INVARIANT THEORY AND ITS APPLICATIONS

Ivo M. Michailov[*]

'As all the roads lead to Rome so I find in my own case at least that all algebraic inquiries, sooner or later, end at the Capitol of modern algebra over whose shining portal is inscribed the Theory Of Invariants.' (Sylvester (1864, p. 380))

KEYWORDS: *Invariant, Noether's problem, Inverse Galois Problem, Embedding problem, Clifford algebra, Quadratic form, Trace form, Galois cohomology, Shape invariant, Möbius invariant, Image processing, Pattern recognition.*

1 Historical background

Invariant theory is concerned with expressions that remain constant (invariant) under a group of transformations. As an everyday example, if a rigid yardstick is rotated, the coordinates (x, y, z) of its endpoints change, but its length L given by the formula $L^2 = \Delta x^2 + \Delta y^2 + \Delta z^2$ remains the same. The roots of invariant theory can be traced back in the research of Lagrange (1773) and Gauss (in his Disquisitiones Arithmeticae from 1801), who are interested in the representation of numbers by binary quadratic forms. They also used the discriminant for distinguishing between non equivalent forms.

In the first decades of invariant theory (1840-1870), people were mainly concerned with the discovery of particular invariants. The major case of interest was that of forms of degree d in n variables with $\mathrm{SL}_n(\mathbb{C})$ acting by linear substitution. Invariant theory was an active area of research in the later nineteenth century, prompted in part by Felix Klein's Erlangen program, according to which different types of geometry should be characterized by their invariants under transformations, e.g., the cross-ratio of projective geometry. For example, the geometric significance of the discriminant is that a quadratic binary form defines two distinct points on the projective line $\mathbb{P}^1(\mathbb{C})$ if and only if its discriminant is non zero. People became interested in such invariant properties especially after the introduction of homogeneous coordinates by Moebius (1827) and Plucker (1830). This was a major impetus for invariant theory.

The archetypal example of an invariant is the discriminant B^2-4AC of a binary quadratic form $Ax^2+Bxy+Cy^2$. This is called an invariant because it is unchanged by linear substitutions $x \mapsto ax + by, y \mapsto cx + dy$ with determinant $ad - bc = 1$. These substitutions form the special linear group SL_2. One can ask for all polynomials in A, B, and C that are unchanged by the action of SL_2; these are called the invariants of binary quadratic forms, and turn out to be the polynomials in the discriminant.

One of the main goals of invariant theory was to solve the "finite basis problem". The sum or product of any two invariants is invariant, and the finite basis problem asked whether it was possible to get all the invariants by starting with a finite list of invariants, called generators, and then, adding or multiplying the generators together. For example, the discriminant gives a finite basis (with one element) for the invariants of binary quadratic forms. Paul Gordan was known as the "king of invariant theory", and his chief contribution to mathematics was his 1870 solution of the finite basis problem for invariants of homogeneous polynomials in two variables. He proved this by giving a constructive method for finding all of the invariants and

[*] This work is partially supported by a project No RD-08-241/13.03.2014 of Shumen University

their generators, but was not able to carry out this constructive approach for invariants in three or more variables. In 1890, David Hilbert proved a similar statement for the invariants of homogeneous polynomials in any number of variables. Furthermore, his method worked, not only for the special linear group, but also for some of its subgroups such as the special orthogonal group. His first proof caused some controversy because it did not give a method for constructing the generators, although in later work he made his method constructive. For her thesis, Emmy Noether extended Gordan's computational proof to homogeneous polynomials in three variables. Noether's constructive approach made it possible to study the relationships among the invariants.

Noether was brought to Göttingen in 1915 by David Hilbert and Felix Klein, who wanted her expertise in invariant theory to help them in understanding general relativity, a geometrical theory of gravitation developed mainly by Albert Einstein. Hilbert had observed that the conservation of energy seemed to be violated in general relativity, due to the fact that gravitational energy could itself gravitate. Noether provided the resolution of this paradox, and a fundamental tool of modern theoretical physics, with Noether's first theorem, which she proved in 1915, but did not publish until 1918. She not only solved the problem for general relativity, but also determined the conserved quantities for every system of physical laws that possesses some continuous symmetry.

Upon receiving her work, Einstein wrote to Hilbert: "Yesterday I received from Miss Noether a very interesting paper on invariants. I'm impressed that such things can be understood in such a general way. The old guard at Göttingen should take some lessons from Miss Noether! She seems to know her stuff."

For illustration, if a physical system behaves the same, regardless of how it is oriented in space, the physical laws that govern it are rotationally symmetric; from this symmetry, Noether's theorem shows the angular momentum of the system must be conserved (known as Kepler's second law, see Fig. 1).

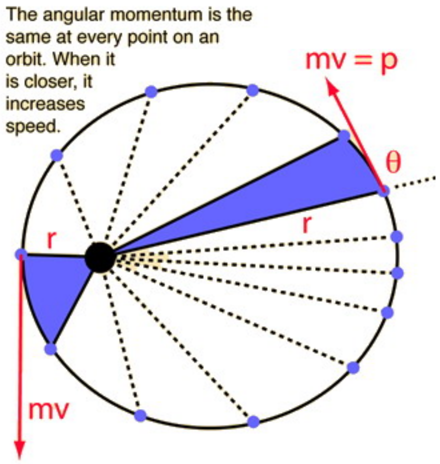
The angular momentum is the same at every point on an orbit. When it is closer, it increases speed.
mv = p
θ
r
r
mv

Figure 1. Kepler's second law of planetary motion.

Noether's theorem has become a fundamental tool of modern theoretical physics, both because of the insight it gives into conservation laws, and also, as a practical calculation tool.

2 Invariant theory of finite groups

Invariant theory of finite groups has intimate connections with Galois theory. One of the first major results was the main theorem on the symmetric functions that described the invariants of the symmetric group S_n acting on the polynomial ring $K[x_1, \ldots, x_n]$ by permutations of the variables. This theorem appears to have been understood, or at least intuited and used, by Newton, as early as 1665. By the turn of the nineteenth century it was regarded as well known. For Galois himself, it was the essential lemma on which his entire theory rested. However, it was not properly proven or even precisely stated until the nineteenth century.

In the following K will always denote an infinite field. (Usually, in invariant theory it is assumed that $K = \mathbb{C}$, the field of complex numbers.) Let W be a finite dimensional K-vector space. A function $f : W \to K$ is called polynomial or regular if it is given by a polynomial in the coordinates with respect to a basis of W. It is easy to see that this is independent of the choice of a coordinate system of W. We denote by $K[W]$ the K-algebra of polynomial functions on W which is usually called the coordinate ring of W or the ring of regular functions on W. If $w_1, \ldots, w_n$ is a basis of W and $x_1, \ldots, x_n$ the dual basis of the dual vector space W^* of W, i.e., the coordinate functions, we have $K[W] = K[x_1, \ldots, x_n]$. This is a polynomial ring in the x_i because the field K is infinite. Appart from the common operations addition and multiplication in a ring, $K[W]$ is a linear space over K, since we can multiply the polynomials with scalars from K. Moreover, for any $\alpha \in K, f, g \in K[W]$ is satisfied the condition $\alpha\cdot(f\cdot g) = (\alpha\cdot f)\cdot g = f\cdot(\alpha\cdot g)$. Such rings are called algebras.

As usual, we denote by $\mathrm{GL}(W)$ the general linear group, i.e., the group of K-linear automorphisms of the K-vector space W. Choosing a basis $(w_1, w_2, \ldots, w_n)$ of W we can identify $\mathrm{GL}(W)$ with the group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices with entries in K in the usual way: The i-th column of the matrix A corresponding to the automorphism $g \in \mathrm{GL}(W)$ is the coordinate vector of $g(w_i)$ with respect to the chosen basis.

Now assume that there is given a subgroup $G \subset \mathrm{GL}(W)$ or, more generally, a group G together with a linear representation on W, i.e., a group homomorphism $\rho : G \to \mathrm{GL}(W)$. The corresponding linear action of G on W will be denoted by $(\sigma, w) \mapsto \sigma w = \rho(\sigma)w$ $(\sigma \in G, w \in W)$, and we will call W a G-module.

Definition 2.1. A function $f \in K[W]$ is called *G-invariant* or shortly *invariant* if $f(\sigma w) = f(w)$ for all $\sigma \in G$ and $w \in W$. The invariants form a subalgebra of $K[W]$ called *invariant ring* and denoted by $K[W]^G$.

There is another way to describe the invariant ring. For this we consider the following linear action of G on the coordinate ring $K[W]$:

$$(\sigma, f) \mapsto \sigma f, \quad \sigma f(w) = f(\sigma^{-1} w), \quad \text{for } \sigma \in G, f \in K[W], w \in W.$$

This is usually called the regular representation of G on the coordinate ring. (The inverse σ^{-1} in this definition is necessary in order to get a left-action on the space of functions.) Clearly, a function f is invariant if and only if it is a fixed point under this action, i.e., $\sigma f = f$ for all $\sigma \in G$. This explains the notation $K[W]^G$ for the ring of invariants.

Example 2.1. Consider the special linear group $\mathrm{SL}_n(K)$, i.e., the sub-group of $\mathrm{GL}_n(K)$ of matrices with determinant 1, and its representation on the space $\mathrm{M}_n(K)$ of $n \times n$-matrices by left multiplication: $(\sigma, A) \mapsto \sigma A$, $\sigma \in \mathrm{SL}_n, A \in \mathrm{M}_n(K)$. Clearly, the determinant function $A \mapsto \det A$ is invariant. In fact, it can be proved that the invariant ring is generated by the determinant: $K[\mathrm{M}_n]^{\mathrm{SL}_n} = K[\det]$.

Example 2.2. Let S_n denote the symmetric group on n letters and consider the natural representation of S_n on $W = K^n$ given by $\sigma(e_i) = e_{\sigma(i)}$, or, equivalently,

$$\sigma(x_1, x_2, \dots, x_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(n)}).$$

The symmetric group S_n acts on the polynomial ring $K[x_1, \dots, x_n]$, and the invariant functions are the symmetric polynomials:

$$K[x_1, \dots, x_n]^{S_n} = \{f \mid f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n) \text{ for all } \sigma \in S_n\}.$$

It is well known and classical that every symmetric function can be expressed uniquely as a polynomial in the elementary symmetric functions $\sigma_1, \sigma_2, \dots, \sigma_n$ defined by

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n, \\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\
&\vdots \\
\sigma_k &= \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}, \\
&\vdots \\
\sigma_n &= x_1 x_2 \dots x_n.
\end{aligned}$$

Formally:

Theorem 2.1. (Fundamental Theorem on Symmetric Polynomials) *Any symmetric polynomial in n variables $x_1, \dots, x_n$ is representable in a unique way as a polynomial in the elementary symmetric polynomials $\sigma_1, \sigma_2, \dots, \sigma_n$.*

The existence part of the latter theorem can be formulated also thus:

Corollary 2.2. *The elementary symmetric polynomials $\sigma_1, \sigma_2, \dots, \sigma_n$ generate the algebra of symmetric polynomials:*

$$K[x_1, \dots, x_n]^{S_n} = K[\sigma_1, \sigma_2, \dots, \sigma_n].$$

One of the fundamental problems in Classical Invariant Theory is the following:

Open Problem. *Describe generators and relations for the ring of invariants $K[W]^G$.*

This question goes back to the 19th century and a number of well-known mathematicians of that time have made important contributions: Boole, Sylvester, Cayley, Hermite, Clebsch, Gordan, Capelli, Hilbert.

Example 2.3. Consider the group

$$C_2 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} < \mathrm{GL}_2(K) \ (\text{char } K \neq 2).$$

It is not hard to show that $f \in K[x_1, x_2]$ is invariant under C_2 if and only if we can write $f(x_1, x_2) = g(x_1^2, x_2^2, x_1x_2)$ for some polynomial $g \in K[x_1, x_2]$. Therefore $K[x_1, x_2]^{C_2} = K[x_1^2, x_2^2, x_1x_2]$.

More generally:

Example 2.4. Let $C_2 = \{id, \sigma\}$, the cyclic group of order 2, act on the n-dimensional K-vector space W by $\sigma(v) = -v$ (char $K \neq 2$). We are going to determine a system of generators for the ring of invariants $K[W]^{C_2}$. Note first that $f \in K[x_1, \ldots, x_n]$ is invariant under C_2 if and only if $f(x_1, \ldots, x_n) = \sigma f = f(-x_1, \ldots, -x_n)$. Hence the invariants are the polynomials that are sums of monomials of even degree. (Recall that the degree d of the monomial $ax_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ is defined as $d = d_1 + d_2 + \cdots + d_n$.) In particular, the monomials $x_1^2, \ldots, x_n^2, x_i x_j$ $(i \neq j)$ are invariants. It can be shown that any monomial of even degree is a product of these monomials, so $K[x_1, \ldots, x_n]^{C_2} = K[x_1^2, \ldots, x_n^2, x_i x_j : i \neq j]$.

Example 2.5. Consider the group

$$E_4 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} < \mathrm{GL}_2(K) \text{ (char } K \neq 2).$$

This is the elementary abelian group of order 4 called sometimes the Klein four group. If a polynomial $f \in K[x_1, x_2]$ is invariant under E_4 then $f(x_1, x_2) = f(-x_1, x_2) = f(x_1, -x_2)$, and clearly the converse is also true. If $f(x_1, x_2) = \sum_{i,j} a_{ij} x_1^i x_2^j$ the condition $f(x_1, x_2) = f(-x_1, x_2)$ is equivalent to $a_{ij} = 0$ for i odd, and the condition $f(x_1, x_2) = f(x_1, -x_2)$ is equivalent to $a_{ij} = 0$ for j odd. Thus we have that $f(x_1, x_2) = g(x_1^2, x_2^2)$ for some polynomial $g \in K[x_1, x_2]$. Therefore $K[x_1, x_2]^{E_4} = K[x_1^2, x_2^2]$.

We can generalize the latter example:

Example 2.6. Let $E_{2^n} = \langle \sigma_1, \ldots, \sigma_n \rangle$, the elementary abelian group of order 2^n, act on the n-dimensional K-vector space W by $\sigma_i(e_j) = (-1)^{\delta_{ij}} e_j$, where δ_{ij} is the Kronecker's delta ($\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$). Note that $f \in K[x_1, \ldots, x_n]$ is invariant under E_{2^n} if and only if $f(x_1, \ldots, x_n) = f(-x_1, x_2, \ldots, x_n) = f(x_1, -x_2, \ldots, x_n) = \cdots = f(x_1, x_2, \ldots, -x_n)$. As in example 2.5 it is easy to see that $f(x_1, \ldots, x_n) = g(x_1^2, \ldots, x_n^2)$ for some polynomial $g \in K[x_1, \ldots, x_n]$. Therefore $K[x_1, \ldots, x_n]^{E_{2^n}} = K[x_1^2, \ldots, x_n^2]$.

3 Some Finiteness Theorems

One of the highlights of the 19th century invariant theory was Gordan's famous theorem showing that the invariants of binary forms (under SL_2) are finitely generated. His proof is rather involved and can be roughly described as follows: He gives a general inductive method to construct all invariants, and then he shows that after a certain number of steps the construction does not produce any new invariant. Thus, the finite number of invariants constructed so far form a system of generators. It was already clear at that time that it will be very difficult to generalize Gordan's method to other groups than SL_2. So it came as a big surprise when Hilbert presented in 1890 his general finiteness result for invariants, using completely new ideas and techniques.

