ISRAEL JOURNAL OF MATHEMATICS **142** (2004), 47–60

ON ALTERNATING AND SYMMETRIC GROUPS AS GALOIS GROUPS

BY

DAVID BRINK*

University of Copenhagen, Universitetsparken 5, 2100 ϕ, Denmark
e-mail: brink@math.ku.dk

ABSTRACT

Fix an integer $n \geq 3$. We show that the alternating group A_n appears as Galois group over any Hilbertian field of characteristic different from 2. In characteristic 2, we prove the same when n is odd. We show that any quadratic extension of Hilbertian fields of characteristic different from 2 can be embedded in an S_n-extension (i.e. a Galois extension with the symmetric group S_n as Galois group). For $n \neq 6$, it will follow that A_n has the so-called GAR-property over any field of characteristic different from 2. Finally, we show that any polynomial $f = X^n + \cdots + a_1 X + a_0$ with coefficients in a Hilbertian field K whose characteristic doesn't divide $n(n-1)$ can be changed into an S_n-polynomial f^* (i.e. the Galois group of f^* over K, $\mathrm{Gal}(f^*, K)$, is S_n) by a suitable replacement of the last two coefficients a_0 and a_1. These results are all shown using the Newton polygon.

1. The Newton polygon

In this paragraph, we review the definition and basic properties of the Newton polygon. Let K be a field with algebraic closure $\tilde{K}$. Let v be a non-archimedean valuation on $\tilde{K}$. Let

$$f = a_0 X^n + a_1 X^{n-1} + \cdots + a_n, \quad a_0, a_n \neq 0$$

* The author acknowledges the financial support provided through the European Community's Human Potential Programme under contract HPRN-CT-2000-00114, GTEM.
Received October 27, 2003

be a polynomial with coefficients in K. Write

$$f = a_0 \cdot \prod_{i=1}^{n} (X - \alpha_i)$$

with $\alpha_i \in \tilde{K}$. Usually, it's difficult to compute the roots α_i by means of the coefficients a_i. In contrast to this, it's easy to compute the valuations $v(\alpha_i)$ by means of the valuations $v(a_i)$. That is what the Newton polygon does.

Definition 1: The Newton polygon of the polynomial f is the maximal convex function NP: $[0, n] \longrightarrow \mathbb{R}$ with $\mathsf{NP}(i) \leqq v(a_i)$ for all i.

The Newton polygon NP is piecewise linear. The maximal linear segments of NP are called **edges**. The slopes of the edges are strictly increasing. The **length** of an edge is the length of the interval on which it is defined

THEOREM 2: *If* NP *has an edge with length* l *and slope* γ, *then* f *has exactly* l *roots with valuation* γ.

For a proof of this theorem and an algorithmic definition of NP, see Neukirch [5].

2. Galois groups as permutation groups

If f is a separable polynomial over a field K, the Galois group $\mathrm{Gal}(f, K)$ is a permutation group on the roots of f. We need criteria to conclude that this permutation group is the entire symmetric group.

LEMMA 3: *The symmetric group* S_n *is the only doubly transitive permutation group of degree* n *containing a transposition.*

Proof: Let G be a doubly transitive permutation group containing a transposition τ. Any transposition can be written $\sigma\tau\sigma^{-1}$ with $\sigma \in G$. Therefore G contains all transpositions, and we get $G = S_n$. ∎

LEMMA 4: *Let* G *be a transitive permutation group of degree* n. *Assume* G *contains a subgroup that fixes one symbol and permutes the other* $n-1$ *symbols transitively. Then* G *is doubly transitive.*

Proof: Let H be a subgroup of G that fixes $a \in \Omega$ and permutes $\Omega \backslash \{a\}$ transitively. Let $x, x', y, y' \in \Omega$ with $x \neq y$ and $x' \neq y'$. We are looking for a $\sigma \in G$ with $\sigma(x) = x'$ and $\sigma(y) = y'$. Pick $\tau_1, \tau_2 \in G$ with $\tau_1(x) = a$ and

$\tau_2(a) = x'$. According to the assumption, $\tau_1(y) \neq a$ and $\tau_2^{-1}(y') \neq a$. Pick $\rho \in H$ with $\rho(\tau_1(y)) = \tau_2^{-1}(y')$. Now, put $\sigma = \tau_2 \circ \rho \circ \tau_1$. ∎

