If $n = m$, $\alpha_0 = 0$, and n is an* Euler numerus idoneus, *then $\ell(n) = 2$.*
(e) *If $n = t$ and $n \not\equiv 7 \pmod 8$, then $\ell(n) = 3$.*

A strategy for determining the level

From all the representations of n discard those that are not good!

Schinzel/Erdös, 1983

1. Compare numbers of representations of an integer n by different *ad hoc* ternary quadratic forms.

2. Since the number of representations $r(n, f)$ cannot be determined in general, approximate this number by an average value $r(n, \text{gen} f)$.

3. Estimate the error $r(n, f) - r(n, \text{gen} f)$.

Some notation

f positive definite ternary quadratic form with integer coefficients

n positive integer

$$r(n, f) = \#\{(x_i) \in \mathbf{Z}^3 : f(x_1, x_2, x_3) = n\}$$

$$r^*(n, f) = \#\{(x_i) \in \mathbf{Z}^3 : f(x_1, x_2, x_3) = n, \gcd(x_i) = 1\}$$

$$r_m(n, f) = \#\{(x_i) \in \mathbf{Z}^3 : f(x_1, x_2, x_3) \equiv n \pmod{m}\}$$

Möbius function:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \text{ is not square-free}, \\ (-1)^r, & \text{if } n = p_1 \dots p_r \text{ is a product of distinct primes.} \end{cases}$$

Sums of three squares

$I_3 = X_1^2 + X_2^2 + X_3^2$

$d_i(n)$ number of representations of n by I_3 with exactly i components not coprime to n

$$g_1(n) := \frac{d_3(n)}{r(n, I_3)}$$

$$g_2(n) := \frac{d_2(n) + d_3(n)}{r(n, I_3)}$$

$$g_3(n) := \frac{d_1(n) + d_2(n) + d_3(n)}{r(n, I_3)}$$

Lemma. **[Arenas]** *Let n be an odd positive integer, $n \not\equiv 7 \pmod 8$, or an even positive integer, $n \not\equiv 0, 4 \pmod 8$. Then, for any $1 \le i \le 3$,*

$$g_i(n) < 1 \iff \ell(n, 3) \ge i.$$

Auxiliary alternating sums

Theorem. [Arenas] *For $1 \le i \le 3$, define*

$$s_i(n) = \rho_i \sum (-1)^i \mu(a_1)\mu(a_2)\mu(a_3) r(n, \langle a_1^2, a_2^2, a_3^2 \rangle),$$

where $\rho_i = 3 - 2[i/3]$ and the sum runs over those square-free positive integers a_j such that $1 < a_j | n$, for $j \le i$, and $a_j = 1$, for $j > i$. Then
(a) $s_3(n) = d_3(n)$,
(b) $s_2(n) = d_2(n) + 3d_3(n)$,
(c) $s_3(n) = d_1(n) + 2d_2(n) + 3d_3(n)$.

- $s_i(n)$ counts the number of representations of n of level $\le (3 - i)$.

Corollary. *Let $n \not\equiv 0, 4, 7 \pmod 8$. Then*

(a) $g_1(n) = \dfrac{s_3(n)}{r(n, I_3)}$,

(b) $g_2(n) = \dfrac{s_2(n) - 2s_3(n)}{r(n, I_3)}$,

(c) $g_3(n) = \dfrac{s_1(n) - s_2(n) + s_3(n)}{r(n, I_3)}$.

Genus theory

f definite integral quadratic integral form, $\text{gen}(f) = \{[f_1], \dots, [f_h]\}$

$$\text{gen} f = \text{gen} g \iff f \overset{\mathbf{Z}_p}{\simeq} g, \text{ for all } p \in P \cup \{\infty\}$$

$$r(n, \text{gen}(f)) := \left(\sum_{i=1}^{h} \frac{1}{o(f_i)} \right)^{-1} \left(\sum_{i=1}^{h} \frac{r(n, f_i)}{o(f_i)} \right)$$

Theorem. [Siegel]

$$r(n, \text{gen}(f)) = \partial_\infty(n, f) \prod_p \partial_p(n, f),$$

where

$$\partial_p(n, f) = \begin{cases} \dfrac{2\pi n^{1/2}}{(\det f)^{1/2}}, & \textit{if } p = \infty, \\[2ex] \dfrac{r_{p^{2\alpha}}(n, f)}{p^{2\alpha}}, & \textit{for all } \alpha \geq 2\beta + 1,\ p^\beta \| 2n,\ \textit{if } p \textit{ is prime.} \end{cases}$$