Definition 3.1. For a ring R and a subset $S \subseteq R$, the *ideal* generated by S is defined as

$$(S) := \{r_1 s_1 + \cdots + r_k s_k \mid k \in \mathbb{N}, r_1, \ldots, r_k \in R, s_1, \ldots, s_k \in S\}.$$

An ideal $I \subseteq R$ is called *finitely generated* if there is a finite set S such that $I = (S)$.

Definition 3.2. A ring R is called *Noetherian* if every ideal I in R is finitely generated.

We will be mostly interested in polynomial rings over $\mathbb{C}$ in finitely many indeterminates, for which the following theorem is essential.

Theorem 3.1. (Hilbert's Basis Theorem) *The polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian.*

With this tool in hand, we can now return to our main theorem of this section.

Theorem 3.2. (Hilbert's Finiteness Theorem)) *Let G be a group and let W be a finite dimensional G-module with the property that $\mathbb{C}[W]$ is completely reducible. Then $\mathbb{C}[W]^G = \{f \in \mathbb{C}[W] \mid gf = f, \forall g \in G\}$ is a finitely generated subalgebra of $\mathbb{C}[W]$. That is, there exist $f_1, \ldots, f_k \in \mathbb{C}[W]^G$ such that every G-invariant polynomial on W, is a polynomial in the f_i.*

The proof uses the so-called *Reynolds operator* ρ, which is defined as follows. We assume that the vector space $\mathbb{C}[W]$ is completely reducible. Consider its isotypic decomposition $\mathbb{C}[W] = \oplus_{i \in I} V_i$ and let $1 \in I$ correspond to the trivial 1-dimensional G-module, so that $\mathbb{C}[W]^G = V_1$. Now let ρ be the projection from $\mathbb{C}[W]$ onto V_1 along the direct sum of all V_i with $i \neq 1$. This is a G-equivariant linear map. Moreover, we claim that

$$\rho(f \cdot h) = f \cdot \rho(h) \quad \text{for all } f \in V_1,$$

where the multiplication is multiplication in $\mathbb{C}[W]$. Indeed, consider the map $\mathbb{C}[W] \to \mathbb{C}[W], h \mapsto fh$. This a G-module morphism, since $g(f \cdot h) = (gf) \cdot (gh) = f \cdot (gh)$, where the first equality reflects that G acts by automorphisms on $\mathbb{C}[W]$ and the second equality follows from the invariance of f. Hence if we write h as $\sum_i h_i$ with $h_i \in V_i$, then $fh_i \in V_i$ by Schur's lemma, and therefore the component of $fh = \sum_i (fh_i)$ in V_1 is just fh_1. In other words $\rho(f \cdot h) = f \cdot \rho(h)$, as claimed.

Exercise 1. *Show that for a finite group G, the Reynolds operator is just $f \mapsto \frac{1}{|G|} \sum_{g \in G} gf$.*

Proof of Hilbert's finiteness theorem. Let $I' = \oplus_{d>0} \mathbb{C}[W]_d^G$ be the ideal in $\mathbb{C}[W]^G$ consisting of all invariants with zero constant term. Denote by $I = \mathbb{C}[W]I'$ the ideal in $C[W]$ generated by I'. Since W is finite dimensional, it follows from Hilbert's basis theorem that there exist $f_1, \ldots, f_k \in I$ that generate the ideal I. We may assume that the f_i belong to I'. Indeed, if $f_i \notin I'$, we can write $f_i = \sum_j f_{ij} g_{ij}$ for certain $f_{ij} \in I'$ and $g_{ij} \in \mathbb{C}[W]$ and replace f_i with the f_{ij} to obtain a finite generating set of I with fewer elements in $I \setminus I'$.

We observe that the ideal I' is generated by the f_i. Indeed, let $h \in I' \subseteq I$ and write $h = \sum_i g_i f_i$ for some $g_i \in \mathbb{C}[W]$. Using the Reynolds operator ρ we find: $h = \rho(h) = \sum_i \rho(f_i g_i) = \sum_i f_i \rho(g_i)$. The proof is now completed by exercise 2. □

Exercise 2. *Let $A \subseteq \mathbb{C}[W]$ be a subalgebra, and let $A^+ = \oplus_{d \geq 1} A \cap \mathbb{C}[W]_d$ be the ideal of polynomials in A with zero constant term. Suppose that the ideal A^+ is finitely generated. Show that A is finitely generated as an algebra over $\mathbb{C}$.*

It is well known that for a finite group G, any G-module V is completely reducible. This implies by Hilbert's theorem that for finite groups, the invariant ring is always finitely generated. Noether proved a result stating that for finite groups G, the invariant ring is already generated by the invariants of degree at most $|G|$, which implies a bound on the number of generators needed.

Theorem 3.3. (Noether's degree bound)) *Let G be a finite group, and let W be a (finite dimensional) G-module. Then the invariant ring $\mathbb{C}[W]^G$ is generated by the homogeneous invariants of degree at most $|G|$.*

4 Noether's problem

In 1918, Emmy Noether published a seminal paper [32] on the *inverse Galois problem*. Instead of determining the Galois group of transformations of a given field and its extension, Noether asked whether, given a field and a group, it always is possible to find an extension of the field that has the given group as its Galois group. Noether reduced this to *Noether's problem*, which asks whether the fixed field of a subgroup G of the permutation group S_n acting on the function field $K(x_1,\dots,x_n)$ always is purely transcendental (i.e. rational) extension of the field K. Recall that a field extension L of K is purely transcendental (or rational) over K if $L \simeq K(x_1,\dots,x_n)$ over K for some integer n, with $x_1,\dots,x_n$ algebraically independent over K.

Example 4.1. The symmetric group S_n acts on the function field $K(x_1,\dots,x_n)$, and the invariant functions are the symmetric functions. According to the Fundamental Theorem on Symmetric Polynomials:

$$K(x_1,\dots,x_n)^{S_n} = K(\sigma_1,\dots,\sigma_n).$$

The elementary symmetric polynomials are algebraically independent over K, so $K(\sigma_1,\dots,\sigma_n)$ is purely transcendental over K, i.e., Noether's problem has an affirmative answer for S_n over any field K.

On the other hand, it is known that the answer is 'no' for some G's, even for an algebraically closed K. For most G's, as for example the alternating groups A_n with $n > 5$, the problem remains open for every K. A more general version of Noether's problem asks, in Serre's terminology [9, 33.1], whether the following property holds:

Noe(G/K): There exists a faithful, finite-dimensional, linear K-representation $G \subset GL(V)$ such that the extension $K(V)^G/K$ is rational.

Usually, Noether's problem is formulated in this way: Let G be a finite group and G act on the rational function field $K(x(g) : g \in G)$ by K automorphisms defined by $g \cdot x(h) = x(gh)$ for any $g, h \in G$. Denote by $K(G)$ the fixed field $K(x(g) : g \in G)^G$. *Noether's problem* then asks whether $K(G)$ is rational over K.

Noether's problem for abelian groups was studied extensively by Swan, Voskresenskii, Endo, Miyata and Lenstra, etc. The reader is referred to Swan's paper for a survey of this problem [47]. Fischer's Theorem is a starting point of investigating Noether's problem for finite abelian groups in general.

Theorem 4.1. (Fischer [47, Theorem 6.1]) *Let G be a finite abelian group of exponent e. Assume that* (i) *either char $K = 0$ or char $K > 0$ with char $K \nmid e$, and* (ii) *K contains a primitive e-th root of unity. Then $K(G)$ is rational over K.*

Example 4.2. The cyclic group $C_2 = \{1, g\}$ acts on the function field $K(x_1, x_g)$ by $g : x_1 \mapsto x_g \mapsto x_1$. Define $y_1 = x_1 + x_g, y_2 = x_1 - x_g$. We have that $K(x_1, x_g) = K(y_1, y_2)$ and $g : y_1 \mapsto y_1, y_2 \mapsto -y_2$. It is easy to see now that $K(x_1, x_g)^{C_2} = K(y_1, y_2)^{C_2} = K(y_1, y_2^2)$ is rational over K.

The following theorem of Kang generalizes Fischer's theorem for the metacyclic p-groups.

Theorem 4.2. (Kang [14, Theorem 1.5]) *Let G be a metacyclic p-group with exponent p^e, and let K be any field such that* (i) *char $K = p$, or* (ii) *char $K \neq p$ and K contains a primitive p^e-th root of unity. Then $K(G)$ is rational over K.*

The next stage is to study Noether's problem for metabelian groups, and in particular the central extensions of bicyclic groups.

Theorem 4.3. (Michailov, Ivanov, Ziapkov [27, Theorem 2.2]) *Let G be a bicyclic p-group generated by two elements σ and τ with relations $\sigma^{p^a} = 1, \tau^{p^b} = 1$ and $\tau^{-1}\sigma\tau = \sigma$. Assume that $\widetilde{G}$ is a central extension of G, i.e., we have the following group extension*

$$1 \longrightarrow C \longrightarrow \widetilde{G} \longrightarrow G \cong C_{p^a} \times C_{p^b} \longrightarrow 1,$$

where $C \leq Z(\widetilde{G})$. Let p^t be the exponent of C, let $a \geq b \geq t$ and let the pre-image of $[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau$ in $\widetilde{G}$ be of order p^t. Let $e = \max\{a, 2t\}$. Assume that (i) *char$K = p$ or* (ii) *char$K \neq p$, K is infinite, and K contains a primitive p^e-th root of unity. Then $K(\widetilde{G})$ is rational over K.*

Recently, Michailov gave an affirmative answer to Noether's problem for p-groups having an abelian normal subgroup of index p.

Theorem 4.4. (Michailov [25, Theorem 1.8]) *Let G be a group of order p^n for $n \geq 2$ with an abelian subgroup H of order p^{n-1}, and let G be of exponent p^e. Choose any $\alpha \in G$ such that α generates G/H, i.e., $\alpha \notin H, \alpha^p \in H$. Denote $H(p) = \{h \in H : h^p = 1, h \notin H^p\} \cup \{1\}$, and assume that $[H(p), \alpha] \subset H(p)$. Denote by $G_{(i)} = [G, G_{(i-1)}]$ the lower central series for $i \geq 1$ and $G_{(0)} = G$. Let the p-th lower central subgroup $G_{(p)}$ be trivial. Assume that* (i) *char $K = p > 0$, or* (ii) *char $K \neq p$ and K contains a primitive p^e-th root of unity. Then $K(G)$ is rational over K.*

The key idea to prove Theorem 4.4 is to find a faithful G-subspace W of the regular representation space $\bigoplus_{g \in G} K \cdot x(g)$ and to show that W^G is rational over K. The subspace W is obtained as an induced representation from H.

5 The inverse problem in Galois theory

The *inverse problem of Galois theory* consists of two parts:

1. **Existence.** Determine whether there exists a Galois extension M/K such that the Galois group Gal(M/K) is isomorphic to G.
2. **Actual construction.** If G is realizable as a Galois group over K, construct explicitly either Galois extensions or polynomials over K having G as a Galois group.

The classical inverse problem of Galois theory is the existence problem for the field $K = \mathbb{Q}$ of rational numbers. The question whether all finite groups can be realized over $\mathbb{Q}$ is one of the most challenging problems in mathematics, and it is still unsolved. If Noether's Problem Noe$(G/\mathbb{Q})$ has an affirmative answer, G can be realised as a Galois group over $\mathbb{Q}$, and in fact over any Hilbertian field of characteristic 0.

In the nineteenth century, the following result was established:

Theorem 5.1. (Kronecker-Weber) *Every algebraic number field whose Galois group over $\mathbb{Q}$ is abelian, is a subfield of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is an n-th root of unity for some natural number n.*

The latter theorem was first stated by Kronecker (1853) though his argument was not complete for extensions of degree a power of 2. Weber (1886) published a proof, but this had some gaps and errors that were pointed out and corrected by Neumann (1981). The first complete proof was given by Hilbert (1896). The proof can be found in most books on class field theory. In the early 20-th century Hilbert's 12-th problem on the generalization of the Kronecker-Weber Theorem gained popularity. The history of the 12-th problem is explained at lenght in [40].

The first systematic study of the inverse Galois problem started with Hilbert in 1892. Hilbert used his Irreducibility Theorem to establish the following result:

Theorem 5.2. *For any $n \geq 1$, the symmetric group S_n and the alternating group A_n occur as Galois groups over $\mathbb{Q}$.*

The first explicit examples of polynomials with the alternating group A_n as a Galois group were given by Schur [42] in 1930.

The next important step was taken in 1937 by A. Scholz and H. Reichard [41, 35] who proved the following existence result:

Theorem 5.3. *For an odd prime p, every finite p-group occurs as a Galois group over $\mathbb{Q}$.*

The final step concerning solvable groups was taken by Shafarevich [45], although with a mistake relative to the prime 2. In the notes appended to his Collected papers, p. 752, Shafarevich sketches a method to correct this. For a full correct proof, the reader is referred to the book by Neukirch, Schmidt and Wingberg [33, Chapter IX].

Theorem 5.4. (Shafarevich) *Every solvable group occurs as a Galois group over $\mathbb{Q}$.*

Of the finite simple groups, the projective groups $\mathrm{PSL}(2,p)$ for some odd primes p were among the first to be realized. The existence was established by Shih in 1974 and later polynomials were constructed by Malle and Matzat:

Theorem 5.5. (Shih [46]) *Let p be an odd prime such that either $2, 3$ or 7 is a quadratic non-residue modulo p. Then $\mathrm{PSL}(2,p)$ occurs as a Galois group over $\mathbb{Q}$.*

Theorem 5.6. (Malle & Matzat [30]) *Let p be an odd prime with $p \not\equiv \pm 1 \pmod{24}$. Then explicit families of polynomials over $\mathbb{Q}(t)$ with Galois group $\mathrm{PSL}(2,p)$ can be constructed.*

For the 26 sporadic simple groups, all but possibly one, namely, the Mathieu group $\mathbf{M}_{23}$, have been shown to occur as Galois groups over $\mathbb{Q}$ by Matzat and his collaborators. It should be noted that all these realization results of simple groups were achieved via the rigidity method and the Hilbert Irreducibility Theorem. Extensive surveys of recent developments regarding the classical inverse problem can be found for example in [28, 13, 29, 44, 48].

6 The embedding problem in Galois theory

Let k be an arbitrary field and let G be a non simple group. Assume that A is a normal subgroup of G. Then the realizability of the quotient group $F = G/A$ as a Galois group over k is a necessary condition for the realizability of G over k. In this way arises the next generalization of the inverse problem in Galois theory – the embedding problem of fields.

Let K/k be a Galois extension with Galois group F, and let

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\alpha} F \longrightarrow 1, \tag{1}$$

be a group extension, i.e., a short exact sequence. Solving *the embedding problem* related to K/k and (1) consists of determining whether or not there exists a Galois algebra (called also a *weak* solution) or a Galois extension (called a *proper* solution) L, such that K is contained in L, G is isomorphic to $\mathrm{Gal}(L/k)$, and the homomorphism of restriction to K of the automorphisms from G coincides with α. We denote the so formulated embedding problem by $(K/k, G, A)$. We call the group A the *kernel* of the embedding problem.

1. Cohomological criteria for solvability of embedding problems with cyclic kernel of order p. Now, let k be an arbitrary field of characteristic not p, containing a primitive p^nth root of unity ζ_{p^n} for $n \in \mathbb{N}$, and put $\mu_{p^n} = \langle\zeta_{p^n}\rangle$. Let K be a Galois extension of k with Galois group F. Consider a non split group extension

$$1 \longrightarrow \langle\varepsilon\rangle \longrightarrow G \longrightarrow F \longrightarrow 1, \tag{2}$$

where ε is a central element of order p^n in G. We are going to identify the groups $\langle\varepsilon\rangle$ and μ_{p^n}, since they are isomorphic as F-modules.