LEMMA 5: *Let K be a field with algebraic closure $\tilde{K}$. Let $\mathbf{T} = (T_1, \ldots, T_n)$ be an n-tuple of indeterminates. Let $f = f(\mathbf{T}, X) \in K[\mathbf{T}, X]$ be a polynomial. Assume f is monic, irreducible and separable in X. Let $\xi = (\xi_1, \ldots, \xi_n) \in K^n$. Assume $f(\xi, X)$ has one double root a in $\tilde{K}$ and else only simple roots. If $f(\mathbf{T}, a)$ is a uniformising element in the field of formal Laurent series*

$$E = \tilde{K}\Big(\frac{T_2 - \xi_2}{T_1 - \xi_1}, \ldots, \frac{T_n - \xi_n}{T_1 - \xi_1}\Big)((T_1 - \xi_1))$$

equipped with the $(T_1 - \xi_1)$-adic valuation, then the Galois group $\mathrm{Gal}(f, K(\mathbf{T}))$ contains a transposition.

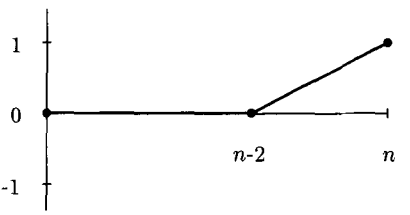
Proof: The valued field E is an extension of $K(\mathbf{T})$. Every $T_i - \xi_i$ is a uniformising element in E. For $i = 1$, this is clear. For $i > 1$, one writes

$$T_i - \xi_i = \frac{T_i - \xi_i}{T_1 - \xi_1} \cdot (T_1 - \xi_1)$$

and notes that the first factor is a unit.

The coefficients of f are in the valuation ring of E. By assumption, the reduction $\bar{f} = f(\xi, X)$ has one double root a and else only simple roots. By Hensel's Lemma, there is a factorisation $f = f_1 f_2 \cdots f_r$ over E with $\bar{f}_1 = (X - a)^2$ and $\deg(f_i) = 1$ for $i \geqq 2$.

We show that $f_1(X + a)$, and therefore also $f_1 = f_1(X)$, is irreducible. First, we compute the Newton polygon of $f(\mathbf{T}, X + a)$. Write $f(\mathbf{T}, X + a) = X^n + \cdots + b_1 X + b_0$. All coefficients b_j are in the valuation ring of E. The reduction of $f(\mathbf{T}, X + a)$ has 0 as double root. It follows that b_2 is a unit, and that b_1 and b_0 are in the valuation ideal. By assumption, $b_0 = f(\mathbf{T}, a)$ is a uniformising element. We have now determined the Newton polygon of $f(\mathbf{T}, X + a)$:



By Theorem 2, $f(\mathbf{T}, X+a)$ has two roots with valuation $\frac{1}{2}$. These roots cannot lie in E. Hence they are the roots of $f_1(X+a)$ which is irreducible.

This implies that $\mathrm{Gal}(f,E)$ consists of the identity and a transposition. As $\mathrm{Gal}(f,E)$ is a subgroup of $\mathrm{Gal}(f,K(\mathbf{T}))$, the claim follows. ∎

3. Regularity and embedding problems

Consider a field K. A field extension E/K is (here) called **regular** if K is algebraically closed in E. Let G be a finite group. A **G-extension** is a field extension which is Galois with Galois group isomorphic to G. The group G is called **regular over** K if there exists a tuple of indeterminates $\mathbf{t} = (t_1, \ldots, t_n)$ and a G-extension $E/K(\mathbf{t})$ with E/K regular. If G is regular over K, then there exists a G-extension $E/K(t)$ with E/K regular, see Völklein [8] page 25.

We say that L/K can be **embedded** in a G-extension if there exists a G-extension E/K with $L \subsetneqq E$. We say that L/K can be **regularly embedded** in a G-extension if there exists a tuple $\mathbf{t} = (t_1, \ldots, t_n)$ of indeterminates so that $L(\mathbf{t})/K(\mathbf{t})$ can be embedded in a G-extension E with E/L regular.

THEOREM 6: *Let K be a Hilbertian field. Let L/K be a finite Galois extension. Let G be a finite group. If L/K can be regularly embedded in a G-extension, then L/K can also be (ordinarily) embedded in a G-extension. In particular, if G is regular over K, then G appears as Galois group over K.*

This is a refinement of Hilbert's Irreducibility Theorem (HIT). A proof of HIT can be found in Fried and Jarden [2] chapter 12. A proof of Theorem 6 appears in the forthcoming edition of [2].

