SECTIONAL MONODROMY GROUPS OF PROJECTIVE CURVES

BORYS KADETS

Abstract. Fix a degree $d$ projective curve $X \subset \mathbb{P}^r$ over an algebraically closed field $K$. Let $U \subset (\mathbb{P}^r)^*$ be a dense open subvariety such that every hyperplane $H \in U$ intersects $X$ in $d$ smooth points. Varying $H \in U$ produces the monodromy action $\varphi : \pi_1^\text{ét}(U) \to S_d$. Let $G_X := \text{im}(\varphi)$. The permutation group $G_X$ is called the sectional monodromy group of $X$. In characteristic zero $G_X$ is always the full symmetric group, but sectional monodromy groups in characteristic $p$ can be smaller. For a large class of space curves ($r \geq 3$) we classify all possibilities for the sectional monodromy group $G$ as well as the curves with $G_X = G$. We apply similar methods to study a particular family of rational curves in $\mathbb{P}^2$, which enables us to answer an old question about Galois groups of generic trinomials.

1. Introduction

Let $K$ be an algebraically closed field. Consider a geometrically integral nondegenerate proper curve $X$ in the projective space $\mathbb{P}^r$ over $K$. Choose coordinates $x_0, ..., x_r$ on $\mathbb{P}^r$. Extend scalars from $K$ to $L = K(t_1, ..., t_r)$ and consider the subscheme $Z \subset \mathbb{P}^r_L$ given by the intersection of $X_L$ with the hyperplane $x_0 + t_1x_1 + ... + t_rx_r = 0$. The scheme $Z$ is the spectrum of a finite separable extension $M$ of $L$ (see Lemma 2.1). The Galois group $G$ of the Galois closure of $M$ over $L$ is our main object of interest and will be referred to as the sectional monodromy group. A folklore result is the following.

Proposition 1.1 (see Remark 3.4). Assume that the characteristic of $K$ is zero. Let $d$ be the degree of $X$. Then $G \cong S_d$.

The result is important in the study of curves in projective space. It can be used to restrict the possibilities for Hilbert polynomials of space curves. For more details see [Har80], [EH82].

The analogue of Proposition 1.1 in characteristic $p$ is false. For example, the sectional monodromy group of the rational plane curve $x^p = yz^{p-1}$ is $\text{AGL}_1(p)$.

Motivated by geometric applications, Rathmann [Rat87] proved a version of Proposition 1.1 valid in all characteristics.

Theorem 1.2 (Rathmann). Assume that $X \subset \mathbb{P}^r$ is a smooth nondegenerate curve of degree $d$. Assume $r \geq 4$. Then the sectional monodromy group of $X$ contains the alternating group $A_d$.

In Section 3 we prove a stronger statement on sectional monodromy groups. Recall that a projective curve is called strange if all of its tangent lines pass through a common point.

Theorem 1.3. Assume $X \subset \mathbb{P}^r$ is a geometrically integral nondegenerate curve of degree $d$. Assume that $r \geq 3$ and $X$ is not strange. Then exactly one of the following is true.

1. The sectional monodromy group of $X$ contains $A_d$.  

Date: September 19, 2018.
(2) \( r = 3 \) and the curve \( X \) is projectively equivalent to the projective closure of the rational curve \( \{(t, t^q, t^{q+1}), t \in K\} \subset \mathbb{A}^3_K \) for some power \( q \) of the characteristic. The sectional monodromy group of \( X \) is \( \text{PGL}_2(q) \).

For plane curves, sectional monodromy groups are not known even in the following very simple case.

**Example 1.4.** Let \( X_{n,m} \) be the rational curve \( x^n = y^m z^{n-m} \) for some relatively prime integers \( n > m > 0 \). Then the sectional monodromy group of \( X \) is the Galois group of the trinomial \( x^n + ax^m + b \) over \( K(a,b) \). Classifying possible Galois groups of generic trinomials is an old problem, see [Coh80], [Smi77], [Uch70], [Smi84]. A closely related problem of classifying Galois groups of trinomials over the function field \( K(t) \) when \( a \) and \( b \) are specialized to powers of \( t \) has also been widely studied; see [Abh92], [Abh93a], [Abh93b], [Abh94], [ASP92].

The curves \( X_{m,n} \) do not satisfy both of the assumptions of Theorem 1.3; they are evidently plane curves \( (r = 2) \) and many of them are strange. Nevertheless, we can use methods similar to those in the proof of Theorem 1.3 to study the curves \( X_{m,n} \). In section 5 we prove the following theorem.

**Theorem 1.5.** Let \( K \) be an algebraically closed field of characteristic \( p \). Let \( G \) be the Galois group of the polynomial \( x^n + ax^m + b \) over \( K(a,b) \).

1. If \( m = 1 \) and \( n = p^d \), then \( G = \text{AGL}_1(p^d) \).
2. If \( m = 1, n = 6, \) and \( p = 2, \) then \( G = \text{PSL}_2(5) \).
3. If \( m = 1, n = 12, \) and \( p = 3, \) then \( G = \text{M}_{11} \) (a Mathieu group, see [Con99]).
4. If \( m = 1, n = 24, \) and \( p = 2, \) then \( G = \text{M}_{24} \).
5. If \( m = 2, n = 11, \) and \( p = 3, \) then \( G = \text{M}_{11} \).
6. If \( m = 3, n = 23, \) and \( p = 2, \) then \( G = \text{M}_{23} \).
7. Let \( q := p^k \) for some integer \( k \). If \( n = (q^d - 1)/(q - 1), m = (q^s - 1)/(q - 1) \) for some integers \( s, d, \) then \( G = \text{PGL}_d(q) \).
8. If none of the above holds, then \( A_n \subset G \).

**Warning.** The aforementioned result of Rathmann as well as the results of this paper depend on the classification of finite simple groups.

### 2. Transitivity of Sectional Monodromy Groups

From now on, let \( K \) denote a fixed algebraically closed field. We first give a more geometric definition of the sectional monodromy groups from the introduction. Let \( r \geq 2 \) be an integer and let \( X \subset \mathbb{P}^r \) be a degree \( d \) projective nondegenerate integral curve. Consider the incidence scheme \( I = I_X \subset X \times (\mathbb{P}^r)^* \) parameterizing pairs \((P,H)\) of points \( P \in X \) and hyperplanes \( H \subset \mathbb{P}^r \) subject to the condition \( P \in H \). The scheme \( Z \) from the introduction is the generic fiber of the projection \( \pi = \pi_X : I_X \to (\mathbb{P}^r)^* \). We call the covering \( \pi_X \) the sectional covering associated to \( X \).

**Lemma 2.1.** The incidence scheme \( I \) is irreducible. The morphism \( \pi \) is finite of degree \( d \) and generically 
\( \text{étale.} \)

**Proof.** The fibers of the first coordinate projection \( I \to X \) are projective spaces of dimension \( r - 1 \); hence \( I \) is irreducible. The morphism is generically 
\( \text{étale by Bertini’s theorem [Jou83, Proposition 6.4], and finite since it is quasi-finite and proper.} \)
Lemma 2.1 implies that the sectional monodromy group $G$ is well-defined and acts transitively on a set of $d$ points. If $U \subset (\mathbb{P}^r)^*$ is a dense open subset over which $\pi$ is étale and $\Omega$ is a fiber of $\pi$ over a geometric point of $U$, then $G$ can be identified with the image of $\pi_1^{\text{ét}}(U)$ in Sym$(\Omega)$. If $Z \subset U$ is a closed subset, then the monodromy group of $\pi^{-1}(Z) \to Z$ is a permutation subgroup of $G$. We now show that the action of $G$ on $\Omega$ is always 2-transitive, and has even higher transitivity degree if the curve is not “strange”.