Assume that $c \in H^2(F, \mu_{p^n})$ is the 2-coclass corresponding to the group extension (2) and denote by Ω_k the Galois group of the algebraic separable closure $\bar{k}$ over k. *The obstruction* to the embedding problem $(K/k, G, \mu_{p^n})$ we call the image of c under the inflation map $\mathrm{inf}_F^{\Omega_k} : H^2(F, \mu_{p^n}) \to H^2(\Omega_k, \mu_{p^n})$.

Note that we have the standard isomorphism of $H^2(\Omega_k, \mu_{p^n})$ with the p^n-torsion in the Brauer group of k induced by applying $H^*(\Omega_k, \cdot)$ to the p^n-th power exact sequence of Ω_k-modules $1 \longrightarrow \mu_{p^n} \longrightarrow \bar{k}^\times \longrightarrow \bar{k}^\times \longrightarrow 1$. In this way, the obstruction equals the equivalence class of the crossed product algebra $(F, K/k, \bar{c})$ for any $\bar{c} \in c$. Hence we may identify the obstruction with a Brauer class in $\mathrm{Br}_{p^n}(k)$.

Note that we have an injection $\mu_{p^n} \hookrightarrow K^\times$, which induces a homomorphism $\nu : H^2(F, \mu_{p^n}) \to H^2(F, K^\times)$. Then the obstruction is equal to $\nu(c)$, since there is an isomorphism between the relative Brauer group $\mathrm{Br}(K/k)$ and the group $H^2(F, K^\times)$.

More generally, the following result holds.

Theorem 6.1. ([15]) *Let $n \geq 1$, and let c be the 2-coclass in $H^2(F, \mu_{p^n})$, corresponding to the non split central group extension* (2)*. Then the embedding problem $(K/k, G, \mu_{p^n})$ is weakly solvable if and only if $\nu(c) = 1$. If $n = 1$ or μ_{p^n} is contained in the Frattini subgroup $\Phi(G)$ of G (for $n > 1$), then the condition $\nu(c) = 1$ is sufficient also for the proper solvability of the problem $(K/k, G, \mu_{p^n})$ (see [11, §1.6, Cor. 5]).*

Henceforth, embedding problems of the kind $(K/k, G, \mu_{p^n})$ we will call μ_{p^n}-embedding problems. We are going to consider first the case $n = 1$.

From the well-known Merkurjev-Suslin Theorem [20] it follows that the obstruction to any μ_p-embedding problem is equal to a product of classes of cyclic p-algebras. The explicit computation of these cyclic p-algebras, however, is not a trivial task. We are going to discuss the methods for achieving this goal. Denote by $(a, b; \zeta_{p^n})$ the equivalence class of the cyclic p^n-algebra which is generated by i_1 and i_2, such that $i_1^{p^n} = b, i_2^{p^n} = a$ and $i_1 i_2 = \zeta_{p^n} i_2 i_1$. Of course, we assume again that k contains ζ_{p^n}, a primitive p^n-th root of unity. For $p = 2$ and $n = 1$ we have the quaternion class $(a, b; -1)$, commonly denoted by (a, b).

In 1987 Massy [19] obtained a formula for the decomposition of the obstruction in the case when $F = \mathrm{Gal}(K/k)$ is isomorphic to $(C_p)^n$, the elementary abelian p-group.

Theorem 6.2. ([19, Théorème 2],[18, Cor. 6.1.6]) *Let $K/k = k(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \dots, \sqrt[p]{a_n})/k$ be a $(C_p)^n$ extension, and let $\sigma_1, \sigma_2, \dots, \sigma_n \in \operatorname{Gal}(K/k)$ be given by $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}$ (δ_{ij} is the Kronecker delta). Let*

$$1 \longrightarrow \mu_p \longrightarrow G \longrightarrow \operatorname{Gal}(K/k) \longrightarrow 1$$

be a non split central extension, and choose pre-images $s_1, s_2, \dots, s_n \in G$ of $\sigma_1, \sigma_2, \dots, \sigma_n$. Define $d_i (1 \le i \le n)$ by $s_i^p = \zeta^{d_i}$, and $d_{ij} (i < j)$ by $s_i s_j = \zeta^{d_{ij}} s_j s_i$. Then the obstruction to the proper solvability of the embedding problem $(K/k, G, \mu_p)$ is

$$\prod_{i=1}^{n} (a_i, \zeta; \zeta)^{d_i} \prod_{i<j} (a_j, a_i; \zeta)^{d_{ij}}.$$

Michailov [21, 22] obtained a formula for the decomposition of the obstruction in the case when the quotient F has a direct factor C_p.

Let H be a p-group and let

$$1 \longrightarrow \mu_p \longrightarrow G \xrightarrow{\pi} F \cong H \times C_p \longrightarrow 1 \tag{3}$$

be a non split central group extension with characteristic 2-coclass $\gamma \in H^2(H \times C_p, C_p)$. By $\operatorname{res}_H \gamma$ we denote the 2-coclass of the group extension

$$1 \longrightarrow \mu_p \longrightarrow \pi^{-1}(H) \xrightarrow{\pi} H \longrightarrow 1.$$

Let $\sigma_1, \sigma_2, \dots, \sigma_m$ be a minimal generating set for the maximal elementary abelian quotient group of H; and let τ be the generator of the direct factor C_p. Finally, let $s_1, s_2, \dots, s_m, t \in G$ be the pre-images of $\sigma_1, \sigma_2, \dots, \sigma_m, \tau$, such that $t^p = \zeta^j$ and $t s_i = \zeta^{d_i} s_i t$, where $i \in \{1, 2, \dots, m\}; j, d_i \in \{0, 1, \dots, p-1\}$.

Theorem 6.3. (Michailov [21, Theorem 4.1],[22, Theorem 2.1]) *Let K/k be a Galois extension with Galois group H and let $L/k = K(\sqrt[p]{b})/k$ be a Galois extension with Galois group $H \times C_p$ ($b \in k^\times \setminus k^{\times p}$). Choose $a_1, a_2, \dots, a_m \in k^\times$, such that $\sigma_k \sqrt[p]{a_i} = \zeta^{\delta_{ik}} \sqrt[p]{a_i}$ (δ_{ik} is the Kronecker delta). Then the obstruction to the proper solvability of the embedding problem $(L/k, G, \mu_p)$ is*

$$[K, H, \operatorname{res}_H \gamma] \left(b, \zeta^j \prod_{i=1}^{m} a_i^{d_i}; \zeta \right).$$

Recently, Michailov proved the following generalizations of theorem 6.2.

Theorem 6.4. (Michailov [26, Theorem 2.5]) *Let L/k be an $H \cong \prod_{i=1}^{t} C_{p^{n_i}}$ extension for some natural numbers $n_1 \le n_2 \le \dots \le n_t$. Let*

$$1 \longrightarrow \mu_p \longrightarrow G \longrightarrow H \cong \prod_{i=1}^{t} C_{p^{n_i}} \longrightarrow 1$$

be a non split central group extension with cohomology class $\gamma \in H^2(H, \mu_p)$. Let K_i/k be the subextension corresponding to the factor $C_{p^{n_i}}$ for $i = 1, \dots, t$. (I.e., K_i is the fixed subfield of $\prod_{j \neq i} C_{p^{n_j}}$.) Let σ_i be the generator of $C_{p^{n_i}}$ for $i = 1, \dots, t$, and choose $a_i \in k^\times$, such that $\sqrt[p]{a_i} \in K_i^\times$ and $\sigma_j \sqrt[p]{a_i} = \zeta^{\delta_{ij}} \sqrt[p]{a_i}$ (δ is the Kronecker delta). Let $s_1, \dots, s_t$ be the pre-images of $\sigma_1, \dots, \sigma_t$, let $d_{ij} \in \{0, \dots, p-1\}$ be given by $s_i s_j = \zeta^{d_{ji}} s_j s_i$, and let $s_i^{p^{n_i}} = \zeta^{m_i}$ for $i = 1, \dots, t; m_i \in \{0, \dots, p-1\}$.

Finally, define $r = \max\{i : m_i > 0\}, n = n_r, A = \{i : n_i = n, m_i > 0\}$*, and assume that* k *contains* ζ_{p^n}*, a primitive* p^n*-th root of unity. Then the obstruction to the proper solvability of the embedding problem* $(L/k, G, \mu_p)$ *given by* γ *is*

$$\prod_{i\in A}(a_i, \zeta_{p^n}^{m_i}; \zeta) \cdot \prod_{i<j}(a_j, a_i; \zeta)^{d_{ij}}.$$

Theorem 6.5. (Michailov [26, Theorem 2.8]) *Let* k *contain a primitive* p^n*-th root of unity* ζ_{p^n}*, and let* $L/k = k(\sqrt[p^n]{a_1}, \dots, \sqrt[p^n]{a_m})/k$ *be an arbitrary* $(C_{p^n})^m$ *extension for some* $m, n \in \mathbb{N}$*. Let*

$$1 \longrightarrow \mu_{p^n} \longrightarrow G \longrightarrow (C_{p^n})^m \longrightarrow 1$$

be a non split central group extension, let $\sigma_1, \sigma_2, \dots, \sigma_m$ *be the generators of* $(C_{p^n})^m$*, and let* $s_1, s_2, \dots, s_m \in G$ *be their pre-images such that* $s_i^{p^n} = \zeta_{p^n}^{j_i}$ *and* $s_j s_i = \zeta_{p^n}^{d_{ij}} s_i s_j$*, where* $i \in \{1, 2, \dots, m\}; j_i, d_{ij} \in \{0, 1, \dots, p^n - 1\}$ *and* $i < j$*. Assume that* $\sigma_j \sqrt[p^n]{a_i} = \zeta_{p^n}^{\delta_{ij}} \sqrt[p^n]{a_i}$ *(*δ_{ij} *is the Kronecker delta). Then the obstruction to the weak solvability of the embedding problem* $(L/k, G, \mu_{p^n})$ *is*

$$\prod_{i=1}^{m}(a_i, \zeta_{p^n}^{j_i}; \zeta_{p^n}) \cdot \prod_{i<j}(a_j, a_i; \zeta_{p^n})^{d_{ij}}.$$

2. Orthogonal representations of Galois groups. We begin with some preliminaries about orthogonal representations. Let k be a field of characteristic $\neq 2$, let V be a finite-dimensional k-vector space, and let (V, q) be a quadratic space, q being a quadratic form. The isometries $(V, q) \mapsto (V, q)$ constitute a subgroup $O(q)$ of $\mathrm{GL}(V)$, called *the orthogonal group* of q. *An orthogonal representation* of a finite group G is then a homomorphism $\mu : G \longrightarrow O(q)$ of G into the orthogonal group of some regular quadratic form q. From now on, by an orthogonal representation we will mean a *faithful* one, i.e., an embedding $\mu : G \hookrightarrow O(q)$.

We adopt the notations about Clifford algebras used in [18, Ch. 5, S. 2]: $C(q)$ is the Clifford algebra of q; $C_0(q)$ is the even Clifford algebra; $C(q) = C_0(q) \oplus C_1(q)$; if $x \in C_i(q)$, we write $\partial x = i$; $C^\times(q)$ is the Clifford group, defined as the subgroup of $C(q)^\times$, consisting of those invertible elements x, for which $xVx^{-1} = V$. The anisotropic vectors of V are in $C^\times(q)$ and $vuv^{-1} = -T_v(u)$ for $u, v \in V$, where v is anisotropic and T_v is the reflection on the hyperplane $v^\perp$. There is an exact sequence

$$1 \longrightarrow k^\times \longrightarrow C^\times(q) \xrightarrow{\ r\ } O(q) \longrightarrow 1,$$

r being a map defined by $r_x : u \mapsto (-1)^{\partial x} x u x^{-1}$, where $x \in C^\times(q)$ and $u \in V$. In particular, for $C_0^\times(q) = C^\times(q) \cap C_0(q)$ we get another exact sequence

$$1 \longrightarrow k^\times \longrightarrow C_0^\times(q) \xrightarrow{\ r\ } SO(q) \longrightarrow 1.$$

Denote by ι the principal involution on $C(q)$, which preserves the scalars, sums and vectors, and reverses products. Denote by $N : C^\times(q) \longrightarrow k^\times$ the norm given by $N(x) = x\iota(x)$, and by $sp : O(q) \longrightarrow k^\times/2$ the spinor norm given by $sp(T_v) = \overline{q(v)}$. Put $\mathrm{Pin}(q) = \ker(N), \mathrm{Spin}(q) = \mathrm{Pin}(q) \cap C_0^\times(q)$.

Hence, we have the long exact sequences

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(q) \xrightarrow{\ r\ } O(q) \xrightarrow{\ sp\ } k^\times/2$$

and

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(q) \xrightarrow{\ r\ } SO(q) \xrightarrow{\ sp\ } k^\times/2.$$

If we take the separable closure $\bar{k}$ of k, we get the short exact sequences

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\bar{q}) \xrightarrow{\ r\ } O(\bar{q}) \longrightarrow 1 \tag{4}$$

and

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(\bar{q}) \xrightarrow{\ r\ } SO(\bar{q}) \longrightarrow 1. \tag{5}$$

Now, let us recall the definition of Galois twist, which involves the existence of the first cohomological group $H^1(G, \mathcal{G})$, where $\mathcal{G}$ is non abelian group with a G-action. Assume again that (V, q) is a quadratic space over k, and that K/k is a Galois extension with Galois group G. Then we can extend the scalars to get a quadratic space (V_K, q_K). The semi-linear action of G then gives us the equation $q_K(\sigma u) = \sigma q_K(u)$. Conversely, if (W, Q) is a quadratic space over K endowed with a semi-linear action such that $Q(\sigma u) = \sigma Q(u)$ is satisfied, we obtain a quadratic space (W^G, Q^G) over k by taking fixed points and restricting Q. These two operations (scalar extension and fixed points) preserve regularity and are each others inverses. Also, $O(Q)$ is a G-group by conjugation: $(\sigma\varphi)(u) = \sigma\varphi(\sigma^{-1}u)$.

Next, let $f : G \to O(q_K)$ be a crossed homomorphism. Then we can define a semi-linear action by ${}^\sigma u = f_\sigma(\sigma u)$ and get an induced quadratic space $(V_f, q_f) = ((V_K)^G, (q_K)^G)$ over k. Furthermore, if g is equivalent to f, i.e., $g_\sigma = \varphi f_\sigma \sigma \varphi^{-1}$ for some $\varphi \in O(q_K)$, then $V_g = \varphi(V_f)$, and consequently (V_f, q_f) and (V_g, q_g) are equivalent. Hence, to each element in $H^1(G, O(q))$ we can associate an equivalence class of quadratic spaces over k.

The quadratic space (V_f, q_f) is said to arise from (V, q) by taking the *Galois twist* with respect to f.

Define the element

$$\mathrm{hw}(q) = \prod_{i<j} (a_i, a_j) \in \mathrm{Br}(k),$$

where $a_i = q(u_i)$ for some canonical orthogonal basis $u_1, \ldots, u_n$ of q. Clearly, $\mathrm{hw}(q)$ depends only on the equivalence class of q.

Definition 6.1. The element $\mathrm{hw}(q)$ is called the *Hasse-Witt invariant* or the *second Stiefel-Whitney class* of q.

The obstruction now can be calculated by the formula, displayed in the following.