The average alternating sums attached to n

$f = \langle a_1^2, a_2^2, a_3^2 \rangle$, $a_i | n$, a_i square-free

$d_{i,j} := \mathrm{gcd}(a_i, a_j)$, $\quad d_{123} := \mathrm{gcd}(a_1, a_2, a_3)$, $\quad d := d_{123}^{-2} d_{12} d_{13} d_{23}$

$$r(n, \langle a_1, a_2, a_3 \rangle) = r(nd^{-2}, \langle b_1, b_2, b_3 \rangle), \text{ where } b_i = d_{ij}^{-1} d_{ik}^{-1} d_{123} a_i$$

$$S_i(n) := \rho_i \sum (-1)^i \mu(a_1)\mu(a_2)\mu(a_3) r(nd^{-2}, \mathrm{gen}\langle b_1^2, b_2^2, b_3^2 \rangle),$$

$$S_i'(n) := \frac{S_i(n)}{r(n, I_3)}, \text{ for } 1 \le i \le 3$$

The main term in the determination of the level of n

$G_1(n) := S_3'(n)$
$G_2(n) := S_2'(n) - 2S_3'(n)$
$G_3(n) := S_1'(n) - S_2'(n) + S_3'(n)$

Computation of the main term $G_i(n)$, square-free case

$n = mt$ square-free positive integer
$m = 2^a p_1 \dots p_r$, $p_i \equiv 1 \pmod 4$, $0 \le a \le 1$
$t = q_1 \dots q_s$, $q_j \equiv 3 \pmod 4$

Theorem. [Arenas] *Let $n = mt$ be square-free, $n \not\equiv 7 \pmod 8$. Then*

(a) *If n is odd,*
$G_1(n) = 1 - 3P_1(m) + 3P_2(m) - P_3(m)$,
$G_2(n) = 1 - 3P_2(m) + 2P_3(m)$,
$G_3(n) = 1 - P_3(m)$.

(b) *If n is even,*
$G_1(n) = 1 - 2P_1(m) + P_2(m)$,
$G_2(n) = 1 - P_2(m)$,
$G_3(n) = 1$,

where $P_j(m) = \prod_{i=1}^{r}(1 - 2j(1 + p_i)^{-1})$, *for* $1 \le j \le 3$.

Computation of the main term $G_i(n)$, non square-free case

Definition. Let $n \not\equiv 0, 4 \pmod{p}$ be a positive integer and let p ba a prime such that $v_p(n) = \alpha > 0$. Writing $n = mp^\alpha$, let

$$\frac{\partial_p(mp^\alpha d^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)}{p\partial_p(mp^\alpha, I_3)} =: \begin{cases} \partial'_p(m,\alpha), & \text{if } p|b_i \text{ for exactly one } i, \\ \partial'_{p^2}(m,\alpha), & \text{if } p|d. \end{cases}$$

Theorem. **[Arenas]** *Let $n = mp^\alpha$, $\alpha = v_p(n) > 0$. We assume that α is even if not all the exponents in the factorization of n are odd. $n \not\equiv 0 \pmod{4}$. Then*

$$\begin{aligned}
G_1(n) &= G_1(m) + \partial'_p(m,\alpha)(G_2(m) - G_1(m)) + \partial'_{p^2}(m,\alpha)(1 - G_2(m)), \\
G_2(n) &= G_2(m) + 2\partial'_p(m,\alpha)(G_3(m) - G_2(m)) + \\
&\qquad + \partial'_{p^2}(m,\alpha)(1 + G_2(m) - 2G_3(m)), \\
G_3(n) &= G_3(m) + (3\partial'_p(m,\alpha) - \partial'_{p^2}(m,\alpha))(1 - G_3(m)).
\end{aligned}$$

Bound of the main term $G_i(n)$

Lemma. **[Arenas]** *Let* $n = mp^\alpha \not\equiv 0, 4 \pmod 8$ *be a positive integer. If* $\alpha > 0$ *and* $p \neq 2$, *then*

(a) $0 \leq \partial'_p(m,\alpha) < 1/2$,
(b) $0 \leq \partial'_{p^2}(m,\alpha) < p^{-1}$,
(c) $0 \leq 3\partial'_p(m,\alpha) - 2\partial'_{p^2}(m,\alpha) < 7/13$, *if* $p \neq 5$.
(d) $3\partial'_5(m,\alpha) - 2\partial'_{5^2}(m,\alpha) = 1$.
(e) $0 \leq 2\partial'_p(m,\alpha) - \partial'_{p^2}(m,\alpha) < 4/5$.

Theorem. **[Arenas]** *Let* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *be a positive integer with* $4 \nmid n$. *Then there exist constants* $c_i = c_i(p_1 \cdots p_k)$ *such that*

$$G_i(n) < c_i(p_1 \dots p_k) < 1,$$

for $i = 1, 2, 3$ *if* $\gcd(n, 10) = 1$; *and* $i = 1, 2$ *if* $\gcd(n, 10) \neq 1$. *In the latter case, we have* $G_3(n) = 1$.

The average level

Definition.

$$\ell_a(n,3) = \begin{cases} -1, & \text{if } n = 4^a(8b+7), \\ 0, & \text{if } 4|n \text{ and } n \neq 4^a(8b+7), \\ 2, & \text{if } \gcd(n,10) \neq 1, \\ 3, & \text{if } \gcd(n,10) = 1. \end{cases}$$

Remark.