**Lemma 2.2.** The sectional monodromy group acts doubly transitorily.

**Proof.** Choose a hyperplane $H$ that intersects $X$ at $d$ distinct smooth points. Let $P$ be one of the points in $H \cap X$. Choose an $(r - 2)$-dimensional subspace $V$ in $\mathbb{P}^r$ such that $V \cap X = P$. Consider the line $l \subset (\mathbb{P}^r)^*$ corresponding to the family of hyperplanes containing $V$. Let $Z = \pi^{-1}(l)$. Projection of $Z$ to $X$ is an isomorphism over $X \setminus P$. The fiber above $P$ is isomorphic to $l$ (via $\pi$). Therefore $Z$ decomposes into a union of two irreducible components $Z = Z_1 \cup Z_2$, where $\pi : Z_1 \to l$ is an isomorphism and $Z_2$ is isomorphic to $X$. Since the fiber of $\pi' = \pi|_{Z_2} : Z_2 \to l$ above the point of $l$ corresponding to $H$ is smooth, the covering $\pi'$ is generically étale. Therefore, the monodromy group $G$ contains a subgroup that acts via fixing one point and acting transitively on the others. Thus $G$ is doubly-transitive.

For every $r$ there are examples of integral nondegenerate curves $X \subset \mathbb{P}^r$ for which $G_X$ is not triply transitive (see [Har77, Example 1.2]). However we will prove that $G_X$ is $r$-transitive if $X$ is not “strange”. We recall the definition of a strange curve.

**Definition 2.3.** An integral curve $X$ in $\mathbb{P}^r$ is called **strange** if the tangent lines to $X$ at the smooth points pass through a common point.

**Remark 2.4.** Equivalently, an integral curve is strange if the tangent lines to $X$ at all but finitely many smooth points pass through a common point.

A secant of a curve $X$ is a line intersecting it in at least 2 points.

**Proposition 2.5.** If every secant intersects $X$ in at least three points, then $X$ is strange.

**Proof.** See [Har77, Proposition 3.3.8].

Most of the results that follow concern curves that are not strange. It is natural to expect higher transitivity for nonstrange curves. This is the case, as we show in Proposition 2.8.

**Lemma 2.6.** Let $X \subset \mathbb{P}^r$, $r \geq 3$ be a proper nondegenerate nonstrange integral curve. Let $\mathcal{L}$ denote the set of lines in $\mathbb{P}^r$ that have nonempty intersection with every tangent to $X$. Then either $\mathcal{L}$ is finite or $r = 3$, $X$ is contained in a smooth quadric, and $\mathcal{L}$ is one of the quadric’s rulings.

**Proof.** Assume that $\mathcal{L}$ is infinite. Consider two distinct lines $\ell_1, \ell_2 \in \mathcal{L}$. If $\ell_1$ and $\ell_2$ intersect, then either every tangent to $X$ passes through $\ell_1 \cap \ell_2$ or every tangent to $X$ is in the plane containing $\ell_1$ and $\ell_2$. Since $X$ is nondegenerate and nonstrange, neither of these is possible. Therefore any two distinct lines from $\mathcal{L}$ are skew. Consider two skew lines $\ell_1, \ell_2 \in \mathcal{L}$. Since every tangent of $X$ crosses both of them, the curve $X$ lies in the dimension three projective subspace of $\mathbb{P}^r$ that contains $\ell_1, \ell_2$. Hence $r = 3$. A classical fact, which we prove below, is that the union of lines that intersect three pairwise skew lines is a smooth quadric. Thus there exists a smooth quadric $Q$ containing every tangent line of $X$. Elements of $\mathcal{L}$ are pairwise skew and lie on $Q$, therefore $\mathcal{L}$ forms one of the rulings of $Q$.
We now show that the union of lines intersecting three fixed lines in \( \mathbb{P}^3 \) is a smooth quadric. Since \( 10 = \dim H^0(\mathbb{P}^3, \mathcal{O}(2)) > 3 \dim H^0(\mathbb{P}^1, \mathcal{O}(2)) = 9 \), there exists a quadric containing any triple of lines. If the lines are pairwise skew, the quadric cannot be a cone or a pair of planes, therefore it must be smooth. Every line intersecting a smooth quadric in at least three points has to lie on it. \( \square \)

**Lemma 2.7.** Let \( X \subset \mathbb{P}^r \), \( r \geq 3 \) be a nonstrange nondegenerate integral curve. If \( r = 3 \) assume additionally that \( X \) is not contained in a quadric. Then the projection from a general point \( P \) of \( X \) is birational onto its image. Moreover, the image of a general projection is nonstrange.

**Proof.** Consider the set \( \mathcal{L} \) of Lemma \( 2.6 \). Since \( X \) is not contained in a quadric, \( \mathcal{L} \) is finite. Proposition \( 2.5 \) implies that a general point of \( X \) lies on finitely many multisecants. Therefore projection from a general point is generically one-to-one on \( K \) points and is thus birational. Let \( P \in X(K) \) be a point such that the projection \( \pi_p : X \to Y \) from \( P \) is birational onto its image \( Y \), and such that \( P \) does not lie on a line from \( \mathcal{L} \). Suppose that \( Y \) is strange and all the tangents pass through \( Q \in \mathbb{P}^{r-1} \). Then the line \( \pi_p^{-1}(Q) \subset \mathbb{P}^r \) is an element of \( \mathcal{L} \) that contains \( P \). Thus \( Y \) is nonstrange. \( \square \)

**Proposition 2.8.** If \( X \subset \mathbb{P}^r \), \( r \geq 2 \) is an integral nondegenerate nonstrange curve, then \( G \) is \( r \)-transitive.

**Proof.** We prove the statement by induction on \( r \). The case \( r = 2 \) is Lemma \( 2.2 \). Assume \( r > 2 \). Assume first that it is not the case that \( r = 3 \) and \( X \) lies on a quadric. Choose a point \( P \in X(K) \) such that the conclusions of Lemma \( 2.7 \) hold. Let \( Y \subset \mathbb{P}^{r-1} \) be the projection of \( X \) from \( P \). Consider the hyperplane \( H \subset (\mathbb{P}^r)^* \) corresponding to the family of hyperplanes in \( \mathbb{P}^r \) passing through \( P \). Let \( Z \) denote \( \pi_p^{-1}(H) \). The scheme \( Z \) has an irreducible component \( Z' = P \times H \subset X \times (\mathbb{P}^r)^* \). The covering \( Z \setminus Z' \to H \) is birational to the sectional covering of \( Y \), since the preimages of hyperplanes in \( \mathbb{P}^{r-1} \) are hyperplanes in \( \mathbb{P}^r \) containing \( P \). By the induction hypothesis the monodromy group of the covering \( Z \setminus Z' \to H \) is \( r - 1 \)-transitive. The covering \( Z' \to H \) is an isomorphism. Therefore the monodromy group of \( Z \to H \) acts by fixing one point and acting \((r - 1)\)-transitively on the rest. Since \( G \) acts transitively and contains a subgroup acting \((r - 1)\)-transitively on all but one (fixed) point, \( G \) is \( r \)-transitive.

We have to show that when \( r = 3 \) and \( X \) lies on a quadric \( Q \) the group is 3-transitive. Consider a generic plane \( H \). We can assume that both \( H \cap X \) and \( H \cap Q \) are smooth. Take two points of \( H \cap X \) and a line \( \ell \) through them. The line \( \ell \) contains exactly two points \( P_1, P_2 \) of the curve. Consider the line \( \ell^* \subset (\mathbb{P}^3)^* \) corresponding to the hyperplanes containing \( \ell \). The restriction of the sectional covering of \( X \) to \( \ell^* \) is generically étale since \( H \cap X \) is smooth. Let \( Y \subset X \times \ell^* \) denote the preimage of \( \ell \) under \( \pi_X \). The projection of \( Y \) to \( X \) is an isomorphism over \( X \setminus \{P_1, P_2\} \). The preimages of \( P_1, P_2 \) in \( Y \) are each isomorphic to \( \ell^* \). Therefore \( Y \) decomposes into a union of irreducible components \( Y = Y_1 \cup Y_2 \cup Y_3 \), where \( Y_1 \) is isomorphic to \( X \) and \( Y_2, Y_3 \) are isomorphic to \( \ell^* \). Hence the monodromy group contains a subgroup that acts by fixing two points and acting transitively on the rest. Therefore \( G \) is triply-transitive. \( \square \)

Multiple transitivity is a very strong condition on the group. For example the only 5-transitive groups are \( A_n \) and \( S_n \) in their natural actions and the Mathieu groups \( M_{11} \) and \( M_{24} \).
acting on 11 and 24 points respectively. The classification of 2-transitive groups is known; see, for example, [DM96, §7.7] for the statement.