Theorem 6.6. (Fröhlich [6, 18]) *Let L/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/k)$ and assume $G \hookrightarrow O(q)$ for some regular quadratic form q over k. Let $e : \mathrm{Gal}(\overline{k}/k) \to O(q)$ be the induced crossed homomorphism, and let q_e be the Galois twist of q by e. Also, let*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

be the group extension induced by $G \hookrightarrow O(q)$ and the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\overline{q}) \xrightarrow{\ r\ } O(\overline{q}) \longrightarrow 1.$$

Let $K/k = k(\sqrt{a_1}, \ldots, \sqrt{a_r})/k$ be the maximal elementary abelian 2-subextension of L/k, and let $\rho_1, \ldots, \rho_r \in G$ be such that $\rho_i(\sqrt{a_j}) = (-1)^{\delta_{ij}} \cdot \sqrt{a_j}$. Then the obstruction to the embedding problem $(L/k, \widetilde{G}, \mu_2)$ is

$$\mathrm{hw}(q)\mathrm{hw}(q_e)(d, -d_e) \prod_{i=1}^{r} (a_i, sp(\rho_i)) \in \mathrm{Br}(k),$$

where d and d_e are discriminants of q and q_e, respectively.

Next, let L/k be a finite Galois extension with Galois group G, let H be a subgroup of G with fixed field $K = L^H$, and let $\mu : H \hookrightarrow O(q)$ be an orthogonal representation over k. Then, according to [6, 7], we can construct an *induced orthogonal representation* $\mathrm{ind}\mu : G \hookrightarrow O(q_{\mathrm{ind}\mu})$, where $\mathrm{ind}\mu$ has as underlying module the induced G-module of the H-module V_q : $V_{\mathrm{ind}\mu} = \oplus(V_q \otimes \sigma) = V_q \otimes_{kH} kG$, σ running over a given right transversal R of H in G. Note that $V_q \subset V_{\mathrm{ind}\mu}$ is a subspace which is H-invariant. It is not hard to show that, given an orthogonal representation $\mu : H \hookrightarrow O(q)$, such $V_{\mathrm{ind}\mu}$ exists and is unique up to an isomorphism (see e.g. [8, §3.3]). Moreover, the action of G can be explicitly determined: Each element $v \in V_{\mathrm{ind}\mu}$ has a unique expression $v = \sum w_\sigma \otimes \sigma$ for elements w_σ in V_q. For a given $g \in G$, we must have

$$g \cdot (w_\sigma \otimes \sigma) = hw_\sigma \otimes \tau \ \text{ if } g\sigma = \tau h \ (\tau \in R). \tag{6}$$

Next, assume that we have a special orthogonal representation $\mu : H \hookrightarrow SO(q)$ over k. Denote by $\bar{k}$ the separable closure of k, and by $\bar{q}$ the extension of q to $\bar{k}$. Then we have a diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \arrow[r] \arrow[d] & \widetilde{H} \arrow[r] \arrow[d] & H \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mu_2 \arrow[r] & \mathrm{Spin}(\bar{q}) \arrow[r] & SO(\bar{q}) \arrow[r] & 1,
\end{tikzcd}$$

where as usual $\mu_2 = \{\pm 1\}$ and $1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$ is the restriction of $1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(\bar{q}) \longrightarrow SO(\bar{q}) \longrightarrow 1$. The induced orthogonal representation $\mathrm{ind}\mu : G \hookrightarrow O(q_{\mathrm{ind}\mu})$, in its turn, gives us the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \arrow[r] \arrow[d] & \widetilde{G} \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mu_2 \arrow[r] & \mathrm{Pin}(\bar{q}_{\mathrm{ind}\mu}) \arrow[r] & O(\bar{q}_{\mathrm{ind}\mu}) \arrow[r] & 1.
\end{tikzcd}$$

We have the following.

Theorem 6.7. (Michailov [23, Theorem 2.2]) *Let G be a finite group, and let H be a subgroup of G, such that $|H| = 2^t m, (t, m \geq 1)$. Let also $\mu : H \hookrightarrow SO(q)$ be an orthogonal representation over k with an underlying module V_q, such that $n = \dim_k V_q \equiv 0 \pmod 4$. Denote by $\bar{f} \in Z^2(H, \mu_2)$ and by $f \in Z^2(G, \mu_2)$ the 2-cocycles given by the described above group extensions $1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$ and $1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$, respectively. Then $[f] = \mathrm{cor}_{G/H}([\bar{f}])$, where $\mathrm{cor}_{G/H} : H^2(H, \mu_2) \longrightarrow H^2(G, \mu_2)$ is the corestriction map.*

We are going to investigate the case when $q = \langle 1, \ldots, 1 \rangle$. Denote by $e_1, \ldots, e_n$ the standard basis of $V = k^n$. The reflection $T_{e_i - e_j}$ $(i < j)$ has spin norm 2, and as pre-image in $\mathrm{Pin}(\bar{q})$ we can pick $x_{ij} = (e_i - e_j)/\sqrt{2}$. Then x_{ij} has order 2, and if i, j, k, ℓ are four different indices with $i < j$ and $k < l$, then $x_{ij} x_{k\ell}$ has order 4.

The reflection $T_{e_i - e_j}$ interchanges e_i and e_j, leaving the other e_k's invariant. Hence, it is the image of the transposition $(ij) \in S_n$ under the obvious embedding of the symmetric group S_n in $O_n(K)$, and we get a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \arrow[r] \arrow[d] & \widetilde{S}_n \arrow[r] \arrow[d] & S_n \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mu_2 \arrow[r] & \mathrm{Pin}(\bar{q}) \arrow[r] & O(\bar{q}) \arrow[r] & 1,
\end{tikzcd}$$

where $\widetilde{S}_n$ is the pre-image of S_n in $\mathrm{Pin}(\bar{q})$.

Definition 6.2. $\widetilde{S}_n$ is called the *stem cover* (or the *positive double cover*) of S_n, and is characterised as a group extension of S_n by μ_2 such that transpositions lift to elements of order 2, and products of two disjoint transpositions lift to elements of order 4.

Now, let L be the splitting field over k of an irreducible polynomial $f(x) \in k[x]$ of degree n, and let $G = \mathrm{Gal}(L/k)$. Let $\theta = \theta_1, \ldots, \theta_n \in K$ be the roots of $f(x)$, and let $K = k(\theta)$. Then we have an embedding $G \hookrightarrow S_n$, given by $\sigma(i) = j$ when $\sigma(\theta_i) = \theta_j$, and a map $e : \mathrm{Gal}(\overline{k}/k) \to S_n$ induced from $\mathrm{res}_K : \mathrm{Gal}(\overline{k}/k) \to G$. Since the $\mathrm{Gal}(\overline{k}/k)$ action on S_n is trivial, e is a crossed homomorphism. The corresponding twisted Galois action is ${}^{\sigma}(x_i)_i = (\sigma x_{\sigma^{-1}i})_i$, and the fixed points are $(g(\theta_i))_i$ for $d(x) \in K[x]$. The fixed points constitute a field isomorphic to K, and the twisted form of q is $Q_K : x \mapsto \mathrm{Tr}_{K/k}(x^2)$.

Definition 6.3. $Q_K : x \mapsto \mathrm{Tr}_{K/k}(x^2)$ is called the *trace form* of K/k.

To apply Fröhlich result, we must also find the term $\prod_{i=1}(a_i, sp(\rho_i))$. Note that $sp : G \to k^*/k^{*2}$ maps even permutations to 1 and odd permutations to 2. Picking a_1 to be the discriminant $d_{K/k}$ of K/k, we get $\rho_2, \ldots, \rho_r$ to be even, and so the term is simply $(2, d_{K/k})$, i.e., we have

Theorem 6.8. (Serre [43]) *Let L/k be Galois with Galois group G, and let*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1 \tag{7}$$

be the extension obtained as a restriction of the positive double cover

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n \longrightarrow S_n \longrightarrow 1.$$

Then the obstruction to the embedding problem given by L/k and (7) *is*

$$\mathrm{hw}(Q_K) \cdot (2, d_{K/k}) \in \mathrm{Br}(k),$$

where $K = L^{G \cap S_n^{(1)}}, S_n^{(1)} = \{\sigma \in S_n \mid \sigma(1) = 1\}$.

Consider the restriction $1 \to \mu_2 \to \widetilde{A}_n \to A_n \to 1$ of $1 \to \mu_2 \to \widetilde{S}_n \to S_n \to 1$. We have

Theorem 6.9. *Let L/k be Galois with Galois group G, and let*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1 \tag{8}$$

be the extension obtained as a restriction of

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{A}_n \longrightarrow A_n \longrightarrow 1.$$

Then the obstruction to the embedding problem given by L/k and (8) *is*

$$\mathrm{hw}(Q_K) \in \mathrm{Br}(k),$$

where $K = L^{G \cap A_n^{(1)}}, A_n^{(1)} = \{\sigma \in A_n \mid \sigma(1) = 1\}$.

Now, assume again that L/k is a normal and separable extension with a finite Galois group G. We can always find a primitive element θ such that $L = k(\theta)$. Let $f(x) \in k[x]$ be the minimal polynomial of θ of degree $n = [L : k]$, and let $\theta = \theta_1, \theta_2, \ldots, \theta_n$ be the conjugates of θ. Then $G = G(f)$ embeds transitively into the symmetric group S_n.

For a given proper subgroup H of G, we set $m = |H|$ and $\kappa = (G : H) = n/m$. Clearly, θ is a primitive element of the extension L/K as well, where $K = L^H$. Since the minimal polynomial of θ over K divides $f(x)$, we can assume that $\theta = \theta_1, \theta_2, \ldots, \theta_m$ for $1 < m = [L : K] < n$ are the conjugates of θ over K. H embeds transitively in S_m, so we can take the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1, \tag{9}$$

which is the restriction of the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_m \longrightarrow S_m \longrightarrow 1,$$

$\widetilde{S}_m$ being the positive double cover of S_m.

Next, recall that for the quadratic form $q_1 = \langle 1, \ldots, 1 \rangle$ on $V_1 = k^m$ we have that S_m embeds in $O_m(k) = O(q_1)$, so we get an orthogonal representation $H \hookrightarrow O_m(k)$. Set $q = q_1 \perp q_2 \perp \cdots \perp q_\kappa$ and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_\kappa$, where $q_1 = q_2 = \cdots = q_\kappa$ and $V_1 = V_2 = \ldots V_\kappa$. In this way, we get the induced orthogonal representation $G \hookrightarrow O_n(k)$, which is identical to the transitive embedding of $G = G(f)$ in S_n. Now, take the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1, \tag{10}$$

which is the restriction of the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n \longrightarrow S_n \longrightarrow 1.$$

Denote by $\overline{f} \in Z^2(H, \mu_2)$ the 2-cocycle representing (9) and by $f \in Z^2(G, \mu_2)$ the 2-cocycle representing (10), i.e., $\overline{f} = \mathrm{res}(s_m)$ and $f = \mathrm{res}(s_n)$. From Theorem 6.7 now follows that $[f] = \mathrm{cor}_{G/H}([\overline{f}])$, under the extra assumptions $H \hookrightarrow SO_m(k)$ and $m \equiv 0 \pmod 4$.

7 Cohomological invariants

In this section we will present a cohomological approach to invariant theory in the terminology of Serre [9]. First, let us recall two basic concepts of homological algebra - category and functor. In general, a category is an algebraic structure that comprises "objects" that are linked by "arrows". A category has two basic properties: the ability to compose the arrows associatively and the existence of an identity arrow for each object. A simple example is the category of sets, whose objects are sets and whose arrows are functions. One commonly used definition is as follows.

Definition 7.1. A category $\mathcal{C}$ consists of

- a class $\mathrm{ob}(\mathcal{C})$ of objects.
- a class $\hom(\mathcal{C})$ of morphisms, or arrows, or maps, between the objects. Each morphism f has a unique source object a and target object b where a and b are in $\mathrm{ob}(\mathcal{C})$. We write $f : a \mapsto b$.

- for every three objects a, b and c, a binary operation $\hom(a, b) \times \hom(b, c) \mapsto \hom(a, c)$ called composition of morphisms; the composition of $f : a \mapsto b$ and $g : b \mapsto c$ is written as $g \circ f$ or gf.

such that the following axioms hold:

- (associativity) if $f : a \mapsto b, g : b \mapsto c$ and $h : c \mapsto d$ then $h \circ (g \circ f) = (h \circ g) \circ f$,
- (identity) for every object x, there exists a morphism $id_x : x \mapsto x$ called the identity morphism for x, such that for every morphism $f : a \mapsto x$ and every morphism $g : x \mapsto b$, we have $id_x \circ f = f$ and $g \circ id_x = g$.

A functor is a type of mapping between categories, which is applied in category theory. Functors can be thought of as homomorphisms between categories.

Definition 7.2. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A functor F from $\mathcal{C}$ to $\mathcal{D}$ is a mapping that

- associates to each object $X \in \mathcal{C}$ an object $F(X) \in \mathcal{D}$,
- associates to each morphism $f : X \to Y \in \mathcal{C}$ a morphism $F(f) : F(X) \to F(Y) \in \mathcal{D}$ such that the following two conditions hold:
  - $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ for every object $X \in \mathcal{C}$
  - $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f : X \to Y$ and $g : Y \to Z$.

That is, functors must preserve identity morphisms and composition of morphisms.

Now, let us fix a ground field k_0, and consider the category $\mathrm{Fields}_{/k_0}$ of field extensions k of k_0 and two functors

$$A : \mathrm{Fields}_{/k_0} \longrightarrow \mathrm{Sets}$$

and

$$H : \mathrm{Fields}_{/k_0} \longrightarrow \text{Abelian Groups}.$$

Definition 7.3. An H-invariant of A is a morphism of functors $a : A \to H$.

Here, we view H as a functor with values in Sets. Hence, $a : A \to H$ means giving, for every $k \in \mathrm{Fields}_{/k_0}$, a map $a_k : E \mapsto a(E)$ of $A(k)$ into $H(k)$ such that, if $\phi : k \to k'$ is a morphism in $\mathrm{Fields}_{/k_0}$, the diagram

$$\begin{tikzcd}
A(k) \arrow[r, "a_k"] \arrow[d] & H(k) \arrow[d] \\
A(k') \arrow[r, "a_{k'}"] & H(k')
\end{tikzcd}$$

is commutative.

Our aim will be to determine explicitly in some cases the group $\mathrm{Inv}(A, H)$ of all such invariants. If it is necessary to emphasize the role of the base field k_0, we will write $\mathrm{Inv}_{k_0}(A, H)$.

We consider several examples below of the functor A for an extension k of k_0.

Example 7.1. (Étale algebras). Let n be a natural number. We define the functor A by

$$k \mapsto \mathrm{Et}_n(k) = \{\text{isomorphism classes of étale algebras over } k \text{ of rank } n\}.$$

Recall that an étale k-algebra E of rank n is a commutative k-algebra such that $E \cong \prod_i k_i$ for k_i finite separable field extensions of k and $\sum_i [k_i : k] = n$. An equivalent definition is that E is commutative, $[E : k] = n$, and the k-bilinear form defined on E by $(x, y) \mapsto \mathrm{Tr}_E(xy)$ is nondegenerate. The two most important cases are the one where E is a field, and the one where E is split, i.e., isomorphic to $k \times \cdots \times k$.

Example 7.2. (Galois algebras). Let G be a finite group. A G-Galois algebra over k is an étale algebra E with an action of G such that G acts simply transitively on $\mathrm{Hom}(E, k_s)$, where k_s is a separable closure of k. We define the functor A by

$$k \mapsto G - \mathrm{Gal}(k) = \{\text{isomorphism classes of } G\text{-Galois algebras over } k\}.$$

Example 7.3. (Central simple algebras). For $n \geq 1$ we define the functor A by

$$k \mapsto \mathrm{CSA}_n(k) = \{\text{isomorphism classes of central simple algebras of dimension } n^2 \text{ over } k\}.$$

Example 7.4. (Quadratic forms). Let char $k_0 \neq 2$. For $n \geq 1$ we define the functor A by

$$k \mapsto \mathrm{Quad}_n(k) = \{\text{isomorphism classes of nondegenerate quadratic forms over } k \text{ of rank } n\}.$$

We write $\langle \alpha_1, \ldots, \alpha_n \rangle$ for the diagonal quadratic form defined by $\alpha_1, \ldots, \alpha_n$.