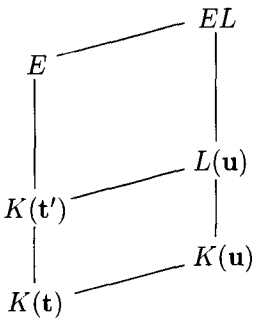
In order to use Theorem 6, we need the following

LEMMA 7: *Let K be a field of characteristic different from 2. Let L/K be a quadratic extension. Let G be a finite group. Let $\mathbf{t} = (t_1, \ldots, t_n)$ be a tuple of indeterminates. Assume that $K(\mathbf{t})$ has a G-extension E containing $\sqrt{t_1}$ and with E/K regular. Then L/K can be regularly embedded in a G-extension.*

Proof: Write $L = K(\alpha)$ with $\alpha^2 \in K$. Define $u = \alpha \cdot \sqrt{t_1}$. We have $u^2 = \alpha^2 t_1$. Each of the tuples $\mathbf{t}' = (\sqrt{t_1}, t_2, \ldots, t_n)$ and $\mathbf{u} = (u, t_2, \ldots, t_n)$ is algebraically independent over K.

Adjoin u to the fields $K(\mathbf{t})$, $K(\mathbf{t}')$ and E. We get: $K(\mathbf{t}, u) = K(\mathbf{u})$, $K(\mathbf{t}', u) =$

$L(\mathbf{u})$ and $E(u) = EL$. See the diagram:



Since $u^2 \in K(\mathbf{t})$, we have $|K(\mathbf{u}) : K(\mathbf{t})| \leqq 2$. Since E/K is regular, $E \cap L = K$. Therefore

$$2 = |EL : E| \leqq |K(\mathbf{u}) : K(\mathbf{t})| \leqq 2,$$

and thus $|EL : E| = |K(\mathbf{u}) : K(\mathbf{t})|$. Consequently, $|E : K(\mathbf{t})| = |EL : K(\mathbf{u})|$. Galois theory gives $\mathrm{Gal}(EL/K(\mathbf{u})) \cong G$.

By Lemma 9.7 in Fried and Jarden [2], E is linearly disjoint from the algebraic closure $\tilde{K}$ over K. Hence L is algebraically closed in EL, i.e. EL/L is regular. ∎

4. Rationality

LEMMA 8: *Let K be a field of characteristic 2. Let F be a quadratic extension of the rational function field $K(x)$ with F/K regular. Then F is a rational function field over K iff only one prime divisor $\mathfrak{p}$ of $K(x)/K$ is ramified in F, and* $\deg(\mathfrak{p}) = 1$.

Proof: Consider the different $\mathfrak{d} = \prod_{i=1}^{r} \mathfrak{P}_i^{s_i}$ of $F/K(x)$. Its degree is $\deg(\mathfrak{d}) = \sum_{i=1}^{r} s_i \deg(\mathfrak{P}_i)$. The prime divisors of F/K, ramified over $K(x)$, are exactly $\mathfrak{P}_1, \ldots \mathfrak{P}_r$. Each $\mathfrak{P}_i$ has ramification index 2 and is thus wildly ramified. Therefore we have $2 \leqq s_i \leqq 3$, see Neukirch [5] Theorem III 2.6. Let g denote the genus of F/K. The Riemann–Hurwitz Genus Formula yields $\deg(\mathfrak{d}) = 2g + 2$ (see e.g. Fried and Jarden [2] section 2.9).

Assume F/K to be rational. Then $g = 0$, and $\deg(\mathfrak{d}) = 2$. Thus $\mathfrak{d}$ has the form $\mathfrak{P}^2$ with $\deg(\mathfrak{P}) = 1$. The prime $\mathfrak{p}$ of $K(x)$ lying under $\mathfrak{P}$ is the only ramified prime in F, and $\deg(\mathfrak{p}) = 1$.

Now assume F/K is not rational. If $g = 0$, the above argument would give the existence of a prime of F of degree 1. Then F would be rational (Fried

and Jarden [2] section 2.9), a contradiction. Therefore $g > 0$, and $\deg(\mathfrak{d}) \geqq 4$. It follows that a prime divisor of degree 1 cannot be the only prime divisor ramified in F. ∎

5. The main results

THEOREM 9: *Let $n \geqq 3$ be an integer and K a field of characteristic different from 2. If $\mathrm{Char}(K) \nmid n(n-1)$, then $K(t)$ has an S_n-extension which is regular over K and contains $\sqrt{t}$. If $\mathrm{Char}(K) \mid n(n-1)$, then $K(s,t)$ has an S_n-extension which is regular over K and contains $\sqrt{t}$. In both cases, any quadratic extension L/K can be regularly embedded in an S_n-extension.*

Proof: We divide the proof into three cases.