For any $n \leq 10^5$ is

$$\ell(n,3) = \ell_a(n,3),$$

except for 24 cases in which is $\ell(n,3) = 1$ and $\ell_a(n,3) = 2$
and for
$n = 13, 37, 403, 793$ for which is $\ell(n,3) = 2$ and $\ell_a(n,3) = 3$.

- To bound the error term $\rightsquigarrow$ use modular forms!

Theorem. **[Siegel, Shimura]** *Let* (V, B, f) *be a quadratic space of dimension* $k \geq 3$. *Let*

$L = \langle e_1, \ldots, e_k \rangle$ *be a* $\mathbf{Z}$*-lattice in* V,

$L^{\#} := \{x \in V : B(x, L) \subseteq \mathbf{Z}\}$ *its dual lattice,*

$e(z) := \exp(2\pi i z)$.

Define $\theta(L, z) = \theta(f, z) = \sum_{x \in L} e(f(x)z)$, $z \in \mathcal{H}$, $\det L = \det(B(e_i, e_j))$,

$$\chi(m) = \begin{cases} \left(\frac{2 \det L}{m}\right), & \text{if } k \text{ is odd,} \\ \\ \left(\frac{(-1)^{d/2} \det L}{m}\right), & \text{if } k \text{ is even.} \end{cases}$$

Suppose that $f(L)\mathbf{Z} = \mathbf{Z}$ *and that* $f(L^{\#})\mathbf{Z} = N^{-1}\mathbf{Z}$. *Then*

(a) $\theta(L, z) \in \mathcal{M}(\Gamma_0(N), k/2, \chi)$.

(b) $\theta(L, z) - \theta(\mathrm{gen} L, z) \in \mathcal{S}(\Gamma_0(N), k/2, \chi)$.

The error term $g_i(n) - G_i(n)$ in the determination of the level

$$\theta(f, z) := \sum_{n=0}^{\infty} r(n, f) e(nz) \qquad z \in \mathcal{H}$$

$$\theta(\mathrm{gen} f, z) := \sum_{n=0}^{\infty} r(n, \mathrm{gen} f) e(nz)$$

$$\theta(z) = \theta(I_1, z) = 1 + 2 \sum_{n=0}^{\infty} e(n^2 z)$$ **Jacobi** theta function

$$\mathcal{M}(\Gamma, k) = \mathcal{E}(\Gamma, k) \oplus \mathcal{S}(\Gamma, k)$$

$$\theta(I_3, z) = \theta^3(z) \in \mathcal{M}(\Gamma_0(4), 3/2)$$

$$\theta(\langle b_1^2, b_2^2, b_3^2 \rangle, z) \in \mathcal{M}(\Gamma_0(N), 3/2) \qquad N = 4 b_1^2 b_2^2 b_3^2$$

$$\theta(\mathrm{gen}\langle b_1^2, b_2^2, b_3^2 \rangle, z) \in \mathcal{E}(\Gamma_0(N), 3/2)$$

$$\theta(\langle b_1^2, b_2^2, b_3^2 \rangle, z) - \theta(\mathrm{gen}\langle b_1^2, b_2^2, b_3^2 \rangle, z) \in \mathcal{S}(\Gamma_0(N), 3/2)$$

Spinor genus of a quadratic space

$(V,B)=(V,f)$ K-quadratic space, char$(K)\neq 2$

$s_v : x \mapsto x - 2v\dfrac{B(v,x)}{B(v,v)}$ reflection orthogonal to v

$$\begin{array}{rccl} \text{Spn}: & O(V) & \longrightarrow & K^*/(K^*)^2 \\ & u = s_{v_1}\dots s_{v_t} & \longrightarrow & f(v_1)\dots f(v_t) \end{array}$$ spinor norm

$$1 \to SO_1(V) \to SO(V) \overset{\text{Spn}}{\to} K^*/(K^*)^2$$

$$1 \to C_2 \to \text{Spn}(V) \to SO_1(V) \to 1$$

Definition. [Eichler] Two $\mathbf{Z}$-lattices L and M in a $\mathbf{Q}$-quadratic space V are said to be spinor equivalent if there exists a transformation $u \in SO(V)$ and, for each p, a transformation $v_p \in SO_1(V)$ such that

$$M_p = uv_pL_p.$$

- Properly equivalent lattices are in the same spinor genus, and lattices in the same spinor genus are in the same genus.

Theta series of ternary quadratic forms

$S(\Gamma_0(N), 3/2, \chi) = U \oplus U^{\perp}, \quad U = \oplus U(a), \quad 4s^2a|N,\ a$ square-free

U subspace spanned by certain Shimura thetaseries

Theorem. [Schulze-Pillot, 1984] *Let L be a lattice of dimension 3, and level N. Let $n_0|N$ be a square-free integer. Then*

(a) $\theta(L, z) - \theta(\mathrm{spn} L) \in U^{\perp}$.

(b) *If* $g(z) = \sum_{n=1}^{\infty} a(n)e(nz) \in U(n_0)^{\perp}$, *then*

$$a(n_0 s^2) = O(s^{1/2+\varepsilon}),$$

the O-constant depending on ε, n_0 and g.