Let $\overline{k}$ be an algebraic closure of k, and let k_s be the separable closure of k in$\overline{k}$. Put $\Gamma_k = \mathrm{Gal}(k_s/k) = Aut(\overline{k}/k)$. We give now the main example of the functor H.

Example 7.5. (Abelian Galois cohomology). Let C be a discrete Γ_{k_0}-module. For any extension k/k_0, we have a natural map $\Gamma_k \to \Gamma_{k_0}$ (defined up to inner conjugation), so that the cohomology groups $H^i(\Gamma_k, C), i = 0, 1, \ldots$ make sense. They are denoted by $H^i(k, C)$, and their direct sum is written $H(k, C)$. These groups are functorial in k, i.e., they define functors

$$\mathrm{Fields}_{/k_0} \longrightarrow \text{Abelian Groups}.$$

These will be the functors "H" that we will consider most of the time, and for such H we write $\mathrm{Inv}^i(A, C)$ or $\mathrm{Inv}(A, C)$, instead of $\mathrm{Inv}^i(A, H)$ or $\mathrm{Inv}(A, H)$. We will assume that C is finite and of order not divisible by the characteristic, the principal example being $C = C_2$, the cyclic group of order 2.

Next, we will determine $\mathrm{Inv}(G, C_2)$ for G elementary abelian of type $(2, 2, \ldots, 2)$. We write $H^i(k)$ for $H^i(k, C_2)$ and $H(k)$ for the direct sum of the $H^i(k)$. Thus $H^0(k) = C_2$ and $H^1(k) = k^*/k^{*2}$. For $a \in k^*$, write (a) for the corresponding class in $H^1(k)$, so that $(ab) = (a) + (b)$. The cup product $(a) \cdot (b)$ corresponds (via the usual identification of $H^2(k)$ with a subgroup of the Brauer group $\mathrm{Br}(k)$) to the quaternion algebra (a, b). In partucular, $(a) \cdot (b) = 0$ if and only if the quadratic form $\langle 1, -a, -b \rangle$ represents 0, i.e., b is a norm from the extension $k(\sqrt{a})/k$ or equivalently from the quadratic étale algebra $k[x]/(x^2 - a)$.

Let $G = C_2$. An arbitrary element of $H^1(k, G)$ is given by $\alpha \in k^*/k^{*2}$. Write <u>id</u> for the invariant (i.e., element of $\mathrm{Inv}_{k_0}(C_2, C_2)$) which sends α to $(\alpha) \in H^1(k)$. The cohomology invariant of C_2 is given by the following.

Proposition 7.1. ([9, 16.2, Proposition]) $\mathrm{Inv}_{k_0}(C_2, C_2)$ *is a free* $H(k_0)$*-module with basis* $\{1, \underline{id}\}$.

Now, let $G = C_2 \times \cdots \times C_2$ (n times). An arbitrary element of $H^1(k, G)$ is given by an n-tuple $(\alpha_1, \ldots, \alpha_n) \in k^*/k^{*2} \times \cdots \times k^*/k^{*2}$. For I a subset of $[1, n]$, we write $(a)_I$ for the cup product $\prod_{i \in I}(\alpha_i) \in H(k)$. We have $(\alpha)_\emptyset = 1 \in H^0(k)$. Write a_I for the invariant $(\alpha_1, \ldots, \alpha_n) \mapsto (\alpha)_I$. The cohomology invariant of G is given by the following.

Theorem 7.2. ([9, 16.4, Theorem]) *Let* $G = C_2 \times \cdots \times C_2$ *(n times). Then* $\mathrm{Inv}_{k_0}(G, C_2)$ *is a free* $H(k_0)$*-module with basis* $(a_I)_{I \subset [1,n]}$.

Next, we determine $\mathrm{Inv}(\mathrm{Quad}_n, C_2)$.

Definition 7.4. If q is a quadratic form of rank n over k, we may write it as $q = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ for $\alpha_i \in k^*$. Let $w_i(q)$ be the i-th elementary symmetric polynomial in the (α_j)'s computed in the commutative ring $H(k)$:

$$\begin{aligned}
w_0 &= 1, \\
w_1 &= \sum_i (\alpha_i) = (\alpha_2 \alpha_2 \cdots \alpha_n) = (d(q)), \\
w_2 &= \sum_{i<j} (\alpha_i) \cdot (\alpha_j), \\
&\vdots \\
w_n &= (\alpha_1) \cdot (\alpha_2) \cdots (\alpha_n), \\
w_i &= 0 \text{ if } i < 0 \text{ or } i > n.
\end{aligned}$$

$w_i(q)$ is called the i-th Stiefel-Whitney class.

It is known that these are indeed invariants of q, i.e., they do not depend on the particular way of writing q as $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$. They provide $n + 1$ elements in $\mathrm{Inv}(\mathrm{Quad}_n, C_2)$.

Definition 7.5. We write $w(q)$ for the total Stiefel-Whitney class

$$w(q) = \sum_{i=0}^{n} w_i(q) \in H(k).$$

It is characterized by the properties

1. $w(\langle \alpha \rangle) = 1 + (\alpha)$
2. $w(q \oplus q') = w(q) \cdot w(q')$.

The cohomology invariant of Quad_n is given by the following.

Theorem 7.3. ([9, 17.3, Theorem]) *The group* $\mathrm{Inv}(\mathrm{Quad}_n, C_2)$ *is a free* $H(k_0)$*-module with basis* $\{w_0, w_1, \ldots, w_n\}$.

In the remaining of this section we will describe the cohomological invariants of Et_n.

We have obvious embeddings $S_n \hookrightarrow O_n \hookrightarrow \mathrm{GL}_n$, where O_n and GL_n are endowed with the usual topology. Let B_{O_n} and B_{S_n} be the "classifying spaces" of O_n and S_n, cf. [2, §8]. The map $B_{S_n} \to B_{O_n}$ defines a map of singular cohomology groups

$$H(B_{O_n}, C_2) \to H(B_{S_n}, C_2).$$

Since S_n is discrete, the cohomology of S_n (in the algebraic sense of the word) is the same as the (topological) cohomology of the classifying space B_{S_n}; that is we have the identity $H(B_{S_n}, C_2) = H(S_n, C_2)$. Thus any element of $H(B_{O_n}, C_2)$ defines a corresponding element of $H(B_{S_n}, C_2) = H(S_n, C_2)$. In particular, the Stiefel-Whitney classes $w_1, \dots, w_n$ of $H(B_{O_n}, C_2)$ define elements of $H(S_n, C_2)$ which we will again denote by $w_1, \dots, w_n$.

Definition 7.6. The associated elements of $\mathrm{Inv}(\mathrm{Et}_n, C_2)$ are called Galois Stiefel-Whitney classes and are denoted by $w_i^{\mathrm{gal}}(E)$ (or just w_i^{gal}).

Recall that if $E \in \mathrm{Et}_n(k)$, its trace form q_E is the quadratic form on E defined by $q_E(x) = \mathrm{Tr}_{E/k}(x^2)$. This gives a morphism $\mathrm{Et}_n \to \mathrm{Quad}_n$. The Stiefel-Whitney invariants of Quad_n thus define cohomological invariants w_i on Et_n by $w_i(E) = w_i(q_E)$. The relation between w_i and w_i^{gal} is given by the following.

Theorem 7.4. (Kahn [12]) *For $E \in \mathrm{Et}_n(k)$,*

$$w_i^{\mathrm{gal}} = \begin{cases} w_i(q_E) & \text{if } i \text{ is odd} \\ w_i(q_E) + (2) \cdot w_{i-1} & \text{if } i \text{ is even} \end{cases}$$

in $H(k, C_2)$.

Example 7.6. $w_1 \in H^1(S_n, C_2) = \mathrm{Hom}(S_n, C_2)$ is the sign homomorphism, and w_1^{gal} is the discriminant. $w_2 \in H^2(S_n, C_2)$ determines the positive double cover $\widetilde{S}_n$ of S_n (see definition 6.2). $w_2^{\mathrm{gal}} = w_2 + (2) \cdot w_1^{\mathrm{gal}}$ is the obstruction to the embedding problem related to the group extension (7) (from theorem 6.8).

Let $m = [n/2]$, the integral part of $n/2$, and let $H = C_2 \times \cdots \times C_2$ (m copies). We identify H with the subgroup of S_n generated by the m transpositions $(12), (34), \dots$. By [9, Theorem 24.11] the restriction map

$$\mathrm{Inv}_{k_0}(\mathrm{Et}_n, C_2) = \mathrm{Inv}_{k_0}(S_n, C_2) \to \mathrm{Inv}_{k_0}(H, C_2)$$

is injective. Moreover, by [9, 13.2], its image lies in the subgroup $\mathrm{Inv}_{k_0}(H, C_2)^{S_n}$ of $\mathrm{Inv}_{k_0}(H, C_2)$ fixed by the action of the symmetric group S_n (acting on H by permuting the factors). The cohomology invariant of Et_n is given by the following.

Theorem 7.5. ([9, Theorem 25.6])

(1) *The map* $\mathrm{res} : \mathrm{Inv}_{k_0}(\mathrm{Et}_n, C_2) \to \mathrm{Inv}_{k_0}(H, C_2)^{S_n}$ *is an isomorphism.*

(2) *The $H(k_0)$-module* $\mathrm{Inv}_{k_0}(\mathrm{Et}_n, C_2)$ *is free with basis* $\{1, w_1^{\mathrm{gal}}, \dots, w_m^{\mathrm{gal}}\}$*, where $m = [n/2]$.*

(3) $w_i^{\mathrm{gal}} = 0$ *for $i > m$.*

8 Noether's problem revisited

Noether's problem can be formulated also thus:

Definition 8.1. $\mathrm{Noe}(G/k_0)$ - There exists an embedding $\rho : G \to \mathrm{GL}_n(k_0)$ such that, if K_ρ is the subfield of $k_0(X_1, \dots, X_n)$ fixed by G, then K_ρ is k_0-rational.

Consider a finitely generated extension K/k_0; let C be a finite Γ_{k_0}-module.

Definition 8.2. An element $a \in H(K, C)$ is said to be unramified over k_0 if, for every discrete valuation v of K which is trivial on k_0, the residue of a at v is 0.

Definition 8.3. There is a natural embedding $H(k_0) \to \mathrm{Inv}_{k_0}(A, H)$; namely, if $h \in H(k_0)$, we define the invariant a_h by setting $a_h(x) =$ image of h in $H(k)$ for every $x \in A(k)$. Such an invariant is called constant. Suppose we have fixed a base point for A. We say that a is normalized if a vanishes on the base point.

Every invariant can be written in a unique way as (constant) + (normalized).

Proposition 8.1. ([9, Prop. 33.7]) *If K/k_0 is rational, every unramified cohomology class in $H(K, C)$ is constant, i.e., belongs to $H(k_0, C)$.*

Proposition 8.2. ([9, Prop. 33.10]) *If $a \in \mathrm{Inv}_{k_0}(G, C)$ is unramified over k_0, and if* $\mathrm{Noe}(G/k_0)$ *is true, then a is constant.*

Corollary 8.3. ([9, Corol. 33.10]) *Suppose that* $\mathrm{Noe}(G/k_0)$ *is true and that a is normalized and unramified. Then $a = 0$.*

Remark. Instead of the assumption $\mathrm{Noe}(G/k_0)$ is true in the latter two results, we may assume that $\mathrm{Rat}(G/k_0)$ is true, where $\mathrm{Rat}(G/k_0)$ is a weaker condition, defined in [9, 33.1] with the help of versal torsors.

We can apply corollary 8.3 in this way: we construct a non-zero cohomological invariant a which is unramified and normalized. By corollary 8.3, this will show that Noether's problem has a negative solution for G over k_0.

Example 8.1. Let $G = C_{2^m}$, the cyclic group of order 2^m for $m \geq 3$. Every $x \in H^1(k, G)$ defines by reduction mod 2 an element $d(x)$ of $H^1(k, C_2) = H^1(k)$. Put

$$b(x) = (2) \cdot d(x) \in H^2(k).$$

This defines an invariant $b \in \mathrm{Inv}_{k_0}(G, C_2)$.

Proposition 8.4. ([9, Prop. 33.15]) *The invariant b defined above is unramified and normalized. If the ground field is $\mathbb{Q}$, this invariant is not* 0*.*

Corollary 8.5. ([9, Theorem 33.16]) *Let G be a group with a 2-Sylow subgroup which is cyclic of order ≥ 8. Then* $\mathrm{Noe}(G/k_0)$ *is false.*

Moreover, we have

Theorem 8.6. ([9, Theorem 34.7]) *Let G be a group with a 2-Sylow subgroup which is isomorphic to the quaternion group Q_{16} of order 16. Then* $\mathrm{Noe}(G/\mathbb{Q})$ *is false.*

Next, we will consider the groups $\widetilde{A}_n$, where $1 \to \mu_2 \to \widetilde{A}_n \to A_n \to 1$ is the restriction of $1 \to \mu_2 \to \widetilde{S}_n \to S_n \to 1$. Take an étale algebra E of rank n over a field k, and let $\varphi_E : \Gamma_k \to S_n$ be the corresponding homomorphism. Let $w_i(E)$ be the Stiefel-Whitney classes of the trace form q_W. By [9, 25.3,25.10] we have that the image of φ_E is contained in A_n if and only if $w_1(E) = 0$. Suppose that the image of φ_E is contained in A_n. The homomorphism $\varphi_E : \Gamma_k \to S_n$ can be lifted to $\widetilde{A}_n$ if and only if $w_2(E) = 0$ (this follows from theorem 6.9 for $G = A_n$).

Set $n = 6$ or 7, let t be an element of $H^1(k, \widetilde{A}_n)$, and let $E(t)$ in $\mathrm{Et}_n(k)$ be the corresponding étale algebra. According to [9, 33.23], the trace form of $E(t)$ is of the form

$$\langle 1, 1, c, c, c, c\rangle \text{ (for } n = 6) \quad \text{or} \quad \langle 1, 1, 1, c, c, c, c\rangle \text{ (for } n = 7)$$

for a suitable $c \in k^*$. Moreover, the element $(c) \cdot (-1) \cdot (-1) \in H^3(k)$ does not depend on the choice of c. Let us denote it by $e(t)$. We may view e as a cohomological invariant

$$e : H^1(k, \widetilde{A}_n) \to H^3(k).$$

Proposition 8.7. ([9, Prop. 33.24]) *The invariant e defined above is unramified and normalized. If the ground field is $\mathbb{Q}$, this invariant is not* 0.

Corollary 8.8. ([9, Theorem 33.25]) *Noether's problem has a negative solution for $\widetilde{A}_6$ and $\widetilde{A}_7$ over $\mathbb{Q}$.*

Corollary 8.9. ([9, Theorem 33.26]) *Noether's problem has a negative solution for any subgroup G of odd index of $\widetilde{A}_7$ over $\mathbb{Q}$.*

Example 8.2. Among the subgroups of odd index of $\widetilde{A}_7$, there are the following

$$\mathrm{SL}_2(\mathbb{F}_9) = \widetilde{A}_6,\ \mathrm{SL}_2(\mathbb{F}_7),\ Q_{16},\ \widehat{S}_4,\ \widehat{S}_5.$$

Here $\widehat{S}_n$ (the negative double cover of S_n) denotes the unique central extension of S_n by μ_2 in which the transpositions and the product of two disjoint transpositions lift as elements of order 4. This is not the same as $\widetilde{S}_n$ (the positive double cover of S_n).