Remark 2.9. It is common to state classification results on permutation groups without specifying the action (or by referring to the “natural” action). This is relatively harmless except for the cases of $M_{11}$, which has two multiply-transitive actions on 11 and 12 points, and of $M_{12}$, which has two multiply transitive actions on 12 points exchanged by an outer automorphism.

The following proposition due to Rathmann describes the behavior of the sectional monodromy group with respect to projections from points outside of the curve.

Proposition 2.10 ([Rat87, Proposition 1.10.]). Let $X \subset \mathbb{P}^r$, $r \geq 3$ be a projective nondegenerate integral curve. Let $Y$ be the projection of $X$ from a general point of $\mathbb{P}^r$. Then the sectional monodromy groups of $X$ and $Y$ are isomorphic.

3. Tangents and inertia groups

We will compute sectional monodromy groups by restricting the sectional monodromy covering $\pi_X$ to a curve in $(\mathbb{P}^r)^*$ and computing inertia groups. A natural choice of a point in $(\mathbb{P}^r)^*$ above which the restricted covering ramifies is a point corresponding to a hyperplane containing a tangent line of $X$. Tangent hyperplanes can behave pathologically in characteristic $p$ (even for nonstrange curves).

For the statements and precise definitions in this paragraph see [Hef89] and references therein. Let $X \subset \mathbb{P}^r$ be an integral projective curve that is not a line. The dual curve $X^* \subset \text{Gr}(2, r + 1)$ is defined to be the closure of the set of tangent lines to $X$. The Gauss map is the rational map $\gamma : X \dashrightarrow X^*$ that sends a point to the tangent line at that point. In characteristic 0 the Gauss map is birational. In characteristic $p$ both the separable degree $s$ and the inseparable degree $q$ of $\gamma$ can be greater than one. A general tangent line of $X$ has $s$ points of tangency with multiplicity $\max(q, 2)$ at each one. It is a theorem of Kaji that Gauss maps can be arbitrary bad in the sense that any finite inseparable extension of function fields can be realized as the generic fiber of a Gauss map; see [Kaj89, Corollary 3.4].

We will use the following group theoretic result due to Jones [Jon14]. Recall that a permutation group $G$ acting on $\Omega$ is primitive if it preserves no nontrivial partition of $\Omega$.

Theorem 3.1 (Jones). Let $G$ be a primitive permutation group of finite degree $n$, not containing $A_n$. Suppose that $G$ contains a cycle fixing exactly $k$ points, where $0 \leq k \leq n - 2$. Then one of the following holds:

1. $k = 0$ and either
   - $C_p \subset G \subset \text{AGL}_1(p)$ with $n = p$ prime, or
   - $\text{PGL}_d(q) \subset G \subset \text{PGL}_d(q)$ with $n = (q^d - 1)/(q - 1)$ and $d \geq 2$ for some prime power $q$, or
   - $G = \text{PSL}_2(11), M_{11}$ or $M_{23}$ with $n = 11, 11, 23$ respectively.

2. $k = 1$ and either
   - $\text{AGL}_d(q) \subset G \subset \text{AGL}_d(q)$ with $n = q^d$ and $d \geq 1$ for some prime power $q$, or
   - $G = \text{PSL}_2(p)$ or $G = \text{PGL}_2(p)$ with $n = p + 1$ for some prime $p \geq 5$, or
   - $G = M_{11}, M_{12}$ or $M_{24}$ with $n = 12, 12, 24$ respectively.

3. $k = 2$ and $\text{PGL}_2(q) \subset G \subset \text{PGL}_2(q)$ with $n = q + 1$ for some prime power $q$. 


The inclusions in Theorem 3.1 are inclusions of permutation groups. We recall the definitions of some of the groups appearing in Theorem 3.1. The group $\text{AGL}_d(q)$ is the affine general linear group acting on $\mathbb{A}^d(\mathbb{F}_q)$; it is an extension of $\text{GL}_d(\mathbb{F}_q)$ by the group of translations $(\mathbb{F}_q)^d$. The group $\text{AGL}_d(q)$ is generated by $\text{AGL}_d(q)$ and the Frobenius automorphism. The group $\text{PGL}_d(q) = \text{GL}_d(q)/\mathbb{F}_q^*$ is the projective general linear group acting on the projective space $\mathbb{P}^{d-1}(\mathbb{F}_q)$. The projective semilinear group $\text{PGL}_d(q)$ is generated by $\text{PGL}_d(q)$ and the Frobenius automorphism.

In Lemma 3.3 we use inertia groups to construct special subgroups of the sectional monodromy group; together Proposition 2.8 and Lemma 3.3 will reduce most of the computation of sectional monodromy groups to pure group theory. First we need to prove the following lemma.

Lemma 3.2. Let $(F,v)$ denote the valued field $K((t))$. Let $O$ denote its ring of integers $O = K[[t]]$. Let $P \in O[x]$ be an arbitrary power series and let $q$ be a power of $p$. Consider a power series $Q = x^{q+2}P(x) + a_{q+1}x^{q+1} + a_qx^q + a_1x + a_0 \in O[x]$, where $v(a_q) = v(a_1) = 1$, $v(a_0) = 0$. Assume that $v(a_1a_q - a_qa_{q+1}) = 1$. Assume that all roots of $Q$ in the open unit disk $D := \{x \in F : v(x) > 0\}$ lie in $F_{\text{sep}}$, so $Q$ has exactly $q$ roots in $D$. The Galois action on these roots defines a homomorphism $\varphi: \text{Gal}(\overline{F}/F) \to S_q$. Let $H$ denote the image of $\varphi$. Then $H$ equals $\text{AGL}_{1}(q)$ embedded via its action on the affine line.

Proof. The Newton polygon of $Q$ has a unique segment of positive slope, it connects $(0,1)$ and $(q,0)$. Therefore $Q$ has $q$ roots in the open unit disk each with valuation $1/q$. Let $\alpha$ be a root of $Q$. The field extension $L = F(\alpha)/F$ has ramification index at least $q$, therefore $[L:F] = q$ and $H$ acts transitively. Consider the roots of $Q(x + \alpha)$ over $L$. We have

$$Q(x + \alpha) = x^q(x + \alpha)^2P(x + \alpha) + \alpha^q(x + \alpha)^2P(x + \alpha) + a_{q+1}x^q(x + \alpha)$$

$$+ a_{q+1}\alpha^q(x + \alpha) + a_qx^q + a_1x + a_1\alpha + a_q\alpha^q + a_0.$$ 

The constant term must be zero since $\alpha$ is a root of $Q$. The constant term of $Q(x + \alpha)/x$ is

$$2\alpha^{q+1}P(\alpha) + \alpha^{q+2}P'(\alpha) + a_{q+1}\alpha^q + a_1.$$ 

Assume $v(a_{q+1}\alpha^q + a_1) > 1$. Then $a_{q+1}\alpha^q + a_1 \equiv 0$ (mod $\alpha^{q+1}$). Reducing the equation $Q(\alpha) = 0$ modulo $\alpha^{q+1}$, we conclude that $a_0 + a_q\alpha^q \equiv 0$ (mod $\alpha^{q+1}$). Hence $\alpha^q \equiv -a_0/a_q$ (mod $\alpha^{q+1}$) and $a_1 - a_0a_{q+1}/a_q \equiv a_{q+1}\alpha^q + a_1 \equiv 0$ (mod $\alpha^{q+1}$). But $v(a_{q+1}a_0/a_q - a_1) = 1$, contradiction. Thus $v(a_{q+1}\alpha^q + a_1) = 1$, and the constant term of $Q(x + \alpha)/x$ has valuation 1.