Proof. (sketch) Shimura's lifting from modular forms of weight $3/2$ to modular forms of weight 2 maps $U(n_0)^{\perp}$ to $S(\Gamma_0(N/2), 2, \chi^2)$. Then apply Eichler proof of the Ramanujan-Petersson conjecture.

Bound of the error term $g_i(n) - G_i(n)$, n square-free

$n = mt$ square-free positive integer

$m = 2^a p_1 \ldots p_r$, $p_i \equiv 1 \pmod 4$, $0 \le a \le 1$

$t = q_1 \ldots q_s$, $q_j \equiv 3 \pmod 4$

Theorem. **[Arenas]** *Let $n = mt$ be a square-free positive integer and $f = \langle a_1^2, a_2^2, a_3^2 \rangle$, $a_i | m$, $\gcd(a_i, a_j) = 1$ for $i \neq j$. Then*

(a) $\mathrm{gen} f = \mathrm{spn} f$.

(b) $r(n, f) - r(n, \mathrm{gen} f) = O_{\varepsilon,m,f}(s^{1/4+\varepsilon})$, *for any* $\varepsilon > 0$.

(c) *If* $n \not\equiv 7 \pmod 8$, *then, for any* $\varepsilon > 0$ *is*

$$g_i(n) - G_i(n) = O_{\varepsilon,m}(s^{-1/4+\varepsilon}),$$

for $1 \le i \le 3$.

The determination of the level, square-free case

Theorem. [Arenas] *Let Let $n = mt$ be a square-free positive, $n \not\equiv 7 \pmod 8$. There exists a constant $c(m)$ such that*

$$\ell(n) = \begin{cases} 2, & \text{if } \gcd(n, 10) \neq 1, \\ 3, & \text{if } \gcd(n, 10) = 1. \end{cases}$$

for any $t > c(m)$.

The constants are non-trivial in general:

m	$c(m) \geq$
13	403
10	27190
37	37
$13 \cdot 61$	793

Application to the Galois embedding problem

Corollary. *Let $n = mt$ be a square-free positive integer, $n \equiv 3 \pmod 8$, $n \not\equiv 0 \pmod 5$. Then there exists a constant $c(m)$ such that any central extension of the alternating group A_n occurs infinitely often as Galois group over $\mathbf{Q}$, for any $n > c(m)$.*

Bound of the error term $g_i(n) - G_i(n)$, general case

$n = n_0 s^2$ be a positive integer, $n \not\equiv 0, 4, 7 \pmod 8$,

n_0 its square-free part

$m_0 = \mathrm{rad}(n)$

Theorem. **[Arenas]** *Let* $f = \langle b_1^2, b_2^2, b_3^2 \rangle$ *be a quadratic form such that* $b_i | n$, $\gcd(b_i, b_j) = 1$, *for* $i \neq j$, b_i *square-free. Then*

(a) $\mathrm{gen} f = \mathrm{spn} f$.

(b) $r(n, f) - r(n, \mathrm{gen} f) = O_{\varepsilon, n_0, f}(s^{1/2+\varepsilon})$, *for any* $\varepsilon > 0$.

(c) *For any* $\varepsilon > 0$ *and* $1 \leq i \leq 3$, *is*

$$g_i(n) - G_i(n) = O_{\varepsilon, m_0}(s^{-1/2+\varepsilon}).$$

The determination of the level, square-free case

Theorem. **[Arenas]** *Let* $n \not\equiv 0, 4, 7 \pmod 8$ *and* $m_0 = \mathrm{rad}(n)$. *There exists a constant* $c(m_0)$ *such that if* $n > c(m_0)$, *then*

$$\ell(n) = \begin{cases} 2, & \text{if } \gcd(n, 10) \neq 1, \\ 3, & \text{if } \gcd(n, 10) = 1. \end{cases}$$

The constants are trivial for $n \leq 10^5$, except for:

m_0	$c(m_0) \geq$
30	90
390	1170
570	1710
1230	3690
6630	19890

Application to the Galois embedding problem

Corollary. *Let* $n \equiv 3 \pmod 8$, $n \not\equiv 0 \pmod 5$, *be a positive integer. Let* $m_0 = \mathrm{rad}(n)$. *Then there exists a constant* $c(m_0)$ *such that any central extension of the alternating group* A_n *occurs infinitely often as Galois group over* $\mathbf{Q}$, *for any* $n > c(m_0)$.