Remark. The strategy we used so far is essentially due to Saltman and Bogomolov. However, there is a difference: the invariants we used come from the properties of the trace form; Saltman and Bogomolov uded a cohomological invariant that we will discuss in what follows.

Saltman [38] found examples of groups G of order p^9 such that $\mathbb{C}(V)^G$ is not stably rational over $\mathbb{C}$. His main method was an application of the unramified cohomology group $H^2_{nr}(\mathbb{C}(V)^G, \mathbb{Q}/\mathbb{Z})$ as an obstruction. Bogomolov [1] proved that $H^2_{nr}(\mathbb{C}(V)^G, \mathbb{Q}/\mathbb{Z})$ is canonically isomorphic to

$$B_0(G) = \bigcap_A \ker\{\mathrm{res}^A_G : H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(A, \mathbb{Q}/\mathbb{Z})\}$$

where A runs over all the bicyclic subgroups of G (a group A is called bicyclic if A is either a cyclic group or a direct product of two cyclic groups).

Definition 8.4. The group $B_0(G)$ is a subgroup of the Schur multiplier $H^2(G, \mathbb{Q}/\mathbb{Z})$, and is called the *Bogomolov multiplier* of G.

According to [38] the vanishing of the Bogomolov multiplier is an obstruction to Noether's problem, that is if $B_0(G) \neq 0$, then $\mathrm{Noe}(G/\mathbb{C})$ is false.

While the non-zero unramified invariants were used so far to give a negative answer to Noether's problem, surprisingly there are some examples of zero invariants giving a positive answer to Noether's problem. This invariants are the obstructioins to some embedding problems, which we are going to describe.

Let $\mathrm{Br}(K)$ denote the Brauer group of a field K, and $\mathrm{Br}_N(K)$ its N-torsion subgroup for any $N > 1$. Following Roquette [36], if $\gamma = [B] \in \mathrm{Br}(K)$ is the class of a K-central simple algebra B and $m \geq 1$ is a multiple of the index of B, then $F_m(\gamma)$ denotes the m-th Brauer field of γ. Moreover, $F_m(\gamma)/K$ is a regular extension of transcedence degree $m-1$, which is rational if and only if γ is trivial. The following result was essentially obtained by Saltman in [39, p. 541] and proved in detail by B. Plans [34, Prop. 7].

Theorem 8.10. (Saltman, Roquette, Plans) *Let $1 \to C \to H \to G \to 1$ be a central extension of finite groups, representing an element $\varepsilon \in H^2(G, C)$. Let K be an infinite field and let N denote the exponent of C. Assume that N is prime to the characteristic of K and that K contains μ_N – the group of N-th roots of unity. Let be given a decomposition $C \cong \mu_{N_1} \times \cdots \times \mu_{N_r}$, and let the corresponding isomorphism $H^2(G, C) \cong \oplus_i H^2(G, \mu_{N_i})$ map ε to $(\varepsilon)_i$. Let also be given a faithful subrepresentation V of the regular representation of G over K, and let $\gamma_i \in \mathrm{Br}_N(K(V)^G) \subset \mathrm{Br}(K(V)^G)$ be the inflation of ε_i with respect to the isomorphism $G \cong \mathrm{Gal}(K(V)/K(V)^G)$. Then*

$$K(H) \textit{ is rational over the } K(V)^G - \textit{ free compositum } F_m(\gamma_1)\cdots F_m(\gamma_r),$$

where m denotes the order of G.

Michailov proved the following applications of the latter theorem.

Theorem 8.11. ([24, Theorem 2.7]) *Let p be a prime, let F be an infinite field with characteristic not p, and let F contain all pth roots of unity. Let $1 \to \mu_p \to H \to G \to 1$ be a non-split central extension of finite groups, representing an element $\varepsilon \in H^2(G, \mu_p)$. Let $L = K(x_g : g \in G)$ be the rational function field with a G-action given by the regular representation of G over K. Assume that the embedding problem given by $L/K(G)$ and the group extension $1 \to \mu_p \to H \to G \to 1$ is solvable. Then $K(H)$ is rational over $K(G)$.*

Proof. Note that the obstruction $i(\gamma) = \inf(\varepsilon) \in \mathrm{Br}_p(K(G))$ is isomorphic to the crossed product algebra $[L, G, \varepsilon]$, which is split in $\mathrm{Br}_p(K(V)^G)$, since the embedding problem is solvable. Hence $F_m(\gamma)$ is rational over $K(G)$, so Theorem 8.10 implies our result. □

Theorem 8.12. ([24, Theorem 5.1]) *Let H be a non-abelian group of order $8n$, having a cyclic subgroup of order $4n$ for any $n \geq 2$, and let $1 \to \mu_2 \to G \to H \to 1$ be a group extension such that G does not have a cyclic subgroup of index 2. Assume that K is a field which contains a primitive $4n$-th root of unity ζ. Then $K(G)$ is rational over K.*

Let us consider the following groups.

$$D_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle - \text{the dihedral group},$$
$$SD_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = \tau^2 = 1, \tau\sigma = \sigma^{2n-1}\tau \rangle - \text{the semidihedral group},$$
$$Q_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = 1, \tau^2 = \sigma^{2n}, \tau\sigma = \sigma^{-1}\tau \rangle - \text{the quaternion group}.$$

Next, we describe the cohomology groups $H^2(H,\mu_2)$ for H being isomorphic to any of the groups D_{8n}, SD_{8n} and Q_{8n}.

I.1) Let $H \cong D_{8n}$.

We have the following non-equivalent exact sequences:

$$1 \to \mu_2 \to G \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} D_{8n} \to 1,$$

where the generators σ and τ of G have relations: $\sigma^{4n} = \varepsilon_1, \tau^2 = \varepsilon_2, \tau\sigma = \varepsilon_3\sigma^{-1}\tau$ for $\varepsilon_i = \pm 1$. The existence of the group G for any choice of ε_i is easily verified. Therefore, $H^2(D_{8n},\mu_2) \cong \mu_2^3$ and all non-split sequences give us 6 non-isomorphic groups:

$$\begin{aligned}
&G_1 \cong D_{16n}, G_2 \cong SD_{16n}, G_3 \cong Q_{16n},\\
&G_4 = \langle \sigma,\tau,\rho \mid \sigma^{4n} = 1, \tau^2 = \rho - \text{central}, \rho^2 = 1, \tau\sigma = \sigma^{-1}\tau\rangle,\\
&G_5 = \langle \sigma,\tau,\rho \mid \sigma^{4n} = 1, \tau^2 = \rho - \text{central}, \rho^2 = 1, \tau\sigma = \sigma^{-1}\tau\rho\rangle,\\
&G_6 = \langle \sigma,\tau,\rho \mid \sigma^{4n} = 1, \tau^2 = 1, \rho^2 = 1, \rho - \text{central}, \tau\sigma = \sigma^{-1}\tau\rho\rangle.
\end{aligned}$$

I.2) Let $H \cong SD_{8n}$.

We have the following non-equivalent exact sequences:

$$1 \to \mu_2 \to G \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} SD_{8n} \to 1,$$

where the generators σ and τ of G have relations: $\sigma^{4n} = 1, \tau^2 = \varepsilon_2, \tau\sigma = \varepsilon_3\sigma^{2n-1}\tau$ for $\varepsilon_i = \pm 1$ $(2 \le i \le 3)$. There is no group extension for $\varepsilon_1 = -1$. Therefore, $H^2(SD_{8n},\mu_2) \cong \mu_2^2$ and all non-split sequences give us 3 non-isomorphic groups:

$$\begin{aligned}
&G_7 = \langle \sigma,\tau,\rho \mid \sigma^{4n} = 1, \tau^2 = \rho - \text{central}, \rho^2 = 1, \tau\sigma = \sigma^{2n-1}\tau\rangle,\\
&G_8 = \langle \sigma,\tau,\rho \mid \sigma^{4n} = 1, \tau^2 = \rho - \text{central}, \rho^2 = 1, \tau\sigma = \sigma^{2n-1}\tau\rho\rangle,\\
&G_9 = \langle \sigma,\tau,\rho \mid \sigma^{4n} = 1, \tau^2 = 1, \rho^2 = 1, \rho - \text{central}, \tau\sigma = \sigma^{2n-1}\tau\rho\rangle.
\end{aligned}$$

Now, let H be isomorphic to D_{8n} or SD_{8n} and let L/F be a H-extension. Then L/F contains a biquadratic extension $K/F = F(\sqrt{a},\sqrt{b})/F$, such that the generators σ and τ of H act in the following way:

$$\begin{aligned}
\sigma &: \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto \sqrt{b},\\
\tau &: \sqrt{a} \mapsto \sqrt{a}, \sqrt{b} \mapsto -\sqrt{b}.
\end{aligned}$$

In [23] and [50] the reader can find two different approaches for the calculation of the obstructions displayed in the following three propositions.

Proposition 8.13. (Ziapkov [50, Th. 2.1]) *Let F be a field with char$(F) \neq 2$, let H be isomorphic to D_{8n} or SD_{8n} and let L/F be a H-extension containing a biquadratic extension $K/F = F(\sqrt{a},\sqrt{b})/F$. Then the obstruction to the embedding problem given by L/F and the group extension*

$$1 \to \mu_2 \to G_i \to H \to 1$$

for $i = 4$ and $i = 7$ is $(b,-1) \in \mathrm{Br}(F)$.

Proposition 8.14. (Ziapkov [50, Th. 2.2]) *Let F be a field with char$(F) \neq 2$, let H be isomorphic to D_{8n} or SD_{8n} and let L/F be a H-extension containing a biquadratic extension $K/F = F(\sqrt{a}, \sqrt{b})/F$. Then the obstruction to the embedding problem given by L/F and the group extension*

$$1 \to \mu_2 \to G_i \to H \to 1$$

for $i = 6$ and $i = 9$ is $(a, -1) \in \mathrm{Br}(F)$.

Proposition 8.15. (Ziapkov [50, Th. 2.3])*Let F be a field with char$(F) \neq 2$, let H be isomorphic to D_{8n} or SD_{8n} and let L/F be a H-extension containing a biquadratic extension $K/F = F(\sqrt{a}, \sqrt{b})/F$. Then the obstruction to the embedding problem given by L/F and the group extension*

$$1 \to \mu_2 \to G_i \to H \to 1$$

for $i = 5$ and $i = 8$ is $(ab, -1) \in \mathrm{Br}(F)$.

Next, we are going to prove the following.

Theorem 8.16. (Michailov [24, Theorem 5.5]) *Assume that K is an infinite field with char$(K) \neq 2$, which contains a primitive $2n$-th root of unity ζ for some n- even. Then $K(G_i)$ is rational over K for any $i = 4, 5, 6, 7, 8, 9$.*

Proof. Let H be isomorphic to D_{8n} or SD_{8n} and let $L/F = K(x_h : h \in H)/K(H)$ be the H-extension obtained by the rational function field $K(x_h : h \in H)$. From Propositions 8.13,8.14 and 8.15 then follows that the obstruction to the embedding problem given by L/F and $1 \to \mu_2 \to G_i \to H \to 1$ is $(*, -1) \in \mathrm{Br}(K(H))$. Note that K has a fourth root of unity (n is even), so the obstruction $(*, -1)$ is always split. Then Theorem 8.11 implies the rationality of $K(G_i)$, since $K(H)$ is rational, as is well known. □

9 Linear codes

Invariant theory and in particular automorphisms of finite fields play an important role in coding theory. A linear code is a linear subspace $C \subseteq \mathbb{F}_q^n$, where F_q is the field of q elements. The number n is called the length of the code. In the following, we will only consider binary codes, that is, $q = 2$. The weight $w(u)$ of a word $u \in \mathbb{F}_2^n$ is the number of nonzero positions in u, that is, $w(u) := |\{i \mid u_i = 1\}|$. The Hamming distance $d(u, v)$ between two words is defined as the number of positions in which u and v, differ: $d(u, v) = w(u - v)$.

A code $C \subseteq \mathbb{F}_2^n$ is called an $[n, k, d]$-code if the dimension of C is equal to k and the smallest Hamming distance between two distinct codewords is equal to d. In the setting of error correcting codes, messages are transmitted using words from the set of $2k$ codewords. If at most $(d - 1)/2$ errors are introduced (by noise) into a codeword, the original can still be recovered by finding the word in C at minimum distance from the distorted word. The higher d, the more errors can be corrected and the higher k, the higher the information rate.

Much information about a code, including the parameters d and k, can be read of from its weight enumerator W_C. This is the polynomial in x, y and homogeneous of degree n, defined by

$$W_C(x, y) := \sum_{i=0}^{n} A_i y^i x^{n-i}, \quad A_i := |\{u \in C \mid w(u) = i\}|.$$

Observe that the coefficient of x_n in W_C is always equal to 1, since C contains the zero word. The number $2k$ of codewords equals the sum of the coefficients $A_0, \dots, A_n$ and d is the smallest positive index i for which $A_i > 0$.

For a code $C \subseteq \mathbb{F}_2^n$, the dual code $C^\perp$ is defined by

$$C^\perp := \{u \in \mathbb{F}_2^n \mid u \cdot c = 0 \text{ for all } c \in C\}, \quad \text{where } u \cdot c := u_1c_1 + \cdots u_nc_n.$$

Clearly, the sum of dimensions of a code C and its dual $C^\perp$ equals n.

The MacWilliams identity relates the weight enumerator of a code C and that of its dual $C^\perp$.

Proposition 9.1. *Let $C \subseteq \mathbb{F}_2^n$ be a code. The weight enumerator of $C^\perp$ satisfies*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y).$$

A code is called self-dual if $C = C^\perp$. This implies that n is even and the dimension of C equals $n/2$. Furhermore, we have for every $c \in C$ that $c \cdot c = 0$ so that $w(c)$ is even. If every word in C has weight divisible by 4, the code is called even (or sometimes doubly even).

Next, Let $W = \oplus_{d=0}^{\infty} W_d$ be a direct sum of finite dimensional (complex) vector spaces W_d. The Hilbert series (or Poincaré series) $H(W,t)$ is the formal power series in t defined by

$$H(W,t) := \sum_{d=0}^{\infty} \dim(W_d) t^d,$$

and encodes in a convenient way the dimensions of the vector spaces W_d. In this section, W will usually be the vector space $\mathbb{C}[V]^G$ of polynomial invariants with respect to the action of a group G, where W_d is the subspace of invariants homogeneous of degree d. For finite groups G, it is possible to compute the Hilbert series directly, without prior knowledge about the generators. This is captured in the following theorem of Molien.

Theorem 9.2. (Molien) *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a finite group on a finite dimensional vector space V. Then the Hilbert series is given by*

$$H(\mathbb{C}[V]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - \rho(g)t)}.$$

Consider an even, self-dual code C. Then its weight enumerator must satisfy

$$W_C(x,y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right), \quad W_C(x,y) = W_C(x, iy).$$

This means that W_C is invariant under the group G generated by the matrices

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

a group of 192 elements.

What can we say about the invariant ring $\mathbb{C}[x,y]^G$? Using Molien's theorem, we can find the Hilbert series:

$$H(\mathbb{C}[x,y]^G, t) = \frac{1}{(1-t^8)(1-t^{24})}.$$

This suggests that the invariant ring is generated by two algebraically independent polynomials f_1, f_2 homogeneous of degrees 8 and 24 respectively. This is indeed the case, just take $f_1 = x^8 + 14x^4y^4 + y^8$ and $f_2 = x^4y^4(x^4 - y^4)^4$. So the invariant ring is generated by f_1 and f_2, which implies the following powerful theorem on the weight enumerators of even self-dual codes.