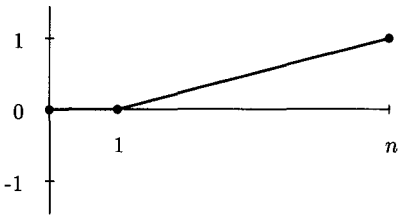
FIRST CASE: $\mathrm{Char}(K) \nmid n(n-1)$. Let T be an indeterminate. Define

$$f = f(T, X) = X^n + X^{n-1} + T.$$

This polynomial is linear and primitive in T. According to Gauss' Lemma, f is irreducible over $K(T)$. We shall always consider f to be a polynomial over $K(T)$. The derivative is

$$f' = nX^{n-1} + (n-1)X^{n-2} = nX^{n-2}\Big(X + \frac{n-1}{n}\Big).$$

In particular, $f' \neq 0$. So f is separable. The Galois group $\mathrm{Gal}(f, K(T))$ is transitive. Over the field $K((T))$, equipped with the T-adic valuation, f has this Newton polygon:



Thus f has an irreducible factor of degree $n-1$ over $K((T))$. According to Lemma 4, $\mathrm{Gal}(f, K(T))$ is doubly transitive.

Put

$$\xi := -\Big(\frac{1-n}{n}\Big)^n - \Big(\frac{1-n}{n}\Big)^{n-1} = -\frac{1}{n}\Big(\frac{1-n}{n}\Big)^{n-1} \in K^*.$$

The polynomial $f(\xi, X) = X^n + X^{n-1} + \xi$ has the double root $a = (1-n)/n$ and else only simple roots. The element $f(T, a) = T - \xi$ satisfies the condition of Lemma 5. By Lemma 5, $\mathrm{Gal}(f, K(T))$ contains a transposition. By Lemma 3, $\mathrm{Gal}(f, K(T)) = S_n$.

The same argument shows $\mathrm{Gal}(f, \tilde{K}(T)) = S_n$ where the tilde denotes algebraic closure. Therefore the splitting field $\mathrm{Spl}(f, K(T))$ is a regular extension of K.

The discriminant of f is

$$\mathrm{disc}(f) = (-1)^{n(n-1)/2} n^n T^{n-2}(T - \xi).$$

In particular, $\mathrm{disc}(f)$ has the form $a \cdot \eta(T)$ where a is a non-zero square in $K(T)$, and η is a linear or fractional linear function over K. Put $t = \eta(T)$. Then $K(t) = K(T)$, and $\sqrt{t} \in \mathrm{Spl}(f, K(T))$. Now use Lemma 7.

SECOND CASE: $\mathrm{Char}(K) \neq 2$ and $\mathrm{Char}(K) \mid n$. Let S, T be indeterminates. Define

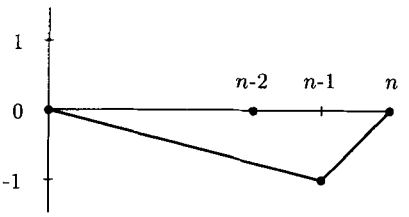
$$f = f(S, T, X) = X^n + X^2 + SX + T.$$

We consider f to be a polynomial over $K(S, T)$. The derivative is

$$f' = 2X + S.$$

As above, one sees that f is irreducible and separable. The Galois group $\mathrm{Gal}(f, K(S, T))$ is transitive.

Over the field $K(T)((S^{-1}))$, equipped with the S^{-1}-adic valuation, f has this Newton polygon:



As above, $\mathrm{Gal}(f, K(S, T))$ is doubly transitive.

The polynomial $f(0, 0, X) = X^n + X^2 = X^2(X^{n-2} + 1)$ has the double root $a = 0$ and else only simple roots (because $\mathrm{Char}(K) \nmid n - 2$). The element $f(S, T, a) = T$ satisfies the condition of Lemma 5. As above, $\mathrm{Gal}(f, K(S, T)) = S_n$.

The same argument shows $\mathrm{Gal}(f, \tilde{K}(S,T)) = S_n$. It follows that the splitting field $\mathrm{Spl}(f, K(S,T))$ is a regular extension of K.

The discriminant of f is

$$\mathrm{disc}(f) = (-1)^{(n-1)(n-2)/2} 2^n \Big(\Big(\frac{-S}{2} \Big)^n + \frac{S^2}{4} - \frac{S^2}{2} + T \Big).$$

In particular, $\mathrm{disc}(f)$ has the form $\eta(T)$ where η is a linear function over $K(S)$. Put $s = S$ and $t = \eta(T)$. Then $K(s,t) = K(S,T)$, and $\sqrt{t} \in \mathrm{Spl}(f, K(S,T))$. Now use Lemma 7.