The power series $Q(x + \alpha)/x = : \sum b_kx^k$ has constant term $b_0$ of valuation 1. Modulo $\alpha$ we have $Q(x + \alpha)/x \equiv x^{q-1}(x + \alpha)^2P(x) + a_{q+1}x^{q-1}(x + \alpha) + a_qx^{q-1}$ (mod $\alpha^q$). So for $1 \leq k \leq q - 2$ the valuation of $b_k$ is at least one. The valuation of $b_{q-1}$ is zero. Therefore Newton polygon of $Q(x + \alpha)/x$ has only one segment of positive slope, it connects $(0,1)$ to $(q-1,0)$. The field $K((t))$ has a unique extension of degree $q - 1$, namely $K((t^{1/q-1}))$. We conclude that the stabilizer of a point in $H$ is a cyclic group of order $(q - 1)$. A cycle in an imprimitive group has to either belong to a block or contain the same number of elements in every block. Since $q - 1$ and $q$ are relatively prime, a $(q - 1)$-cycle belongs to a single block. So the group cannot be imprimitive. Since $F$ is a nonarchimedean local field, $H$ is solvable. Theorem 3.1 implies that in this case $\text{AGL}_1(q) \subset H \subset \text{AGL}_1(q)$. The group $\text{AGL}_1(q)$ is the group of semilinear transformation of the affine line, namely the group generated by $\text{AGL}_1(q)$.
and the Frobenius automorphism. Since the stabilizer of a point in $H$ is a cyclic group, $H = AGL_1(q)$. 

\[\square\]

**Lemma 3.3.** Let $X$ be a nondegenerate nonstrange plane curve of degree $d$. Assume that the Gauss map of $X$ has separable degree $s$ and inseparable degree $q$. Choose a geometric point $x$ above which the covering $\pi_X$ is étale. Denote by $\Omega$ the fiber of $\pi_X$ above $x \in (\mathbb{P}^2)^*$, so the group $G_X$ acts on $\Omega$ by permutations and $\# \Omega = d$. Then the following hold:

1. If $q = 1$, then $G$ contains a transposition.
2. If $q > 1$, then there is a decomposition $\Omega = A_1 \cup \ldots \cup A_s \cup B$, $\# A_i = q, \# B = d - sq$, a subgroup $H \subset G$ and a collection of subgroups $H_i \subset G, i = 1, \ldots, s$ such that the following properties hold:
   - $H$ fixes every point of $B$ and preserves the decomposition $\Omega = A_1 \cup \ldots \cup A_s \cup B$.
   - The image of $H$ in the symmetric group $\text{Sym}(A_i)$ equals $AGL_1(q)$ embedded via its action on the affine line.
   - There exists and element $h \in H$ that acts on each $A_i$ by fixing one point and moving the rest cyclically.
   - $H_i$ fixes $B \cup A_i$ and acts transitively on each $A_j$ for $j \neq i$.

**Proof.** Let $U \subset (\mathbb{P}^2)^*$ be a dense open subset over which the covering $\pi_X$ is étale. The complement of $U$ contains finitely many lines. A line in $(\mathbb{P}^2)^*$ defines a point $((\mathbb{P}^2)^*)^* = \mathbb{P}^2$. Let $S \subset \mathbb{P}^2$ be the set of points corresponding to lines in the complement of $U$. Then for every point $P \notin S$ the restriction of $\pi$ to the family of lines passing through $P$ is generically étale. A general tangent to $X$ is tangent at exactly $s$ points with multiplicity max$(2, q)$ at each one. Since $X$ is not strange, a general tangent line does not intersect the set of singular points $\text{Sing}_X$ of $X$ and does not intersect $S$. Choose a tangent line $\ell$ to $X$ that does not intersect $S \cup \text{Sing}_X$ and such that $\ell \cap X$ has $s$ points with multiplicity max$(2, q)$ and $d - qs$ points with multiplicity $1$. In particular for every point $P$ on $\ell$ the restriction of $\pi$ to the family of lines passing through $P$ is generically étale.

Let $P_1, \ldots, P_s$ be the points of tangency and $Q_1, \ldots, Q_{d-qs}$ be the rest of the intersection. Choose a line in $\mathbb{P}^2$ that is disjoint from both $\bigcup_i P_i$ and $\bigcup_j Q_j$. Consider the affine plane $\mathbb{A}^2$ obtained by removing the chosen line. Choose coordinates $x, y$ in $\mathbb{A}^2$ so that $\ell$ is the line $y = 0$, and the coordinates of $P_1, \ldots, P_s$ are $(\alpha_1, 0), (\alpha_2, 0), \ldots, (\alpha_s, 0)$. Choose an algebraic closure of the fraction field of the local ring at $[\ell] \in (\mathbb{P}^2)^*$; identify $\Omega$ with the fiber at the geometric point corresponding to this choice. Let $A_i \subset \Omega$ be the set that reduces to $P_i$, and let $B = \Omega \setminus \bigcup_i A_i$ be the rest of $\Omega$. For an element $\alpha \in K$ consider the family of lines $\ell_\alpha = \ell_\alpha(x)$ given by the equation $y = t(x - \alpha)$. The family $\ell_\alpha(x)$ is the family of lines passing through $(\alpha, 0)$, so the covering $\pi$ is generically étale above the line corresponding to $\ell_\alpha(x)$ in $(\mathbb{P}^2)^*$. We want to analyze inertia groups at $t = 0$ of the restriction of $\pi$ to these families.

1. Assume $q = 1$. In this case char $K \neq 2$, see [Kat73, Proposition 3.3]. We need to describe the extension of $K\langle t \rangle$ obtained by adjoining the coordinates of the intersection of $X$ with $y = t(x - \alpha)$. Choose a uniformizer $x_i = x - \alpha_i$. For each point $P_i$ consider the local uniformization $y = p_i(x_i)$ of $X$ with respect to $x_i$, where $p_i(x_i)$ is a power series with coefficients in $K$. Since $q = 1$ the power series $p_i(x_i)$ vanishes at 0 with multiplicity max$(q, 2) = 2$. When $\alpha \neq \alpha_i$ the Newton polygon of $Q_i = p_i(x_i) - tx_i - t\alpha + t\alpha_i$ has a unique positive slope segment, it connects $(0, 1)$ and
Then either map of 3.4 Let Lemma 3.5.

In section 4 we use Lemma 3.3 to figure out the possibilities for the sectional monodromy of $(2,0)$. Hence the positively valued roots of $Q_i$ have valuation 1/2. Therefore when $\alpha \neq \alpha_i$ the extension obtained by adding the positively valued roots of $Q_i$ to $K((t))$ is the (unique) ramified degree 2 extension. Similarly, if $\alpha = \alpha_i$ the equation $Q_i = 0$ has two positively valued roots, both lying in $K((t))$. Taking $\alpha$ to be distinct from each $\alpha_i$ gives an element $g \in G$ that fixes $B$ and acts on each $A_i$ as a transposition. Taking $\alpha = \alpha_i$ gives an element $g_1 \in G$ that acts by identity on $B \cup A_1$ and as a transposition on $A_j$ for all $j \neq 1$. The product $gg_1$ is a transposition.

(2) Now assume $q > 1$ is a power of the characteristic. This statement is similar to part $[1]$, except the degrees of the extensions are no longer 2 and some wild ramification appears. Take $x_i = x - \alpha_i$ as a uniformizer for $X$ at $P_i$. Let $(x_i, p_i(x_i))$ be the uniformization and define $c_i, d_i$ by $p_i(x_i) = d_i x^q + c_i x^{q+1} + O(x^{q+1})$. Choose $\alpha \in K$ so that both $d_i + (\alpha - \alpha_i)c_i \neq 0$ and $\alpha \neq \alpha_i$ hold for every $i$. Consider the intersection of $X$ with the line $y = t(x - \alpha)$ over the field $K((t))$. The $x$-coordinates of the intersection points that reduce to $P_i$ are the positively valued roots of $Q_i(x) = p_i(x_i) - tx_i + t(\alpha - \alpha_i)$. Since $\alpha \notin S$, the intersection of $X$ with $y = t(x - \alpha)$ over $K(t)$ defines a separable extension of $K(t)$. Therefore the positively valued roots of $Q_i$ lie in a separable extension of $K((t))$. Lemma 3.2 applies to the power series $Q_i$ (condition $v(a_1a_q - a_0a_{q+1}) = 1$ becomes $d_i + (\alpha - \alpha_i)c_i \neq 0$). Let $L_i/K((t))$ be the extension obtained by adjoining all positive valuation roots of $Q_i$ to $K((t))$. Then the Galois group of $L_i/K((t))$ is $AGL_1(q)$. The ramification index of $L_i/K((t))$ is divisible by $q(q-1)$. In particular every field $L_i$ is an overfield of $K((t^{1/(q-1)})$. Let $H$ be the Galois group of the compositum of $L_i, i = 1, \ldots, s$. Take an element $h \in H$ that surjects onto a generator of $\text{Gal}(K((t^{1/(q-1)}))/K((t)))$. Every such element $h$ will surject onto an element of order $q - 1$ on each $\text{Gal}(L_i/K((t)))$.