□ □ □

CHAPTER III

1995: BCN *Journées Arithmétiques*

From September 1984 to February 1988

First explicit solutions to some Galois embedding problems

$$1 \to C_2 \to H_8 \to C_2 \times C_2 \to 1 \qquad \text{the quaternion group}$$

Theorem. [Dedekind] *Let* $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. *The embedding problem* $H_8 \to C_2 \times C_2 \simeq \mathrm{Gal}(L|\mathbf{Q})$ *is solvable by the field*

$$\widetilde{L} = \mathbf{Q}\left(\sqrt{(2+\sqrt{2})(3+\sqrt{6})}\right).$$

Theorem. [Witt, 1936] *Let* K *be a field of characteristic* $\neq 2$. *A biquadratic extension* $L = K(\sqrt{a}, \sqrt{b}, \sqrt{c})$, $abc = 1$, *can be embedded in a Galois extension* $\widetilde{L}|K$ *with Galois group* H_8 *if and only if the quadratic forms*

$$aX_1^2 + bX_2^2 + cX_3^2, \quad Y_1^2 + Y_2^2 + Y_3^2$$

are K*-equivalent.*
If the matrix $P = (p_{ij}) \in \mathrm{SL}(2, K)$ *yields the required isomorphism, then all the fields* $\widetilde{L}$ *solving the embedding problem are given by*

$$\widetilde{L} = \mathbf{Q}\left(\sqrt{r(1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{c}}\right),$$

where r *runs through* K^*.

Clifford algebras

$$V \simeq K^n, \quad Q \text{ a quadratic form}, \quad T(V) \text{ tensor algebra}$$

$I(Q) = \langle v \otimes v - Q(v)1 \rangle_{v \in V} \subseteq T(V)$ two sided ideal

$$\mathsf{Cl}(Q) := T(V)/I(Q)$$

$\alpha : \mathsf{Cl}(Q) \circlearrowleft,\ \alpha(v) := -v,\ v \in V,$ principal automorphism

$$\mathsf{Cl}(Q) = \mathsf{Cl}^0(Q) \oplus \mathsf{Cl}^1(Q)$$

$\beta : \mathsf{Cl}(Q) \circlearrowleft,\ \beta(v_1 \dots v_k) = v_k \dots v_1$ principal antiautomorphism

$N(x) := \beta(x)x, \quad x \in \mathsf{Cl}(V, Q)$ spinor norm

$\Gamma^+(Q) = \{x \in \mathsf{Cl}^0(Q)^* : xVx^{-1} = V\}$ special Clifford group

$1 \to \Gamma_0^+(Q) \to \Gamma^+(Q) \xrightarrow{N} K^*$ reduced Clifford group

$1 \to C_2 \to \Gamma_0^+(Q) \xrightarrow{\varphi} \mathsf{SO}(Q)$ where $\varphi(x)(v) := xvx^{-1}$

Spinor construction of central extensions

$V = \langle e_1, \ldots . e_n \rangle_K$, I_n standard form
$\mathsf{Cl}(n,K)$: $e_i^2 = 1$, $e_ie_j = -e_je_i$, $i \neq j$

$n \geq 4$, $\qquad A_n \subseteq \mathsf{SO}(n,K)$, $s \mapsto p_s$, $p_s(e_i) = e_{s(i)}$

$s = (i,k)(j,\ell) \in A_n$, $\#\{i,j,k,l\} = 4$, $x_s = \dfrac{1}{2}(e_i - e_j)(e_k - e_\ell) \in \mathsf{Cl}(n,K)$

$$N(x_s) = 1, \quad x_s^2 = -1$$

$x_s \in \varphi^{-1}(A_n) \subseteq \Gamma_0^+(n,K)$, are elements of order 4.

$\widetilde{A}_n := \varphi^{-1}(A_n)$ is the unique non-trivial double cover of A_n.

$$\begin{tikzcd}
1 \arrow[r] & C_2 \arrow[r] \arrow[d, "\wr"] & \widetilde{G} \arrow[r] \arrow[d, hook] & G \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & C_2 \arrow[r] \arrow[d, "\wr"] & \widetilde{A}_n \arrow[r] \arrow[d] & A_n \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C_2 \arrow[r] & \Gamma_0^+(n,K) \arrow[r, "\varphi"] & \mathsf{SO}(n,K) &
\end{tikzcd}$$

The Clifford algebra of the trace form

$K \subseteq E \subseteq \overline{K}$, $[E:K]=n$, $L|_G K$ its splitting field

$Q(E) := \mathrm{Tr}_{E|K}(X^2)$, $d(E) := \mathrm{disc}(\mathrm{Tr}_{E|K}(X^2))$, $w(E) := w(\mathrm{Tr}_{E|K}(X^2))$

$\Phi = \mathrm{Hom}_K(E, \overline{K})$, G acts on Φ; $G \subseteq A_n \Leftrightarrow d(E) = 1 \in K^*/(K^*)^2$

Theorem. [Springer 1959, Serre 1982, Crespo]

(a) *The L-quadratic spaces (L^n, I_n) and $(L \otimes_K E, Q(E))$ are isomorphic. Thus, there exists an isomorphism of Clifford algebras*

$$f : \mathrm{Cl}(n, L) \xrightarrow{\sim} \mathrm{Cl}(L \otimes_K E, Q(E))$$

such that $f(L^n) = L \otimes_K E$.