Theorem 9.3. (Gleason) *The weight enumerator of an even self-dual code is a polynomial in* $x^8 + 14x^4y^4 + y^8$ *and* $x^4y^4(x^4 - y^4)^4$.

For more information about the weight enumerator, automorphisms and related topics we refer the reader to [51, 31].

We conclude this section with an interesting application of Clifford algebras and orthogonal groups in coding theory found by J. Wood. He showed that there is an equivalence of self-dual codes and abelian subgroups of $\widetilde{V} \subseteq \mathrm{Spin}(n)$. Let $V' = V'(n) = \{\text{diagonal matrices in } O(n)\}$, with basis $v_1, v_2, \ldots, v_n$, where $v_i = v_{\{i\}}$ is the diagonal matrix with -1 in position i, 1's elsewhere on the diagonal. The dot product is defined with respect to this basis. $V' \cong (\mathbb{Z}/2)^n$ is an n-dimensional vector space over $\mathbb{Z}/2 = \mathbb{F}_2$, and $V \subseteq V'$.

Theorem 9.4. (Wood [49, Theorem 2.1]))

(1) *There is a* $1-1$ *correspondence between the abelian subgroups of* $\widetilde{V} \subseteq \mathrm{Spin}(n)$ *which contain* -1 *and the self-dual binary linear codes in* $V'(n)$.

(2) *There is a* $1-1$ *correspondence between the elementary abelian* 2*-subgroups of* $\widetilde{V} \subseteq \mathrm{Spin}(n)$ *which contain* -1 *and the even self-dual binary linear codes in* $V'(n)$.

10 Shape invariants of space curves

The direct similarities of the Euclidean space $\mathbb{R}^3$ preserve the orientation and the angles. Geometric objects in $\mathbb{R}^3$ like triangles and tetrahedra have a natural description with respect to the group of direct similarities by measures of two and four angles. It is well-known that a regular space curve with nonzero curvarure, so called a Frenet space curve, is determined up to a Euclidean motion of $\mathbb{R}^3$ by its curvature and torsion (see [10, Ch. 7]). For a Frenet space curve we introduce a shape as an ordered pair of two invariants called a shape curvature and a shape torsion. The use of a spherical arc-length parameter plays a key role in these considerations.

Definition 10.1. ([5]) Let $\boldsymbol{c} : \mathrm{I} \longrightarrow \mathbb{R}^3$ be a Frenet space curve of the class C^3 parameterized by a spherical arc length parameter σ. Let $\kappa_1(\sigma)$ and $\kappa_2(\sigma)$ be the curvature and the torsion of $\boldsymbol{c}$, respectively. The functions $\widetilde{\kappa}_1 = -\frac{d\kappa_1}{\kappa_1 d\sigma}$ and $\widetilde{\kappa}_2 = \frac{\kappa_2}{\kappa_1}$ are called shape curvature and shape torsion of $\boldsymbol{c}$. The ordered pair $(\widetilde{\kappa}_1, \widetilde{\kappa}_2)$ is called a (local) shape of the curve $\boldsymbol{c}$.

The definition of the "shape curvature" in terms of a spherical arc length parameter suggests to recognize the curve from its "shape data". Two Frenet curves with the same torsion and the same always positive curvature are equivalent modulo a Euclidean motion. This statement can be extended for the Frenet curves with the same shape curvature and shape torsion.

Encheva and Georgiev obtained an analog of the fundamental theorem of space curves.

Theorem 10.1. (Encheva, Georgiev [5]) *Let* $f_i : \mathrm{I} \longrightarrow \mathbb{R}$, $i = 1, 2$ *be two functions of class* C^1. *Modulo a direct similarity of* $\mathbb{R}^3$, *there exists a unique Frenet curve with the shape curvature* f_1 *and the shape torsion* f_2.

Let $\boldsymbol{c} : \mathrm{I} \longrightarrow \mathbb{R}^3$ be a Frenet curve of class C^3 defined in an open interval $\mathrm{I} \subset \mathbb{R}$ and parameterized by a spherical arc length parameter σ. Then, the shape of $\boldsymbol{c}$ is the pair $(\widetilde{k}_1(\sigma),\, \widetilde{k}_2(\sigma))$, where $\widetilde{k}_i : \mathrm{I} \longrightarrow \mathbb{R}\ \ (i = 1,\, 2)$ are functions of class C^1. From Theorem 10.1 we have that the curve $\boldsymbol{c}$ is determined uniquely by its shape up to a direct similarity of the Euclidean space. We shall construct space curves with given shape. First we fix a right - handed orthonormal triad of vectors $\boldsymbol{e}_1^0,\ \boldsymbol{e}_2^0,\ \boldsymbol{e}_3^0$. The unique solution of the system of differential equations

$$\frac{d\boldsymbol{\gamma}}{d\sigma} = \boldsymbol{t}(\sigma), \qquad \frac{d\boldsymbol{t}}{d\sigma} = -\boldsymbol{\gamma}(\sigma) + \widetilde{k}_2(\sigma)\boldsymbol{p}(\sigma), \qquad \frac{d\boldsymbol{p}}{d\sigma} = -\widetilde{k}_2(\sigma)\boldsymbol{t}(\sigma) \tag{11}$$

with initial conditions $\boldsymbol{e}_1^0,\ \boldsymbol{e}_2^0,\ \boldsymbol{e}_3^0$, determine a spherical curve $\boldsymbol{\gamma} = \boldsymbol{\gamma}(\sigma)$ such that $\boldsymbol{\gamma}(\sigma_0) = \boldsymbol{e}_1^0$ for some $\sigma_0 \in \mathrm{I}$. Let $\mu(\sigma) = \int_{\sigma_1}^{\sigma} \widetilde{k}_1(\sigma)\, d\sigma$ for fixed $\sigma_1 \in \mathrm{I}$. We find that the curve

$$\boldsymbol{c}(\sigma) = \boldsymbol{c}_0 + \int_{\sigma_0}^{\sigma} e^{\mu(\sigma)}\boldsymbol{\gamma}(\sigma)\, d\sigma \tag{12}$$

has a shape $(\widetilde{k}_1(\sigma),\, \widetilde{k}_2(\sigma))$ and passes through a point $\boldsymbol{c}_0 = \boldsymbol{c}(\sigma_0)$. In simple cases the system (11) and the equation (12) can be solved explicitly, but in the general case only a numerical solution is possible.

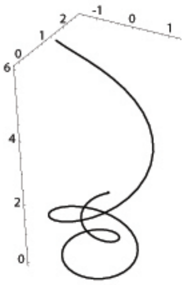

Figure 2.

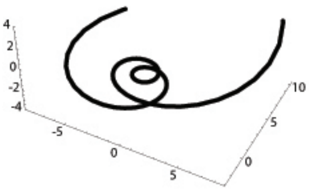

Figure 3.

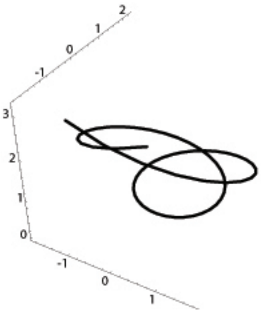

Figure 4.

A lot of computer programmes can be used effectively to determine numerically a space curve with a given shape and then to construct it. The above figure illustrate space curves with shapes $(b,\, a\sigma)$(see Fig. 2.), $(b\sigma,\, a)$(see Fig. 3.) and $(b\sigma, a\sigma)$(see Fig. 4.), where $a,\, b$ are nonzero real constants.

11 Möbius invariants

Let $S^2 :\ (x^1)^2 + (x^2)^2 + (x^3)^2 = 1$ be the unit sphere in $\mathbb{R}^3$, centered at the origin O and $\mathbf{l}(x^1, x^2, x^3),\ x^1 \neq 1$ be the position vector of an arbitrary point in S^2, different from the pole $P(1, 0, 0)$.

The group of rigid motions on the sphere S^2 coincides with the group of rotations $SO(3)$ in $\mathbb{R}^3$ that preserve the sphere S^2. This group induces on the plane via the stereographic projection π a subgroup F_0 of the Möbius group Möb(2). We identify $\mathbb{R}^2 \cong C$, where C is the field of complex numbers, and denote $C \cup \infty$ by C_∞.

The elements of the subgroup $F_0 \subset M\ddot{o}b(2)$ corresponding of the group $SO(3)$ of rotations on the sphere S^2 via the stereographic projection π are the following transformations:

a) rotations in C, represented by the equation $f(z) = a.z,\ \|a\| = 1, a,\ z \in C$;

b) möbius transformations in C_∞, represented by the equation
$$f(z) = \frac{a.z + b}{-\bar{b}.z + \bar{a}},\ \|a\|^2 + \|b\|^2 = 1, a,\ b,\ z \in C,\ b \neq 0.$$

Definition 11.1. ([3]) Let $c : \mathbf{u} = \mathbf{u}(\sigma)$ be a Frenet plane curve, parameterized by an arc length parameter σ of the spherical image $\gamma = \pi^{-1}(c)$, where π^{-1} is the reverse stereographic projection $\pi^{-1} : \mathbb{R}^2 \to S^2 \setminus \{P\}$. We denote by $\mathfrak{M} = \mathfrak{M}(\sigma)$ the function

$$\mathfrak{M}(\sigma) = \frac{1}{\mu}.\varkappa^2(\sigma) - 1 + 2.\left(S_s\right)(\sigma), \tag{13}$$

where s is an arc length function of c and $\varkappa = \varkappa(\sigma)$ is the Euclidean curvature of c.

It is clear that the function, defined by (13), is an invariant under the group F_0. Recently, Encheva proved the following two results.

Theorem 11.1 (Uniqueness Theorem, [3]). *Let $\mathrm{I} \subset \mathbb{R}$ be an open interval and let $\boldsymbol{c}_i : \mathrm{I} \longrightarrow \mathbb{R}^2$, $i = 1,\ 2$ be two Frenet curves of the class C^2, parameterized by the same arc length parameter σ of their stereographic images on the sphere S^2. Assume that $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ have the same invariants $\mathfrak{M}_i = \mathfrak{M}_i(\sigma)$, $i = 1, 2$ defined by (13), i.e. $\mathfrak{M}_1(\sigma) = \mathfrak{M}_2(\sigma)$ for any $\sigma \in \mathrm{I}$. Then, there exists a transformation $f \in F_0$ such that $\boldsymbol{c}_2 = f \circ \boldsymbol{c}_1$.*

Theorem 11.2 (Existence Theorem, [3]). *Let $g : \mathrm{I} \longrightarrow \mathbb{R}$ be a function of class C^∞. Let $\boldsymbol{e}_1^0$, $\boldsymbol{e}_2^0$ be right-handed orthonormal pair of vectors at a point $\boldsymbol{c}_0$ in the plane $\mathbb{R}^2$. There exists a unique Frenet curve $\boldsymbol{c} : \mathrm{I} \longrightarrow \mathbb{R}^2$, which satisfies the conditions:*
(i) *there is $\sigma_0 \in \mathrm{I}$ such that $\boldsymbol{c}(\sigma_0) = \boldsymbol{c}_0$ and the Frenet frame of $\boldsymbol{c}$ at $\boldsymbol{c}_0$ is $\{\mathbf{e_1^0},\ \mathbf{e_2^0}\}$.*
(ii) *For any $\sigma \in \mathrm{I}$, $\mathfrak{M}(\sigma) = g^2(\sigma)$.*

Example 11.1. Let $\mathfrak{M}(\sigma) = \cos^2\sigma$, $\boldsymbol{c}_0 = (1, 0)$, $\boldsymbol{e}_1^0 = (0, 1) \in \mathbb{R}^2$. A plane curve with a conformal invariant $\mathfrak{M}(\sigma) = \cos^2\sigma$ and its corresponding spherical curve under stereographic projection π are obtained by Mathematica and represented on Fig. 5.

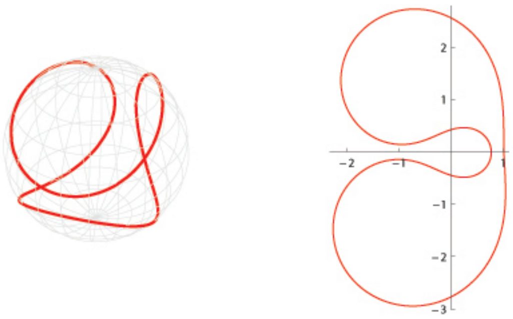

Figure 5.

Other examples are considered in the demonstration [4], published on the site of Wolfram Demonstration Project. Moreover, it is shown here, how the curve depends on the parameters of the three-parameter subgroup F_0 of the Möbius group in the plane.

12 Image processing and pattern recognition

One of the main and interesting problems of information science is clarification of how animals' eyes and brain recognize objects in the real world. Practice shows that they successfully cope with this problem and recognize objects at different locations, of different views and illumination, and with different degrees of blurring. But how is it done by the brain? How do we see? How do we recognize moving and changing objects of the surrounding world? A moving object is fixed in the retina as a sequence of different images (Fig. 6).

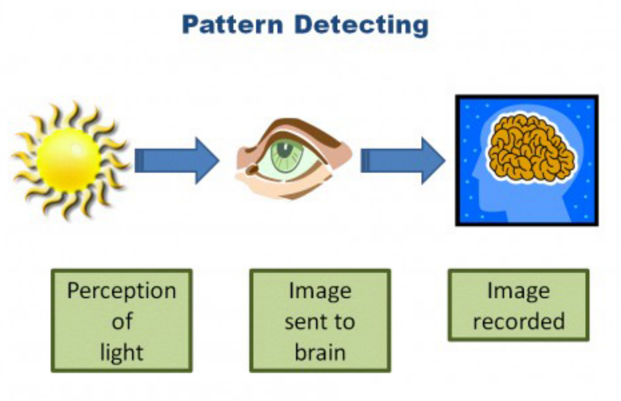

Figure 6.

As in the famous aphorism of Heraclitus, who pointed out that one cannot step into the same river twice, we literally never see the same object twice. No individual image allows reaching a conclusion about the true shape of the object. This means that a set of sequential images appearing in the retina must contain a constant "something," thanks to which we see and recognize the object as a whole. This constant "something" is called *invariant*. For example, all letters 'F' in Fig. 7 we interpret as the same for different geometric distortions. This fact means that all geometrically

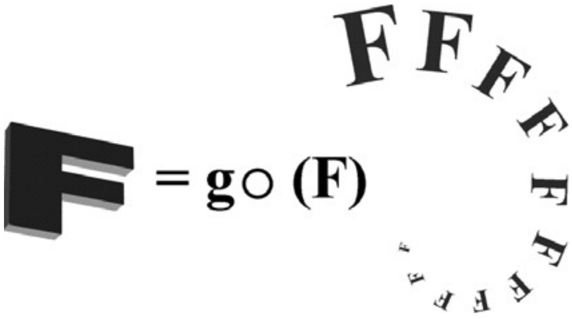

Figure 7. Geometrical distorted versa of letter "F".

distorted letters 'F' contain invariant features, which are not changed, when the shape of 'F' is changed. Our brain can extract these invariant features. In Fig. 8 we see hyperbolic (non-Euclidean) motions of grey-level mice and color fish.