We now examine the possibilities for the action of $h$ on the positive valued roots of $Q_i$. Assume that for some fixed $i$ the element $h$ has an orbit of length less than $q - 1$ on the roots of $Q_i$. The extension $L_i/K((t))$ is generated by adjoining any two roots of $Q_i$. Assume that $h$ has an orbit of length $k$ with $1 < k < q - 1$. Then $h^k$ fixes at least two roots and therefore is the identity element in $\text{Gal}(L_i/K((t)))$. Contradiction. Therefore $h$ acts on each $A_i$ by fixing one point and moving the rest cyclically.

$\square$

Remark 3.4. When $\text{char} K = 0$ Lemmas 3.3 and 2.2 imply that $G$ is 2-transitive and contains a transposition, so $G = S_d$.

In section 4 we use Lemma 3.3 to figure out the possibilities for the sectional monodromy groups of nonstrange curves. The element $h$ of Lemma 3.3 will play an important role. When $q = 2$ the element $h$ is the identity and we will use some alternative arguments based on the following lemma.

Lemma 3.5. Let $X \subset \mathbb{P}^3$ be a degree $d$ projective integral curve. Assume that the Gauss map of $X$ has separable degree $s$ and inseparable degree $q$. Then $sq < d$. Let $k > 2$ be an integer. Let

$$L = \left\lfloor \frac{(k + 2)(k + 3)}{6} \right\rfloor - 1, \quad P = \binom{k + 3}{3} - (k + 1)L - 2.$$ 

Then either $2sL + P \leq kd$ or $d \leq k^2 - L$. 

8
Proof. Suppose $sq \geq d$. Take a tangent line $\ell$ to $X$ that is tangent at $s$ points with multiplicity $q$ at each one. Consider a hyperplane $H$ that contains $\ell$ and some point of $X$ not on $\ell$. Then the intersection number of $X$ and $H$ is at least $sq + 1 > d$. Contradiction. Therefore $sq < d$.

Choose $L$ distinct tangent lines $\ell_1, ..., \ell_L$ of $X$, so that each $\ell_i$ has exactly $s$ points of tangency. Since

$$\dim H^0(\mathbb{P}^3, \mathcal{O}(k)) - (P + 2) = \binom{k + 3}{3} - (P + 2) \geq (k + 1)L = L \dim H^0(\mathbb{P}^3, \mathcal{O}(k)),$$

there exists a $P + 2$ dimensional family of degree $k$ surfaces containing $\ell_1, ..., \ell_L$. If there are two distinct degree $k$ surfaces $Q_1, Q_2$ that contain $\ell_1, ..., \ell_L$ and $X$, then $\deg X \leq \deg Q_1 \cap Q_2 - \deg \cup_i \ell_i = k^2 - L$. Assume $d > k^2 - L$. Then there is a two-dimensional family of degree $k$ surfaces that contain the lines $\ell_1, ..., \ell_L$ and $P$ distinct points on $X$. Choose one such surface $Q_k$ that does not contain $X$. Then $Q_k \cap X$ has at least $sL$ points of multiplicity greater than 2 and at least $P$ more points. Hence $2sL + P \leq kd$ as claimed. \hfill \Box

4. SECTIONAL MONODROMY GROUPS OF NONSTRAINS CURVES

The main result of this section is Theorem 4.4 that describes all possible sectional monodromy groups of nonstrange space curves. The sectional monodromy group of a nonstrange space curve is triply transitive by Proposition 2.8. Triply transitive permutation groups can be classified; see, for example, [Rat87, Theorem 2.4].

Proposition 4.1. If $G$ is a triply transitive permutation group of degree $d$ then either $G \supset A_d$ or one of the following holds.

1. $G = \text{AGL}_n(2)$, $d = 2^n$;
2. $G = G_1$, $d = 16$;
3. $\text{PSL}_2(r) \subset G \subset \text{PGL}_2(r)$, $d = r + 1$, $r$ is a power of a prime;
4. $G = M_{11}$, $d = 11$;
5. $G = M_{12}$, $d = 12$;
6. $G = M_{23}$, $d = 23$;
7. $G = M_{24}$, $d = 24$.

We will also need two geometric statements before proving Theorem 4.4.

Proposition 4.2 (Kaji). Let $X \subset \mathbb{P}^r$, $r \geq 3$ be a projective integral nonstrange curve, let $\gamma_X : X \to X^*$ be its Gauss map. Let $Y \subset \mathbb{P}^{r-1}$ be the projection of $X$ from a general point $P \in \mathbb{P}^r$. Identify $K(X)$ and $K(Y)$ via the projection from $P$. Then the subfield $K(X^*)$ of $K(X)$ defined by $\gamma_X$ and the subfield $K(Y^*)$ of $K(X) = K(Y)$ defined by the Gauss map $\gamma_Y : Y \to Y^*$ coincide.

Proof. See [Kaj89, Theorem 2.1] and the remark following the theorem. \hfill \Box

Proposition 4.3 ([BC00, Theorem 3.1]). Let $X \subset \mathbb{P}^3$ be a smooth curve of degree $d$. Assume that for a general point $P$ of $X$ there is no tangent line to $X$ at a point $Q \neq P$ that intersects with the tangent line at $P$. Then either $d = 3$ and $X$ is a twisted cubic or $d = q + 1$ for some power $q$ of the characteristic. In the latter case $X$ is rational and isomorphic to the projective closure of the parametrized curve $(t, t^q, t^{q+1})$.

The following theorem is the main result of this section.
Theorem 4.4. Let $X \subset \mathbb{P}^m$, $m \geq 3$ be a nondegenerate integral nonstrange curve of degree $d$. Then one of the following holds.

1. The sectional monodromy group $G$ contains the alternating group $A_d$.
2. $m = 3$ and $X$ is projectively equivalent to the rational curve given as the projective closure of the parametrized curve $(t, t^q, t^{q+1}) \subset \mathbb{A}^3$ for some power $q$ of the characteristic. In this case $G = \text{PGL}_2(q)$.

Proof. Let $s, q$ be the separable and inseparable degrees of the Gauss map of $X$. By Proposition 4.2, $s$ and $q$ are also the separable and inseparable degrees of a general projection of $X$. Lemma 3.5 applied to a generic projection of $X$ to $\mathbb{P}^3$ implies that $sq < d$. Let $X'$ be a general projection of $X$ to $\mathbb{P}^2$. Proposition 4.2 implies that $G_X = G_{X'}$ as permutation groups. Since $X'$ is a plane curve Lemma 3.3 applies. We conclude that if $q = 1$ the group $G$ contains a transposition, and therefore $G = S_q$. Assume $q > 1$ and fix a decompositions $\Omega = A_1 \cup \ldots \cup A_s \cup B$, subgroups $H, H_i \subset G$, and an element $h \in H$ as in Lemma 3.3. We will use the properties of $(A_i, B, H_i, H, h)$ stated in Lemma 3.3 throughout this proof. Since $sq < d$ the set $B$ is nonempty.

The group $G$ is triply transitive by Proposition 2.8. Therefore it is on the list of Proposition 4.1. We analyze each possibility.

1. $G \subset \text{AGL}_n(2)$ and $\Omega = \mathbb{F}_2^n$. This case also covers the $G_1$ group of Proposition 4.1 since $G_1$ is a permutation subgroup of $\text{AGL}_4(2)$. Assume first that $q \neq 2$. The element $h \in G$ acts as a product of $s q - 1$-cycles. Since $h$ fixes at least one point, we can interpret $h$ as an operator $A \in \text{GL}_n(\mathbb{F}_2)$. Consider $V := \mathbb{F}_2^n$ as an $\mathbb{F}_2[t]$ module, where $t$ acts as $A$. Since $A$ has fixed points and is not equal to the identity, one of the following cases holds.

   1. $V$ has a submodule $W$ isomorphic to $\mathbb{F}_2[t]/(t-1)^n$ for some $n > 1$. Let $M$ be the restriction of $A$ to $W$. Then $M^q - 1 = 0$. So $t^{q-1} - 1$ is divisible by $(t-1)^n$ in $\mathbb{F}_2[t]$, therefore $n \leq v_2(q - 1)$. This implies that the number of points in $W$ is $2^n \leq q - 1$. But $q - 1$ is the minimal size of a nontrivial orbit of $h$, contradiction.