(b) *If $d(E)$ and $w(E)$ are trivial, then there exists a K-algebra isomorphism $g : \mathrm{Cl}(n, K) \xrightarrow{\sim} \mathrm{Cl}(Q(E))$ such that*

$$g(\mathrm{Cl}^0(n, K)) = \mathrm{Cl}^0(E), \quad g(\mathrm{Cl}^1(n, K)) = \mathrm{Cl}^1(Q(E)).$$

The proof of the proposition (sketch)

(a) $f : \mathsf{Cl}(n, L) \xrightarrow{\sim} \mathsf{Cl}(L \otimes_K E, Q(E))$

$$E = \langle e_1, \ldots, e_n \rangle, \quad M = (e_i^{s_j}) \in \mathsf{GL}(n, L), \quad s_j \in \Phi, \quad 1 \leq i, j \leq n$$

$$M^T M = (\mathsf{Tr}_{E|K}(e_i e_j)) \Rightarrow (L^n, I_n) \simeq (L \otimes_K E, Q(E)).$$

The vectors $v_i := f(e_i)$ yield a basis of $\mathsf{Cl}(L \otimes_K E)$ and satisfy

$$v_i^2 = 1, \quad v_i v_j = -v_j v_i, \quad \text{for } i \neq j; \quad v_i^s = v_{s(i)}, \quad \text{for all } s \in G.$$

(b) $g : \mathsf{Cl}(n, K) \xrightarrow{\sim} \mathsf{Cl}(Q(E))$, if $d(E)$ and $w(E)$ are trivial.

The proof goes back to Springer. He uses the description of $w(E)$ in terms of non-commutative cohomology classes in $H^1(G_K, \mathsf{SO}(n, \overline{K}))$. The elements $w_i = g(e_i) \in \mathsf{Cl}^1(Q(E))$ are invariant under G. They satisfy

$$w_i^2 = 1, \quad w_i w_j = -w_j w_i, \quad \text{for } i \neq j.$$

$$
\begin{tikzcd}
\varepsilon & 1 \arrow[r] & C_2 \arrow[r] \arrow[d, "\wr"] & \widetilde{G} \arrow[r] \arrow[d, hook] & G \arrow[r] \arrow[d, hook] & 1 \\
& 1 \arrow[r] & C_2 \arrow[r] & \Gamma_0^+(n,K) \arrow[r, "\varphi"] & \mathrm{SO}(n,K) &
\end{tikzcd}
$$

- Let (u_s) be a system of representatives in $\widetilde{G}$ of the elements of G. From the construction of $\widetilde{G}$ they satisfy

$$u_s e_i u_s^{-1} = u_{s(i)}, \quad s \in G, \quad 1 \leq i \leq n.$$

- The 2-cocycle $\varepsilon \in H^2(G, C_2)$ corresponding to the extension $\widetilde{G}$ is defined by a factor set $(a_{s,t})$, $a_{s,t} \in C_2$, such that

$$u_s u_t = a_{s,t} u_{st}.$$

- On the other hand, if the embedding problem is solvable, we need to find an element $\gamma \in L$ such that $\widetilde{L} = L(\sqrt{\gamma})$ and

$$\gamma^s = b_s^2 \gamma, \text{ for all } s \in G, \text{ and } b_s \in L^* \text{ satisfying}$$

$$b_s b_t^s b_{st}^{-1} = a_{s,t}.$$

Main tool for the construction of γ: Clifford algebras

$f : \mathsf{Cl}(n, L) \xrightarrow{\sim} \mathsf{Cl}(L \otimes_K E, Q(E))$
$g : \mathsf{Cl}(n, K) \xrightarrow{\sim} \mathsf{Cl}(Q(E))$, if $d(E)$ and $w(E)$ are trivial.

Theorem. [Crespo] *Let $v_i = f(e_i)$, $w_i = g(e_i)$.*
(a) *The isomorphisms f, g can be chosen so that the element*

$$z := \sum_{\epsilon_j \in \{0,1\}} v_1^{\epsilon_1} v_2^{\epsilon_2} \cdots v_n^{\epsilon_n} w_n^{\epsilon_n} \cdots v_2^{\epsilon_2} v_1^{\epsilon_1} \in \mathsf{CL}(L \otimes_K E)$$

is nonzero. Accordingly, z and $N(z)$ are invertible in $\mathsf{CL}^0(L \otimes_K E)$ and L, respectively.
(b) *Let $m_s = f(u_s)$, $b_s = m_s^{-1} z^s z^{-1}$. Then, for all $s, t \in G$, is*

(i) $b_s \in L^*$.
(ii) $N(z)^s = b_s^2 N(z)$.
(iii) $b_s b_t^s = a_{s,t} b_{st}$.