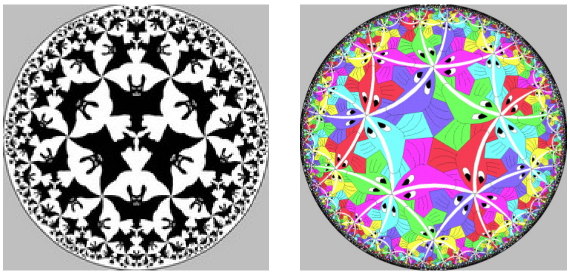

Figure 8. Non-Euclidean motions

All transformed figures are interpreted as being the same. This fact means that all figures contain invariant features with respect to hyperbolic motions (and color transformations), and our brain can extract these invariant features from images, too. So, we see, we live in 3D Euclidean space but our brain can calculate invariants of images with respect to non-Euclidean transformations. In order for an artificial pattern recognition system to perform in the same way as any biological visual system, the recognition result should be invariant with respect to various transformation groups of the patterns such as translation, rotation, size variation, and change in illumination and color. Labunets describes in [16] new methods of image recognition based on an algebraic-geometric theory of invariants. In this approach, each color or multicolor pixel is considered not as a kD vector, but as a kD hypercomplex number (k is the number of image spectral channels). Changes in the surrounding world which cause object shape and color transformations are treated not as matrix transforms, but as the action of some Clifford numbers in physical and perceptual spaces.

We suppose that a brain calculates some hypercomplex-valued invariants of an image when recognizing it. Hypercomplex algebras generalize the algebras of complex numbers, quaternions and octonions. Of course, the algebraic nature of hypercomplex numbers must correspond to the spaces with respect to geometrically perceivable properties. For recognition of 2D, 3D and nD images we turn the spaces $\mathbb{R}^2, \mathbb{R}^3$ and $\mathbb{R}^n$ into corresponding algebras of hypercomplex numbers. Let "small" nD space $\mathbb{R}^n$ be spanned by the orthonormal basis of n space hyperimaginary units $I_i, i = 1, 2, \dots n$. We assume

$$I_i^2 = \begin{cases} +1 & \text{for } i = 1, 2, \dots, p, \\ -1 & \text{for } i = p+1, p+2, \dots, p+q, \\ 0 & \text{for } i = p+q+1, p+q+2, \dots, p+q+r = n, \end{cases}$$

and $I_iI_j = -I_jI_i$. Now, we we construct the "big" 2^nD hypercomplex space $\mathbb{R}^{2^n}$. Let $b = (b_1, \dots, b_n) \in \mathbb{B}_2^n$ be an arbitrary n-bit vector, where $b_i \in \mathbb{B}_2 = \{0, 1\}$ and $\mathbb{B}_2^n$ is the nD Boolean algebra. Let us introduce $I^b = I_1^{b_1} I_2^{b_2} \cdots I_n^{b_n}$. Then 2^n elements I^b form a basis of 2^nD space, i.e., for all $\mathcal{C} \in \mathbb{R}^{2^n}$ we have $\mathcal{C} = \sum_{b \in \mathbb{B}_2^n} c_b I^b$. If $\mathcal{C}_1, \mathcal{C}_2 \in \mathbb{R}^{2^n}$, then we can define their product $\mathcal{C}_1\mathcal{C}_2$. There are 3^n possibilities for $I_i^2 = +1, 0, -1, \forall i = 1, \dots, n$. Every possibility generates one algebra. Therefore, the space $\mathbb{R}^{2^n}$ with 3^n rules of the multiplication forms 3^n different 2^nD algebras, which are called the space Clifford algebras. We denote these algebras by $\mathcal{A}_{2^n}^{Sp(p,q,r)}$.

All even Clifford numbers $\mathcal{E}_0 \in \mathcal{A}_{2^n}^{\{0\}}$ of unit modulus represent the rotation group of the corresponding space $\mathcal{GR}_n^{Sp(p,q,r)}$, which is called the spinor group and is denoted by $\mathrm{Spin}(A_{2^n}^{Sp(p,q,r)})$. Generalized complex numbers and quaternions of unit modulus have the forms: $e_0 = e^{I\varphi} = \cos\varphi + I\sin\varphi$, $\mathcal{Q}_0 = e^{u_0\varphi} = \cos\varphi + u_0\sin\varphi$, where $\cos\varphi$ and $\sin\varphi$ are trigonometric functions in the corresponding nD $\mathcal{GR}_n^{Sp(p,q,r)}$-geometries, φ is a rotation angle around the vector-valued quaternion u_0 of unit modulus ($|u_0| = 1, u_0 = -\overline{u_0}$). Clifford numbers $\mathcal{E}_0 \in \mathrm{Spin}(A_{2^n}^{Sp(p,q,r)})$ with unit modulus have the analogous form $\mathcal{E}_0 = e^{u_0\varphi} = \cos\varphi + u_0\sin\varphi$ for the appropriate bivector u_0.

Theorem 12.1. (Lasenby, Doran, Gull [17])) *All motions in 2D, 3D and nD spaces* $\mathcal{GR}_2^{Sp(p,q,r)}$, $\mathcal{GR}_3^{Sp(p,q,r)}$, $\mathcal{GR}_n^{Sp(p,q,r)}$ *are represented in the forms:*

$$z' = e_0 z e_0 + w, \quad x' = \mathcal{Q}_0 x \mathcal{Q}_0^{-1} + w, \quad x' = \mathcal{E}_0 x \mathcal{E}_0^{-1} + w.$$

If $|e_0|, |\mathcal{Q}_0|, |\mathcal{E}_0| \neq 0$, *then the latter transformations form the "small" affine groups* $\mathrm{Aff}(\mathcal{GR}_2^{Sp(p,q,r)})$, $\mathrm{Aff}(\mathcal{GR}_3^{Sp(p,q,r)})$, $\mathrm{Aff}(\mathcal{GR}_n^{Sp(p,q,r)})$, *respectively.*

Using this theorem, we can describe geometric distortions of images in the language of Clifford algebras. These distortions will be caused by: 1) nD translations $x \longrightarrow x + w$; 2) nD rotations $x \longrightarrow \mathcal{E}_0(x + w)\mathcal{E}_0^{-1}$; 3) dilatation: $x \longrightarrow \lambda x$, where $\lambda \in \mathbb{R}^+$. If $f(x)$ is an initial image and ${}_{\lambda\mathcal{E}_0 w}f(q)$ is its distorted version, then ${}_{\lambda\mathcal{E}_0 w}f(x) = f(\mathcal{E}_0(x+w)\mathcal{E}_0^{-1})$, where λ is a scale factor, $x, w \in \mathcal{GR}_n^{Sp(p,q,r)}$. We suppose that the human brain can use the spinor and "small" affine groups for mental rotations (see Fig. 9) and motions of images (for example, in a dream), which are contained in the brain memory on the so-called "screen of mind."

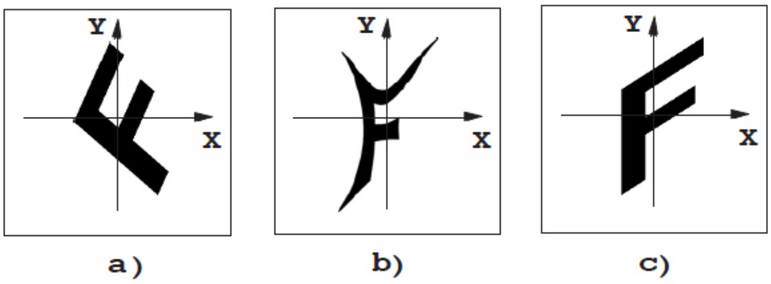

Figure 9. Rotations in a) 2D Euclidean space $\mathcal{GR}_2^{Sp(2,0,0)}$, b) 2D Minkowskian space $\mathcal{GR}_2^{Sp(1,1,0)}$ and c) 2D Galilean space $\mathcal{GR}_2^{Sp(1,0,1)}$.

ACKNOWLEDGMENTS. I would like to thank R. Encheva for providing the content of sections 10 and 11.

Литература

[1] F. A. Bogomolov, The Brauer group of quotient spaces by linear group actions, *Math. USSR Izv.* **30** (1988), 455—485.

[2] A. Borel, Topology of Lie groups and characteristic classes, *Bull. Amer. Math. Soc.* **61** (1955), 397–432.

[3] R. Encheva,Geometric invariants with respect to one subgroup of the Mobius group in the plane, In: 10th International Conference on Geometry and Applications, Journal of Geometry, August 2012, Volume **103**, Issue 2, 347–366.

[4] R. Encheva,Family of Plane Curves in the Extended Gauss Plane Generated by One Function, http://demonstrations.wolfram.com/FamilyOfPlaneCurvesInTheExtendedGaussPlaneGeneratedByOneFunc/, Wolfram Demonstrations Project, Published: July 8, 2013.

[5] R. Encheva and G. Georgiev, Shapes of space curves, *J. Geom. Graph.* **7** (2003), 145–155.

[6] A. Fröhlich, Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants, *J. Reine Angew. Math.* **360** (1985), 84–123.

[7] A. Fröhlich and A. M. McEvett, The representations of groups by automorphisms of forms, *J. Algebra* **12** (1969), 114–133.

[8] W. Fulton, J. Harris, "Representation theory. A first course", Graduate Texts in Mathematics, **129**, Springer-Verlag, New York, 1991.

[9] S. Garibaldi, A. Merkurjev and J-P. Serre, Cohomological invariants in Galois cohomology, AMS Univ. Lecture Series vol. 28, Amer. Math. Soc., Providence, 2003.

[10] A. Gray, "Modern Differential Geometry of Curves and Surfaces", CRC Press, Boca Raton, 1993.

[11] V. V. Ishanov, B. B. Lur'e and D. K. Faddeev, "The embedding problem in Galois theory", Amer. Math. Soc., Providence, 1997.

[12] B. Kahn, Classes de Stiefel-Whitney de formes quadratiques et de represéntations galoisiennes réelles, *Invent. Math.* **78** (1984), 223–256.

[13] C. Jensen, A. Ledet and N. Yui, "Generic polynomials: constructive aspects of the inverse Galois problem", Cambridge University Press, 2002.

[14] M. Kang, Noether's problem for metacyclic p-groups, *Adv. Math.* **203** (2005), 554–567.

[15] I. Kiming, Explicit classifications of some 2-extensions of a field of characteristic different from 2, *Cand. J. Math.* **42** (1990), 825–855.

[16] V. Labunets, Clifford Algebras as Unified Language for Image Processing and Pattern Recognition, *Computational Noncommutative Algebra and Applications, NATO Science Series II: Mathematics, Physics and Chemistry* Vol. 136, 2005, 197–225.

[17] A.N. Lasenby, C.J.L. Doran, and S.F. Gull, " Lectures in Geometric Algebra", In: W. E. Baylis, Ed., Clifford (Geometric) Algebras with Applications to Physics, Mathematics and Engineering, Birkhouser, Boston (1996) 256 p.

[18] A. Ledet, "Brauer Type Embedding Problems", Fields Institute Monographs **21**, American Mathematical Society, 2005.

[19] R. Massy, Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p, *J. Algebra* **109** (1987), 508–535.

[20] A. S. Merkurjev and A. A. Suslin, K-Cohomology of Severi-Brauer Varieties and the norm residue homomorphism, *Izv. Akad. Nauk SSSR*, Ser. Mat. **46** (1982), 1011–1046; English transl. in *Math. USSR Izvestiya* **21** (1983), 307–340.

[21] I. Michailov, Embedding obstructions for the cyclic and modular 2-groups, *Math. Balk., New Series*, **21** (2007), Fasc. 1-2, 31-50.

[22] I. Michailov, Four non-abelian groups of order p^4 as Galois groups, *J. Algebra* **307** (2007), 287-299.

[23] I. Michailov, Induced orthogonal representations of Galois groups, *J. Algebra* **322** (2009), 3713-3732.

[24] I. Michailov, Noether's problem for some groups of order $16n$, *Acta Arith.* **143** (2010), 277-290.

[25] I. Michailov, Noether's problem for abelian extensions of cyclic p-groups, *Pacific J. Math*, **270** (1) (2014), 167–189.

[26] I. Michailov, Galois realizability of groups of orders p^5 and p^6, *Cent. Eur. J. Math.*, **11 (5)**, 2013, 910–923.

[27] I. Michailov, I. Ivanov, N. Ziapkov, Noether's problem for abelian extensions of bicyclic and metacyclic p-groups, *Compt. Rend. de'l Acad. Bulg. D. Sc.*, **67** (2014), N 6, 737–744.

[28] I. Michailov and N. Ziapkov, The Inverse Problem Of Galois Theory, *Proceedings of the 37th spring conference of the Union of Bulgarian Mathematicians in Borovets*, 2008, 17–28.

[29] G. Malle & B. H. Matzat, "Inverse Galois Theory", Springer Monographs in Mathematics, Springer-Verlag, 1999.

[30] G. Malle & B. H. Matzat, Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$, *Math. Ann.* **272** (1985), 549-565.

[31] F. J. Mac Williams and N. J. A. Sloane, "The theory of error-correcting codes", North Holland, Amsterdam, 1977.

[32] E. Noether, Gleichungen mit vorgeschriebener Gruppe, *Math. Ann.* **78** (1918), 221–29.

[33] J. Neukirch, A. Schmidt & K. Wingberg, "Cohomology of number fields", Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.

[34] B. Plans, On Noether's problem for central extensions of symmetric and alternating groups, *J. Algebra* **321** (2009), 3704-3713.

[35] H. Reichardt, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, *J. Reine Angew. Math.* **177** (1937), 1–5.

[36] P. Roquette, On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras, *Math. Ann.* **150** (1963), 411-439.

[37] D. J. Saltman, Generic Galois extensions and problems in field theory, *Adv. Math.* **43** (1982), 250–283.

[38] D. J. Saltman, Noether's problem over an algebraically closed field, *Invent. Math.* **77** (1984), 71–84.

[39] D.J. Saltman, Twisted multiplicative field invariants, Noether's problem, and Galois extensions, *J. Algebra* **131** (2) (1990), 535-558.

[40] N. Schappacher, On the History of Hilbert's Twelfth Problem, *Societe Mathematique de France* (1998).

[41] A. Scholz, Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I, *Math. Z.* **42** (1937), 161–188.

[42] I. Schur, Gleichungen ohne Affekt, Sitzungsberichte Akad. Berlin (1930), 443–449.

[43] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.* **59** (1984), 651-676.

[44] J.-P. Serre, ”Topics in Galois Theory”, Research Notes in Mathematics, Jones & Barlett, 1992.

[45] I. R. Shafarevich, Construction of fields of algebraic numbers with given solvable Galois group (in Russian), *Izv. Aksd. Nauk SSSR, Ser. Mat.* **18** (1954), 525–578.

[46] K.-Y. Shih, On the construction of Galois extensions of function fields and number fields, Math. Ann. **207** (1974), 99-120.

[47] R. Swan, Noether's problem in Galois theory, in ”Emmy Noether in Bryn Mawr”, edited by B. Srinivasan and J. Sally, Springer-Verlag, Berlin, 1983.

[48] H. Völklein, ”Groups as Galois Groups, an Introduction”, Cambridge Studies in Advanced Mathematics 53, Cambridge University Press, 1996.

[49] J. Wood, Spinor groups and algebraic coding theory, *J. of Comb. Theory* **51** (1989), 277–313.

[50] N. Ziapkov, Some relatives of the dihedral group as Galois groups, *Compt. Rend. de L'Acad. Bulg. D. Sc.*, **62** No. 10 (2009), 1203–1206.

[51] Н. Зяпков, Групи от автоморфизми в теорията на Галоа и в теорията на кодирането, MATTEX 2010, Сборник научни трудове посветен на 130-годишнината на академик К.Попов, т. 1, ISSN 1314-3921,(2011) , 11-38.