THIRD CASE: $\mathrm{Char}(K) \neq 2$ and $\mathrm{Char}(K) \mid n-1$. Let S, T be indeterminates. Define

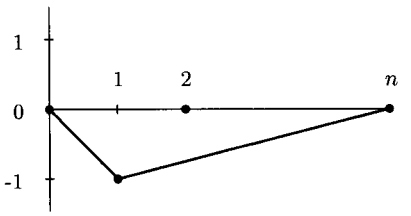
$$f = f(S,T,X) = X^n + SX^{n-1} + X^{n-2} + T.$$

We consider f to be a polynomial over $K(S,T)$. The derivative is

$$f' = X^{n-1} - X^{n-3} = X^{n-3}(X+1)(X-1).$$

As above, one sees that f is irreducible and separable over $K(S,T)$. The Galois group $\mathrm{Gal}(f, K(S,T))$ is transitive.

Over the field $K(T)((S^{-1}))$, equipped with the S^{-1}-adic valuation, f has this Newton polygon:



As above, $\mathrm{Gal}(f, K(S,T))$ is doubly transitive.

The polynomial $f(-1,-1,X) = X^n - X^{n-1} + X^{n-2} - 1$ has the double root $a = 1$ and else only simple roots. The element

$$f(S,T,a) = S + T + 2 = (T+1)\Big(1 + \frac{S+1}{T+1}\Big)$$

satisfies the condition of Lemma 5. As above, $\mathrm{Gal}(f, K(S,T)) = S_n$.

The same argument shows $\mathrm{Gal}(f, \tilde{K}(S,T)) = S_n$. It follows that the splitting field $\mathrm{Spl}(f, K(S,T))$ is a regular extension of K.

The discriminant of f is

$$\mathrm{disc}(f) = (-1)^{(n+1)(n+2)/2} T^{n-3}(S+T+2)(T+(-1)^n(2-S)).$$

In particular, it has the form $a \cdot \eta(S)$ where a is a non-zero square in $K(S,T)$, and η is a fractional linear function over $K(T)$. Put $s = \eta(S)$ and $t = T$. Then $K(s,t) = K(S,T)$, and $\sqrt{s} \in \mathrm{Spl}(f, K(S,T))$. Now use Lemma 7. ∎

COROLLARY 10: *Let $n \geqq 3$. Any quadratic extension of Hilbertian fields of characteristic different from 2 can be embedded in an S_n-extension.*

Proof: Use Theorem 6. ∎

THEOREM 11: *Let $n \geqq 3$. The alternating group A_n is regular over any field of characteristic different from 2. In characteristic 2, the same holds when n is odd.*

Proof: Let K be any field of characteristic different from 2. By Theorem 9, either $K(t)$ or $K(s,t)$ has an S_n-extension which contains $\sqrt{t}$ and is regular over K. This field is an A_n-extension of $K(\sqrt{t})$ or $K(s,\sqrt{t})$, respectively.

Now assume that K is a field of characteristic 2, and that n is odd. Let S,T be indeterminates. Define

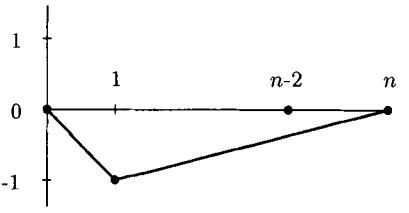
$$f = f(S,T,X) = X^n + SX^{n-1} + X^2 + T^n.$$

We consider f to be a polynomial over $K(S,T)$. The derivative is

$$f' = X^{n-1}.$$

As in the proof of Theorem 9, one sees that f is irreducible and separable. The Galois group $\mathrm{Gal}(f, K(S,T))$ is transitive.

Over the field $K(T)((S^{-1}))$, equipped with the S^{-1}-adic valuation, f has this Newton polygon:

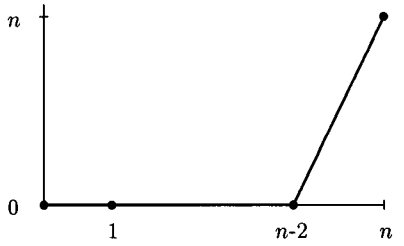


As in the proof of Theorem 9, one sees that $\mathrm{Gal}(f, K(S,T))$ is doubly transitive.