Answering Serre's question

Theorem. [Crespo] *Let K be any fiel of characteristic $\neq 2$. Let $E|K$ be a separable extension of degree n whose Galois closure $L|K$ has a Galois group* $\mathrm{Gal}(L|K) \simeq G \subseteq A_n$, $n \geq 4$, $n \neq 6, 7$. *The spinor embedding problem $\widetilde{G} \to G \simeq \mathrm{Gal}(L|K)$ is solvable if and only if $w(E)$ is trivial. If this is the case, the general solution to the embedding problem is*

$$\widetilde{L} = L(\sqrt{r\gamma}),$$

where γ is a nonzero component of $N(z)$ in a G-invariant basis of $\mathrm{Cl}(L \otimes_K E)$ *and r runs through K^*.*

Remark. If $Q(E) \simeq I_n$ over K, and $P \in \mathrm{GL}(n, K)$ is such that $P^T(\mathrm{Tr}(e_i e_j))P = I_n$, then

$$\gamma = N(z) = 2^n \det(MP + I).$$

- In Witt's example: $\det(MP + I) = 4(p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{c})$.

□ □ □

First Publications

1 Vila, N.: Polynomials over $\mathbb{Q}$ solving an embedding problem. *Ann. Inst. Fourier* 35(1985), 79-83.

2 Vila, N.: On central extensions of A_n as Galois group over Q. *Archiv Math.* 44 (1985), 424-437.

3 Arenas, A.; Bayer, P.: Arithmetic behaviour of the sums of three squares. *J. Number Theory* 27 (1987), 273-284.

4 Arenas, A.: An arithmetic problem on the sums of three squares. *Acta Arithmetica* 51 (1988), 131-140.

5 Arenas, A.: On the summation of the singular series. *Manuscripta Mathematica* 57 (1987), no.4, 469-475.

6 Crespo, T.: Embedding problems with ramification conditions. *Archiv Math.* 53 (1989), 270-276.

7 Crespo, T.: Explicit construction of $\widetilde{A}_n$–type fields. *J. Algebra* 127 (1989), 452-461.

8 Crespo, T.: Explicit solutions to embedding problems associated to orthogonal Galois representations. *J. Reine Angew. Math.* 409 (1990), 180-189.

First Lectures and Proceedings

9. Vila, N.: Sur la résolution d'un problème de plongement. Proceedings of the 13èmes *Journées arithmétiques*. Noordwijkerhout (Holand), 1983. Lecture Notes in Math. 1068, Springer, 1984, 243-253.

10. Vila, N.: Sur la réalisation des extensions centrales du groupe alterné comme groupe de Galois sur Q. Seminar on Number Theory, 1983–1984, Exp. No. 18, 9 pp., Univ. Bordeaux I, Talence, 1984.

11. Arenas, A.: On positive integers representable as a sum of three squares. Proceedings of the 14èmes *Journées arithmétiques.* Besançon, 1985. Astérisque No. 147-148 (1987), 259–263.

12. Arenas, A.: Quantitative aspects of the representations of integers by quadratic forms. Théorie des nombres (Quebec, PQ, 1987), 7–14, de Gruyter, Berlin, 1989.

13. T. Crespo: Construcción efectiva de soluciones a problemas de inmersión de la Teoría de Galois. Jornadas Hispano-Lusas. Valladolid, 1988.

14. T. Crespo: Résolution explicite de doubles recouvrements comme groupes de Galois. *Journées Arithmétiques.* Marseille (France), 1989.

EPILOGE: construction of modular forms of weight one

$H^2(S_4, C_2) \simeq C_2 \times C_2, \qquad 1 \to C_2 \to \tilde{S}_4 \to S_4 \to 1$

$f_4(X)$ polynomial defining E, $[E : \mathbb{Q}] = 4$, $d =$ discriminant of E

$\widetilde{S_4}$ order	$1\tilde{A}$ 1	$2\tilde{A}$ 1	$4\tilde{A}$ 12	$3\tilde{A}$ 6	$6\tilde{A}$ 8	$2\tilde{B}$ 8	$8\tilde{A}$ 6	$8\tilde{B}$ 6
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	1	1	1	-1	-1	-1
χ_3	2	2	2	-1	-1	0	0	0
χ_4	3	3	-1	0	0	1	-1	-1
χ_5	3	3	-1	0	0	-1	1	1
χ_6	2	-2	0	-1	1	0	$i\sqrt{2}$	$-i\sqrt{2}$
χ_7	2	-2	0	-1	1	0	$-i\sqrt{2}$	$i\sqrt{2}$
χ_8	4	-4	0	1	-1	0	0	0

$\tilde{S}_4$ admits two faithful irreducible representations of dimension 2.

Modular forms of octahedral type

Let $\widetilde{S}_4 \to S_4 \simeq \mathrm{Gal}(L|\mathbf{Q})$ be a solvable embedding problem

- $\rho : G_{\mathbf{Q}} \to \mathrm{Gal}(\widetilde{L}|\mathbf{Q}) \simeq \widetilde{S}_4 \hookrightarrow \mathrm{GL}(2, \mathbf{C})$ odd Galois representation

$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi i z}$ modular form of weight one

$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{Gal}(L|\mathbf{Q}) \simeq S_4 \hookrightarrow \mathrm{PGL}(2, \mathbf{C})$

$\ell \nmid d$, a prime, $\quad \mathrm{Frob}_{\rho,\ell} \subset \widetilde{S}_4, \quad \mathrm{Frob}_{\overline{\rho},\ell} \subset S_4 \quad$ conjugacy classes

- $\mathrm{Frob}_{\overline{\rho},\ell}$ determines only a_ℓ^2

- $\mathrm{Frob}_{\rho,\ell}$ determines a_ℓ, but the computation of $\mathrm{Frob}_{\rho,\ell}$ requires an explicit solution of the embedding problem.