   2. $V = V_1 \oplus V_2$, where $V_1 \neq 0$ is indecomposable and $V_2$ contains all nonzero fixed points of $A$. Then for every fixed point $v$ of $A$, $v + V_1$ is invariant under the action of $A$. Therefore, $A$ has at least as many orbits of length greater than 1 as it has fixed points. On the other hand, since $A$ acts on $A_1$ via fixing one point and permuting the rest cyclically and also fixes $B \neq \emptyset$, $A$ has more fixed points than it has orbits of length greater than one. Contradiction.

Assume $q = 2$. Consider an element $g \in H_1$, $g \neq \text{id}$. Then $g$ acts as a product of transpositions. Since $g$ fixes $B$, we can interpret $g$ as an element of $\text{GL}_n(\mathbb{F}_2)$. Nontrivial elements of $\text{GL}_n(\mathbb{F}_2)$ fix at most $2^{n-1}$ elements, when applied to $g$ this yields $\#A_1 + \#B = 2 + \#B \leq 2^{n-1}$, so $s = 1/2(\#H - \#B) \geq 2^{n-2} + 1$. We will now use the inequalities of Lemma 3.5 with a suitable $k$ to get a contradiction.

   • If $d \leq 4$, then $g$ is a transposition and $G = S_d$.
   • If $d = 8$ use Lemma 3.5 with $k = 3$. In this case $L = 4, P = 2$ and the degree $d$ is larger than $k^2 - L = 5$. Therefore $8s + 2 \leq 24$, while $s \geq 3$, contradiction.
   • Assume $d = 16$ and $s = 5$. Choose nontrivial elements $h_1 \in H_1$ and $h_2 \in H_2$. Each $h_i$ fixes at least 8, and therefore exactly 8 points. So $h_i$ acts on $A_j, j \neq i$ as a transposition. Therefore $h_i h_j$ has exactly 12 fixed points. The group AGL$_4(2)$ has no elements fixing 12 points, contradiction.
We have shown that

We consider several subcases.

Proposition 2.8 implies that the curve

The case

The only pairs of prime powers

or equivalently

of fixed points of

least

A

on

element

h

and act transitively on

of transpositions. However elements of

is at least as large as the number of nontrivial orbits

action of

number

is a power of the Frobenius. Since

onto

AGL

pointwise stabilizer of three points in

generated by the Frobenius, and thus cannot have exactly

and fixes

Assume

holds. Contradiction.

We apply Lemma 3.5 with

\( r \leq 3 \). If

we apply Lemma 3.5 with

\( 2 \rangle + 1 \) gives

\( 18(2^{n-1} + 2) + 1 \leq 2^{n+3} \). Contradiction.

(2) \( \text{PSL}_2(r) \subset G \subset \text{PGL}_2(r) \) and \( \Omega = \mathbb{P}^1(\mathbb{F}_r) \). In this case \( \deg X = r + 1 \). Suppose \( q < r \). We consider several subcases.

(1) \( s = 1 \). In this case the set \( B \) of Lemma 3.3 contains \( r + 1 - q \geq 2 \) elements. Suppose \( r - 1 = q \) and \( q > 2 \). Then the element \( h \in H \) acts as a \((q - 1)\)-cycle and fixes 3 points. The stabilizer of a triple of points in \( \text{PGL}_2(r) \) is a cyclic group generated by the Frobenius, and thus cannot have exactly 3 fixed points when \( q > 2 \). If \( q = 2 \), then \( G \) contains a transposition. Therefore \( r - 1 - q \geq 3 \). The pointwise stabilizer of three points in \( \text{PGL}_2(q) \) is abelian and maps surjectively onto \( \text{AGL}_1(q) \) by Lemma 3.3 Contradiction.

(2) \( s \geq 2, q > 2 \). The element \( h \in \text{PGL}_2(r) \) fixes \( s + \#B \geq 3 \) points, and therefore \( h \) is a power of the Frobenius. Since \( h \) only has orbits of sizes 1 and \( q - 1 \), the number \( q - 1 \) must be prime. Thus \( \mathbb{F}_r = \mathbb{F}_{\ell^k} \) for some prime power \( \ell \). The action of \( h \) on \( \mathbb{F}_{\ell^k} \) is such that the number of fixed points is \( s + \#B - 1 \) which is at least as large as the number of nontrivial orbits \( s \). So \( \ell^{k-1} - \ell \leq (q - 1)\ell \).

The only pairs of prime powers \((\ell, q)\) with \( q > 2 \) that satisfy this inequality are \((2, 4), (2, 3), \) and \((3, 3)\). These correspond to \((r, q)\) being \((8, 4), (4, 3)\), and \((9, 3)\). The case \((r, q) = (4, 3)\) is impossible since \( s > 1 \). Suppose \((r, q) = (9, 3)\). The element \( h \) must have exactly \( 3 + 1 \) fixed points, and therefore \( s = 3 \). Any element \( g \in H_1 \), \( g \neq \text{id} \) fixes \( B \cup A_1 \). Since \( \#B + \#A_1 \geq 3 \), the element \( g \) must equal to the Frobenius in a degree \( q - 1 = 2 \) extension, and therefore be a product of transpositions. However elements of \( H_1 \) preserve the decomposition \( A_2 \cup A_3 \) and act transitively on \( A_2 \), contradiction. Similarly, in the case \((r, q) = (8, 4)\) the element \( h \) must have \( 3 \) fixed points, and hence \( s = 2 \). In this case any nontrivial element of \( H_1 \) is a power of the Frobenius, and hence \( H_1 \) can not act transitively on \( A_2 \), contradiction.

(3) \( q = 2, s \neq 1 \). If \( s = 2 \), then a nontrivial element of \( H_1 \) is a transposition, proving \( G = S_4 \). In particular we can assume \( r \neq 7 \). A nontrivial element \( g \in H_1 \) fixes at least 3 points, and therefore is a power of the Frobenius. Frobenius acting on an extension of finite fields \( \mathbb{F}_r/\mathbb{F}_\ell \) can not fix more than \( \sqrt{r} \) points. Hence the number of fixed points of \( g \) is at most \( \sqrt{r} + 1 \), so \( \#B + \#A_1 = r + 3 - 2s \leq \sqrt{r} + 1 \), or equivalently \( s \geq (r - \sqrt{r})/2 + 1 \). Lemma 3.5 applied with \( k = 3 \) gives \( s \leq 3/8r - 1/4 \). Therefore \( 3/8r - 1/4 \geq (r - \sqrt{r})/2 + 1 \), which is equivalent to \( \sqrt{r} \geq 1/4r + 5/2 \). The last inequality is never satisfied, contradiction.

We have shown that \( q \) can not be less than \( r \). Suppose \( q = r \). The group \( \text{PGL}_2(q) \) is not quadruply transitive unless it contains \( A_{q+1} \) (i.e. unless \( q = 2, 3, 4 \)). Therefore Proposition 2.8 implies that the curve \( X \) lies in \( \mathbb{P}^3 \). Take a smooth point \( P \) of \( X \) and consider the family of hyperplanes passing through the tangent line to \( X \) at \( P \). Since
the multiplicity of the intersection of such a hyperplane with \( X \) at \( P \) is at least \( q \) and \( \deg X = q + 1 \), the curve \( X \) is smooth. If two tangent lines to \( X \) meet, then the plane containing both of them intersects \( X \) with multiplicity \( 2q > q + 1 \) which is impossible. Therefore we can apply Proposition 4.3. We conclude that \( X \) is projectively equivalent to the projective closure of the rational curve \((t, t^q, t^{q+1})\). The monodromy group in this case is \( \text{PGL}_2(q) \), see [Rat87, Example 2.15].

(3) \( G \) is one of the Mathieu groups and the action on \( \Omega \) is in the list of Theorem 3.1. From Lemma 3.3 it follows that there is an element in \( G \) that acts via a product of \( (q - 1) \)-cycles. Take an element \( g, G \) that maps onto an element of order \( p \) in \( \text{AGL}_1(p) \). Replacing \( g \) by \( g^k \) is necessary we can assume that \( g \) acts as a nontrivial product of cycles of length \( p \). Cycle types of the Mathieu groups (in different permutation representations) are listed in Appendix A (borrowing from [WWT]). Together the existence of cycle type \((q - 1)^s\), existence of a product of \( p \)-cycles, and the condition \( sq < d \) leaves the following cases.