Consider the field $E = \widetilde{K(S)}((T))$ equipped with the T-adic valuation. The coefficients of f are in the valuation ring of E, and the reduction

$$\bar{f} = X^n + SX^{n-1} + X^2 = X^2(X^{n-2} + SX^{n-3} + 1)$$

has one double root and else only simple roots. By Hensel's Lemma, there exists a factorisation $f = f_1 f_2 \cdots f_r$ over E with $\deg(f_1) = 2$ and $\deg(f_i) = 1$ for $i \geqq 2$. Over E, f has this Newton polygon:



Thus f has two roots α, β with valuation $n/2$. Since n is odd, these roots are not in E. It follows that $f_1 = (X - \alpha)(X - \beta)$ is irreducible over E. Therefore $\mathrm{Gal}(f, E)$ contains a transposition. This transposition also belongs to $\mathrm{Gal}(f, K(S,T))$. By Lemma 3, $\mathrm{Gal}(f, K(S,T)) = S_n$.

The same argument shows $\mathrm{Gal}(f, \tilde{K}(S,T)) = S_n$. It follows that the splitting field $\mathrm{Spl}(f, K(S,T))$ is a regular extension of K.

Now, let F be the quadratic extension of $K(S,T)$ contained in $\mathrm{Spl}(f, K(S,T))$. The field $\mathrm{Spl}(f, K(S,T))$ is an A_n-extension of F. We show that F has the form $K(S,T')$.

The Galois group $\mathrm{Gal}(f, \widetilde{K(S)(T)})$ contains a transposition and is therefore not contained in A_n. Thus $F \cap \widetilde{K(S)}(T) = K(S,T)$. It follows that $K(S)$ is algebraically closed in F.

Let $\mathfrak{p}$ be a prime divisor of the function field $K(S,T)$ over $K(S)$. It is determined by the reduction $\bar{T} \in \widetilde{K(S)} \cup \{\infty\}$. Assume that $\bar{T} \neq 0, \infty$. Then the coefficients of f are in the valuation ring of $K(S,T)$, and the reduction $\bar{f}$ has only simple roots. It follows that $\mathfrak{p}$ is unramified in $\mathrm{Spl}(f, K(S,T))$ and therefore also in F.

Now assume that $\bar{T} = \infty$. Then the coefficients of f are not all in the valuation ring of $K(S,T)$. Let

$$g(X) = \frac{1}{T^n} f(TX) = X^n + \frac{S}{T} X^{n-1} + \frac{1}{T^{n-2}} X^2 + 1.$$

Obviously, f and g have the same splitting field over $K(S,T)$. The reduction $\bar{g} = X^n + 1$ has only simple roots. It follows that $\mathfrak{p}$ is unramified in $\mathrm{Spl}(f, K(S,T))$ and therefore also in F.

We conclude that a prime divisor $\mathfrak{p}$ is ramified in F only when $\bar{T} = 0$, and in this case $\deg(\mathfrak{p}) = 1$. By Lemma 8, F has the form $K(S,T')$. ∎

COROLLARY 12: *Let $n \geqq 3$. The alternating group A_n appears as Galois group over any Hilbertian field of characteristic different from 2. In characteristic 2, the same holds when n is odd.*

As a last application of our method, we show:

THEOREM 13: *Any polynomial of the form*

$$f = f(S,T,X) = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + SX + T$$

with coefficients a_i in a field K with $\mathrm{Char}(K) \nmid n(n-1)$ has Galois group S_n over $K(S,T)$.

Proof: It is enough to show that $f(X)$ is a Morse polynomial, i.e. that $f'(X)$ has only simple roots, and that f takes different values on these roots. This follows either from Theorem 4.4.5 of Serre [6], or, more elementary, using the same arguments as in the proof of Theorem 9 above.

Write $f'(X) = n \cdot \prod_{i=1}^{n-1}(X - \beta_i)$ and define the invariant

$$M = \prod_{i<j}(f(\beta_i) - f(\beta_j))^2.$$

Then $f(X)$ is a Morse polynomial iff $M \neq 0$. M is a polynomial in $a_1 = S, a_2, \ldots, a_{n-1}, \beta_1, \ldots, \beta_{n-1}$. Each term of this polynomial has total degree $n(n-1)(n-2)$ with respect to $\beta_1, \ldots, \beta_{n-1}$ and by letting the total degree of a_i be $n - i$.

By the Main Theorem on Symmetric Polynomials, M can be written as a polynomial in $a_1, \ldots, a_{n-1}$ with rational coefficients, each term of which has total degree $n(n-1)(n-2)$.