An explicit reciprocity law of octahedral type

$$f(X) = X^4 - 2X - 1 \in \mathbb{Q}[X], \quad x_i \in \overline{\mathbb{Q}}, \quad f(x_i) = 0,\ 1 \le i \le 4,$$

$$E = \mathbb{Q}(x_1),\ L = \mathbb{Q}(\{x_i\}),\ d = -688 = -2^4 \cdot 43,\ \ \mathrm{Gal}(L|\mathbb{Q}) \simeq S_4$$

$$\Phi(S_4) = \{1A,\ 2A,\ 2B,\ 3A,\ 4A\}$$

$\lambda\mathcal{O}_1$	$\mathrm{Fr}_\ell(L\|\mathbb{Q})$	$\sharp$	δ	$\ell \quad (\neq 2, 43)$
$\lambda_1\lambda_1'\lambda_1''\lambda_1'''$	$1A$	1	$1/24$	173, 487, 619, 719, 827, 857, ...
$\lambda_2\lambda_2'$	$2A$	6	$1/4$	47, 59, 79, 107, 181, 197, ...
$\lambda_1\lambda_1'\lambda_2$	$2B$	3	$1/8$	c, 19, 37, 71, 113, 131, 137, 149, ...
$\lambda_1\lambda_3$	$3A$	8	$1/3$	11, 13, 17, 23, 31, 41, 53, 67, 83, ...
λ_4	$4A$	6	$1/4$	3, 5, 7, 29, 61, 73, 89, 151, 163, ...

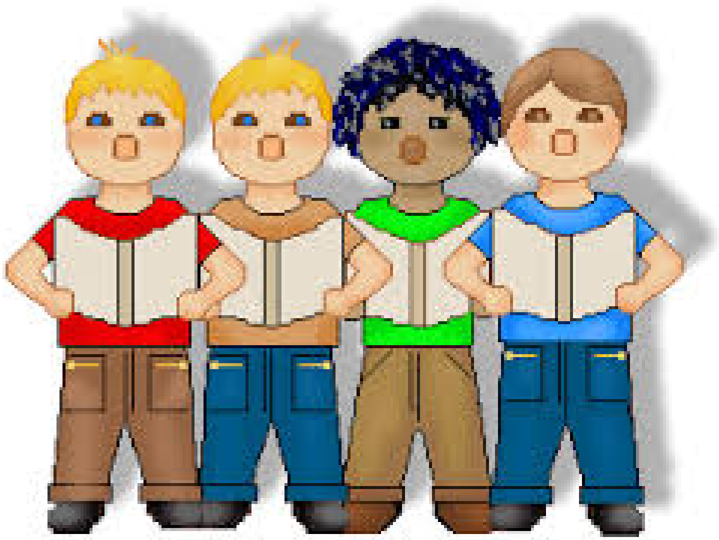
$\widetilde{S}_4$	$1\widetilde{A}, 2\widetilde{A}$	$4\widetilde{A}$	$2\widetilde{B}$	$3\widetilde{A}, 6\widetilde{A}$	$8\widetilde{A}, 8\widetilde{B}$
S_4	$1A$	$2A$	$2B$	$3A$	$4A$

$$\widetilde{L} = L(\sqrt{\gamma}), \quad \gamma = 3(x_1^3 x_2^2 - x_2^2 - x_1^2 x_2 + x_1 x_2 + x_2) + x_1^3 - 2x_1^2 + 4x_1$$

Fr_ℓ	$\sharp$	$\mathrm{Tr}(\mathrm{Fr}_\ell)$	$\det(\mathrm{Fr}_\ell)$	$\ell \quad (\neq 2, 43)$
$1\widetilde{A}$	1	2	1	$487, 619, 719, \cdots$
$2\widetilde{A}$	1	-2	1	$173, 827, 857, \cdots$
$2\widetilde{B}$	6	0	-1	$c, 19, 37, 71, 113, 131, 137, \cdots$
$3\widetilde{A}$	8	-1	1	$11, 17, 53, 67, 97, 101, \cdots$
$4\widetilde{A}$	12	0	1	$47, 59, 79, 107, 181, 197, \cdots$
$6\widetilde{A}$	8	1	1	$13, 23, 31, 41, 83, 109, \cdots$
$8\widetilde{A}$	6	$i\sqrt{2}$	-1	$7, 29, 61, 89, 179, \cdots$
$8\widetilde{B}$	6	$-i\sqrt{2}$	-1	$3, 5, 73, 151, 163, \cdots$

□ □ □

Other contributions...



From 1981 to 1988

♡♡♡