(1) \( G = M_{11}, d = 11, q = 2, s = 4 \). Any nontrivial element of \( H_1 \) has cycle type \( 2^t, 1 \leq t \leq 3 \). However there are no element with such cycle type in this representation.

(2) \( G = M_{11}, d = 12, s = 5, q = 2 \). All elements having cycle type \( 2^t, t > 0 \) have cycle type \( 2^4 \). These cannot form the subgroup \( H \), since taking a product of two distinct such elements gives an element of type \( 2^2 \).

(3) \( G = M_{11}, d = 11, q = 5, s = 2 \). Every element of \( H_1 \) fixes at least 6 points; \( M_{11} \) has no such elements.

(4) \( G = M_{11}, d = 12, q = 2, s = 5 \). Any element of type \( 2^t \) with \( t > 0 \) has \( t = 4 \). Therefore every element of \( H \) is a product of 4 transpositions. A product of two distinct elements acting as products of four \( 2 \)-cycles is not a product of four \( 2 \)-cycles.

(5) \( G = M_{11}, d = 12, q = 2, s = 6 \). We use Lemma 3.5 with \( k = 3 \). We have \( L = 4, P = 2 \) and \( d \leq k^2 - L = 5 \). Therefore the inequality \( 2sL + P \leq dk \) must hold. But \( 2sL + P = 50 > 33 = dk \). Contradiction.

(6) \( G = M_{23}, d = 23, q = 2 \). Every element with cycle type \( 2^t, t > 0 \) has \( t = 8 \). Since every element of \( H_1 \) is a product of at most \( s - 1 \) transpositions, \( s \geq 9 \). Also \( sq < d \) implies \( s \leq 11 \). Since \( H \) acts transitively on each \( A_i \), there exist two distinct nontrivial elements \( h_1, h_2 \in H \) each having the cycle type \( 2^8 \). But \( h_1h_2 \) cannot have cycle type \( 2^8 \), contradiction.

(7) \( G = M_{24}, d = 24, q = 2, s \geq 8 \). Since \( sq < d \), we have \( s \leq 11 \). In this representation every \( 2^t \) element of \( H \) has \( t = 0, 8 \). A product of two \( 2^8 \) elements of \( H \) cannot be a \( 2^8 \) element. Contradiction.

\( \square \)

**Remark 4.5.** Suppose \( \text{char} \, K \neq 2 \). Then the group \( G \) is contained in the alternating group if and only if the separability degree of the Gauss map is even [Rat87, Theorem 2.10]. When \( \text{char} \, K = 2 \) we do not know under what conditions \( G \) is equal to \( S_n \).
5. Galois groups of trinomials

In this section we study the Galois group $G$ of the polynomial $x^n + ax^m + b$ over the field $K(a, b)$. The following theorem of Cohen covers most of the previously known results about $G$.

**Theorem 5.1** ([Coh80 Corollary 3]). Assume that $n$ and $m$ are relatively prime, $p \nmid m(n - m)$ and if $m = 1$ or $m = n - 1$ assume additionally that $p \nmid n$. Then $A_n \subset G$. Moreover, if $p$ is odd, then $G = S_n$.

Some cases not covered by Theorem 5.1, such as a trinomial with $G = M_{11}$, are described in [Uch70]. Our goal is to compute all the possibilities for $G$.

We begin by fixing notation. Throughout this section, $(n, m)$ is a pair of relatively prime positive integers, $X_{n,m}$ denotes the projective rational curve plane $x^n = y^m z^{n-m}$, and $G = G_{n,m}$ is the sectional monodromy group of $X_{n,m}$. An affine parametrization of $X_{n,m}$ is $(t^m, t^n)$. Therefore $G$ is also the Galois group of the trinomial $x^n + ax^m + b$ over $K(a, b)$.

Without loss of generality we assume that $m < n/2$ since $X_{n,m} \approx X_{n,n-m}$.

We start by describing properties of tangent lines and Gauss maps of the curves $X_{n,m}$.

**Proposition 5.2.**

1. If $n, m$ and $(n - m)$ are prime to $p$, then $X_{n,m}$ is nonstrange. In this case the Gauss map has separability degree 1, and inseparability degree 1 when $p > 2$ and 2 when $p = 2$.

2. Assume that $k \in \{n, m, n - m\}$ is divisible by $p$. Write $k = qd$ where $q$ is the largest power of $p$ that divides $k$. Then $X_{n,m}$ is strange and the Gauss map has inseparability degree $q$ and separability degree $d$.

**Proof.** If $p|m$, then $p \nmid n$, so we can replace $X_{n,m}$ by the projectively isomorphic curve $X_{n,n-m}$, and $p \nmid n - m$. Thus we may assume $p \nmid m$. An affine equation of $X_{n,m}$ is $x^n = y^m$. The tangent line to $X_{n,m}$ at the point $(\alpha^n, \alpha^m)$ is given by the equation

$$n\alpha^{m(n-1)} x - m\alpha^{n(m-1)} y = (n - m)\alpha^{nm}.$$  

Restricting the equation $x^n = y^m$ to the tangent line $Y = \frac{n}{m}\alpha^{n-m} X - (\frac{n}{m} - 1)\alpha^n$ gives the polynomial

$$p(X) = X^n - \left(\frac{n}{m}\alpha^{n-m} X - \left(\frac{n}{m} - 1\right)\alpha^n\right)^m.$$  

Recall that the inseparability degree $r$ of the Gauss map is greater than 1 if and only if $\alpha^m$ is a root of $p(X)$ with multiplicity greater than 2; in this case $r$ is equal to the multiplicity of the root $\alpha^m$. Set $X = \alpha^m + Z$. Then

$$p(X) = (Z + \alpha^m)^n - \left(\frac{n}{m}\alpha^{n-m} Z + \alpha^n\right)^m.$$  

The coefficient of $Z^2$ is

$$\left(\frac{n(n-1)}{2} - \frac{n(m-1)}{2}\right)\alpha^{m(n-2)}.$$  

This coefficient is identically zero if and only if either $p|n$ or $p|(n - m)$.}
Proof. Both parts of the statement are proved similarly to Lemma 3.3. We will pick a tangent line \( \ell \) to \( X_{n,m} \). We will then restrict the covering to a family of lines that includes \( \ell \) and

(1) \( p \nmid n, p \nmid n-m \). In this case the inseparability degree of the Gauss map is 1. We can recover the point \((\alpha^n, \alpha^m)\) from its tangent line

\[
na^{m(n-1)}X - ma^{n(m-1)}Y = (n-m)\alpha^{nm}
\]

using ratios of the coefficients of the equation. Therefore the separability degree of the Gauss map is also 1. Finally the dual curve \((na^{m(n-1)} : ma^{n(m-1)} : (n-m)\alpha^{nm})\) is not a line, therefore the tangent lines do not pass through one common points and the curve is nonstrange.

(2) \( p | n \). Let \( q \) be the largest power of \( p \) dividing \( n \), write \( n = qd \). In this case the equation of the tangent line becomes \( Y = \alpha^n \), and therefore the curve is strange. The Gauss map in affine coordinates is \( \alpha \rightarrow \alpha^n \), therefore it has separable degree \( d \) and inseparable degree \( q \).

(3) \( p | (n-m) \). Let \( q \) be the largest power of \( p \) dividing \( n-m \), and let \( n = qd \). The equation of the tangent line becomes \( Y = \alpha^{n-m}X \). Therefore the curve is strange. The Gauss map in affine coordinates is just \( \alpha \rightarrow \alpha^{n-m} \) therefore the separable degree of the Gauss map is \( d \) and the inseparable degree is \( q \).

\[ \square \]

We now prove a stronger version of Lemma 3.3 for curves \( X_{n,m} \).

**Lemma 5.3.** Let \( X = X_{n,m} \) be one of the trinomial curves. Choose a geometric point \( \delta \) of \( (\mathbb{P}^2)^* \) above which the covering \( \pi_X \) is \( \text{étale} \). Denote by \( \Omega \) the fiber of \( \pi_X \) above \( \delta \), so the group \( G_X \) acts on \( \Omega \) by permutations. Then the following hold.