Now we evaluate M at $(S, 0, \ldots, 0)$. Then $f(X) = X^n + SX$ and $f'(X) = nX^{n-1} + S$. Each root β_i of f' satisfies $f(\beta_i) = \frac{n-1}{n}S\beta_i$. Thus

$$M(S,0,\ldots,0) = \left(\frac{n-1}{n}\right)^{(n-1)(n-2)} S^{(n-1)(n-2)} \prod_{i<j}(\beta_i - \beta_j)^2.$$

The product $\prod_{i<j}(\beta_i - \beta_j)^2$ is simply the discriminant of $X^{n-1} + S/n$. We get

$$M(S,0,\ldots,0) = (-1)^{(n-1)(n-2)/2}(n-1)^{(n-1)^2} n^{-n(n-2)} S^{n(n-2)}.$$

As S has total degree $n-1$, $S^{n(n-2)}$ has total degree $n(n-1)(n-2)$. Therefore $M(S,0,\ldots,0)$ is the only term in the general polynomial $M = M(S,a_2,\ldots,a_{n-1})$ containing S to the power $n(n-2)$. It follows that M is non-zero for any choice of $a_2,\ldots,a_{n-1} \in K$. This finishes the proof. ∎

COROLLARY 14: *Consider a polynomial* $f = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$ *with coefficients in* $\mathbb{Q}$. *Let* $|\ |$ *be the usual absolute value or a p-adic valuation on* $\mathbb{Q}$. *Let an* $\epsilon > 0$ *be given. Then there are* $a_0^*, a_1^* \in \mathbb{Q}$ *with* $|a_0 - a_0^*| < \epsilon$ *and* $|a_1 - a_1^*| < \epsilon$ *so that* $f^* = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1^*X + a_0^*$ *is an* S_n*-polynomial, i.e.* $\mathrm{Gal}(f^*, \mathbb{Q}) = S_n$.

Proof: Put $F(S,T,X) = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + SX + T$. By Theorem 13, the splitting field $E = \mathrm{Spl}(F(X), \mathbb{Q}(S,T))$ is an S_n-extension of $\mathbb{Q}(S,T)$. Let $\alpha_1,\ldots,\alpha_n \in E$ be the roots of $F(X)$. Write $E = \mathbb{Q}(S,T)(\beta)$ with $\beta = m_1\alpha_1 + \cdots + m_n\alpha_n$ and $m_i \in \mathbb{Z}$. Let G be the minimal polynomial of β over $\mathbb{Q}(S,T)$. It has degree $n!$ and its coefficients are in $\mathbb{Q}[S,T]$. Thus we may consider G as a polynomial in S, T and X over $\mathbb{Q}$ and write $G = G(S,T,X)$.

By Hilbert's Irreducibility Theorem, there are $a_0', a_1' \in \mathbb{Q}$ so that $G(a_1', a_0', X)$ is irreducible over $\mathbb{Q}$. Then $G(a_1', T, X)$ is irreducible over $\mathbb{Q}(T)$. By Corollary 4, VIII §2 in Lang [3], there is an a_0^* close to a_0 so that $G(a_1', a_0^*, X)$ is irreducible over $\mathbb{Q}$. Then $G(S, a_0^*, X)$ is irreducible over $\mathbb{Q}(S)$. By [3] again, there is an a_1^* close to a_1 so that $G(a_1^*, a_0^*, X)$ is irreducible over $\mathbb{Q}$.

Put $f^* = F(a_1^*, a_0^*, X)$ and write $f^* = \prod_{i=0}^n (X - \alpha_i^*)$. Then $\beta^* = m_1\alpha_1^* + \cdots + m_n\alpha_n^*$ is a root of $G(a_1^*, a_0^*, X)$. The splitting field of f^* contains β^* and therefore has degree at least $n!$ over $\mathbb{Q}$. It follows that f^* is an S_n-polynomial over $\mathbb{Q}$. ∎

6. The GAR-property

Let G be a finite centerless group, considered as a subgroup of its automorphism group $\mathrm{Aut}(G)$. Let $\mathbf{t} = (t_1,\ldots,t_n)$ be a tuple of indeterminates. The group G is said to be GAR over a field K if there is a G-extension $E/K(\mathbf{t})$ with E/K regular, and if in addition the following two conditions hold:

(GA) There is a subfield F of $K(\mathbf{t})$, containing K, such that E is Galois over F with Galois group isomorphic to $\mathrm{Aut}(G)$, and under this isomorphism, $\mathrm{Gal}(E/K(\mathbf{t}))$ corresponds to G.

(R) Every field extension F' of F with $K_sF' = K_s(\mathbf{t})$ is a rational function field over $K' := K_s \cap F'$. Here K_s denotes the separable algebraic closure of K.

By Matzat's *Embedding Theorem for Centerless Kernel*, see [4], Theorem IV 3.6, a finite embedding problem over a Hilbertian field K is solvable if each composition factor of the kernel is GAR over K. Thus the following theorem generalises Corollary 10 for $n \neq 3, 6$.

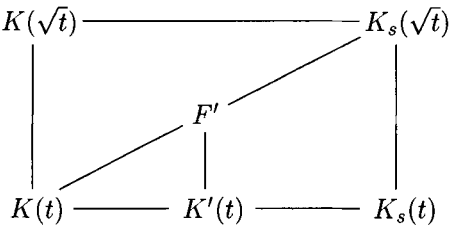
THEOREM 15: *The alternating group A_n with $n \geqq 4$ and $n \neq 6$ is GAR over any field of characteristic different from 2.*

Proof: A_n is centerless for $n \geqq 4$. If in addition $n \neq 6$, then $\mathrm{Aut}(A_n) = S_n$ (see Suzuki [7], page 299, but note that the case $n = 3$ is falsely included). Assume that $\mathrm{Char}(K) \nmid n(n-1)$. Then, by Theorem 9, $K(t)$ has an S_n-extension E, regular over K and containing $\sqrt{t}$. Thus condition (GA) is satisfied.

Now let $F'/K(t)$ be an extension with $K_sF' = K_s(\sqrt{t})$. Put $K' := K_s \cap F'$. By Galois theory, all fields between $K(t)$ and $K_s(t)$ have the form $L(t)$ with $K \subsetneqq L \subsetneqq K_s$. Hence $F' \cap K_s(t) = K'(t)$. Furthermore,

$$[F' : K'(t)] = [K_s(\sqrt{t}) : K_s(t)] = 2.$$

If F' contains $\sqrt{t}$, then $F' = K'(\sqrt{t})$, and we are done. If F' doesn't contain $\sqrt{t}$, then $F'(\sqrt{t})$ is a V_4-extension of $K'(t)$, containing F' and $K'(\sqrt{t})$ as quadratic subfields. The intersection $F'(\sqrt{t}) \cap K_s(t)$ has degree 2 over $K'(t)$. Hence it is the third quadratic subfield of $F'(\sqrt{t})/K'(t)$. It has the form $F'(\sqrt{t}) \cap K_s(t) = K'(\sqrt{\alpha}, t)$ for some (non-square) $\alpha \in K'$. Thus $F' = K'(\sqrt{\alpha t})$, and condition (R) is satisfied.



Now assume $\mathrm{Char}(K)$ divides $n(n-1)$ and is different from 2. Then, by Theorem 9 again, $K(s,t)$ has an S_n-extension E, regular over K and containing $\sqrt{t}$. Thus condition (GA) is satisfied.

Let $F'/K(s,t)$ be an extension with $K_sF' = K_s(s, \sqrt{t})$. As above, F' is a quadratic extension of $F' \cap K_s(s,t) = K'(s,t)$. The same arguments show that

either $F' = K'(s, \sqrt{t})$, or $F' = K'(s, \sqrt{\alpha t})$ for some non-square $\alpha \in K'$. Hence condition (R) is satisfied. ∎

Notes: In Section 4.5 of [6], Serre shows that A_n is regular over $\mathbb{Q}$ using the same polynomial as in the first case of the proof of Theorem 9 above. In a series of papers, Abhyankar et al. show that A_n is regular over any algebraically closed field of positive characteristic $p \leqq n$, see [1] and the references therein. In Chapter IV of [4], Malle and Matzat show the GAR-property over $\mathbb{Q}$ for many families of finite simple groups, including all A_n with $n \neq 6$. It is also shown that A_6 is GAR over $\mathbb{Q}^{\mathrm{ab}}$, the maximal abelian extension of $\mathbb{Q}$.

References

[1] S. S. Abhyankar, J. Ou and A. Sathaye, *Alternating group coverings of the affine line for characteristic two,* Discrete Mathematics **133** (1994), 25–46.

[2] M. D. Fried and M. Jarden, *Field Arithmetic,* Springer-Verlag, Berlin, 1986.

[3] S. Lang, *Diophantine Geometry,* Wiley, New York, 1962.

[4] G. Malle and B. H. Matzat, *Inverse Galois Theory,* Springer-Verlag, Berlin, 1999.

[5] J. Neukirch, *Algebraische Zahlentheorie,* Springer-Verlag, Berlin, 1992.

[6] J.-P. Serre, *Topics in Galois Theory,* Jones and Bartlett Publishers, Boston, 1992.

[7] M. Suzuki, *Group Theory I,* Springer-Verlag, Berlin, 1982.

[8] H. Völklein, *Groups as Galois Groups,* Cambridge Studies in Advanced Mathematics 53, Cambridge University Press, 1996.