1. Assume \( p | n \). Write \( n = qd \) with \( q \) a power of \( p \) and \( d \) prime to \( p \). Then there exists a decomposition \( \Omega = A_1 \sqcup \ldots \sqcup A_d \), a subgroup \( H \subset G \), a collection of subgroups \( H_i \subset G \), \( i = 1, \ldots, d \), and an element \( h \in H \) with the following properties.
   - For every \( i \) the set \( A_i \) is of cardinality \( q \).
   - The image of \( H \) in \( \text{Sym}(A_i) \) equals \( \text{AGL}_1(q) \) embedded via its action on \( \mathbb{A}^1(\mathbb{F}_q) \).
   - The element \( h \in H \) acts on each \( A_i \) with one fixed point and one orbit of size \( q-1 \).
   - The group \( H_i \) acts on \( A_i \) with one fixed point and one orbit of size \( q-1 \). The image of \( H_i \) in \( \text{Sym}(A_j) \) for \( i \neq j \) contains \( \text{AGL}_1(q) \) embedded via its action on \( \mathbb{A}^1(\mathbb{F}_q) \).

2. Assume \( p | n-m \). Write \( n-m = qd \) with \( q \) a power of \( p \) and \( d \) prime to \( p \). Then there exists a decomposition \( \Omega = A_1 \sqcup \ldots \sqcup A_d \sqcup B \), a subgroup \( H \subset G \), a collection of subgroups \( H_i \subset G \), \( i = 1, \ldots, d \), and an element \( h \in H \) with the following properties.
   - For every \( i \) the set \( A_i \) is of cardinality \( q \).
   - The image of \( H \) in \( \text{Sym}(A_i) \) equals \( \text{AGL}_1(q) \) embedded via its action on \( \mathbb{A}^1(\mathbb{F}_q) \).
   - The element \( h \in H \) acts on each \( A_i \) with one fixed point and one orbit of size \( q-1 \).
   - The image of \( H \) in \( \text{Sym}(B) \) is \( \mathbb{Z}/m\mathbb{Z} \) in its natural embedding; \( h \) maps to a generator of \( \mathbb{Z}/m\mathbb{Z} \).
   - The group \( H_i \) fixes \( A_i \cup B \) and acts transitively on each \( A_j \) for all \( j \neq i \).

**Proof.** Both parts of the statement are proved similarly to Lemma 3.3. We will pick a tangent line \( \ell \) to \( X_{n,m} \). We will then restrict the covering to a family of lines that includes \( \ell \) and
compute the inertia group at \([\ell] \in (\mathbb{P}^2)^*\). To calculate the inertia groups we will use Lemma 3.2 and a computation of local uniformization.

(1) Replacing \(K\) with a larger algebraically closed field if necessary, we can choose an element \(u \in K\) that is not a root of unity. Consider the affine model \(x^n = y^m\) of \(X\). The line \(y = u^n\) is tangent to \(X\). Choose a root of unity \(\zeta_d \in K\). The points of tangency are \(P_i = (\alpha_i, u^n)\), where \(\alpha_i = \zeta_d^i u^n\). Let \(x_i = x - \alpha_i\). A local uniformization of \(X\) at \(P_i\) is given by \((\alpha_i + x_i, p_i(x_i))\), where \(p_i(x_i) = u^n(1 + x/\alpha_i)^{m/n}\). The \(x^{q+1}\) coefficient of \(p_i\) is zero. Choose an element \(\alpha \in K\) and identify \(\Omega\) with the intersection of \(X_{n,m}\) and the line \(\ell\) given by the equation \(y - u^n = t(x - \alpha)\) over the field \(K((t))\).

Let \(H(\alpha)\) be the Galois group of the field extension \(L_\alpha\) obtained by adjoining to \(K((t))\) the coordinates of the intersection. Then \(H(\alpha)\) acts on \(\Omega\) and is a subgroup of \(G\). The field \(L_\alpha\) is the field obtained by adding the roots of \(x^n - tx^m + t\alpha - u^n\) to \(K((t))\). In particular it is separable. Let \(A_i \subset \Omega\) be the set of intersection points that reduce to \(P_i\). The \(x\)-coordinates of the points in \(\ell \cap X\) that reduce to \(P_i\) are the positively valued roots of the equation \(p_i(x_i) - u^n = tx_i + t\alpha - t\alpha\). Lemma 3.2 applies with \(a_0 = t(\alpha - \alpha_i), a_1 = t, a_q = u^q d_\alpha^{-mq}/m, a_{q+1} = 0\). Hence if \(\alpha \neq \alpha_i\), the Galois group of the field \(L_{i,\alpha}\) obtained by adding these roots to \(K((t))\) equals \(\text{AGL}_1(q)\).

When \(\alpha = \alpha_i\) the equation has a rational root \(x_i = 0\) and the rest of the roots have valuation \(1/(q-1)\). Therefore when \(\alpha = \alpha_i\) the field \(L_{i,\alpha}\) is the unique extension of \(K((t))\) of degree \(q - 1\). Let \(H_i\) be the group \(H(\alpha_i)\). Fix \(\alpha \in K\) distinct from each \(\alpha_i\) and let \(H\) be the group \(H(\alpha)\). We have shown that the actions of \(H\) and \(H_i\)'s on \(A_j\)'s are as claimed. Now we need to show the existence of \(h \in H\) that acts on each \(A_i\) as a \((q - 1)\)-cycle. The extension \(L_{i,\alpha}\) has ramification index \(q(q - 1)\) and therefore contains the field \(K((t^{1/(q-1)})\). Let \(h \in H\) be an element that surjects onto a generator of \(\text{Gal}(K((t^{1/(q-1)}))/K((t)))\). Then the order of \(h\) acting on \(A_i\) is \(q - 1\). Elements of \(\text{AGL}_1(q)\) of order \((q - 1)\) act with two orbits of lengths \(1\) and \(q - 1\).

(2) Consider the affine model \(x^n = y^m\) of \(X\). Choose an element \(u \in K\) that is not a root of unity. Let \(\ell\) be the tangent line \(y = u^{n-m}x\) to \(X\). Choose a root of unity \(\zeta_d\). The points of tangency are \(P_i := (\zeta_d^i u^n, \zeta_d^i u^n)\). The intersection \(\ell \cap X\) consists of points \(P_i\) and the point \((0,0)\). For an element \(\alpha \in K\) let \(\ell_\alpha\) denote the line \(y = (t + u^{n-m})x - \alpha t\) over the field \(K((t))\). Identify \(\Omega\) with the intersection \(\ell_\alpha \cap X\) over \(K((t))\). The absolute Galois group of \(K((t))\) acts on \(\Omega\) as a subgroup of \(G\). Let \(A_i \subset \Omega\) be the subset corresponding to points that reduce to \(P_i\), and let \(B\) be the subset that corresponds to points reducing to \(0,0\). Let \(L_\alpha\) be the extension obtained by adding the coordinates of the intersection \(\ell_\alpha \cap X\) to \(K((t))\). Then \(L_\alpha\) is the splitting field of the trinomial \(x^n - (t + u^{n-m})x^m + \alpha\). In particular \(L_\alpha\) is separable. Consider the uniformizer \(x_i = x - \zeta_d^i u^m\) at \(P_i\). Let the local uniformization of \(X\) at \(P_i\) be given by \((\zeta_d^i u^m + x_i, p_i(x_i))\).

The power series \(p_i(x_i) = \zeta_d^i u^m(1 + x_i/(\zeta_d^i u^m))^{m/n} = \zeta_d^i u^m(1 + x_i/(\zeta_d^i u^m))^{(1 + x_i/(\zeta_d^i u^m))^{m/n}}\). The \(x\)-coordinates of the points in the intersection \(\ell_\alpha \cap X\) that reduce to \(P_i\) are the positively valued roots of the power series \(Q_i = p_i(x_i) - (t + u^{n-m})(x_i + \zeta_d^i u^m) + \alpha\). We have

\[Q_i = a_0 + a_1 x_i + a_q x_i^q + a_{q+1} x_i^{q+1} + O(x^{2q}),\]

where \(a_0 = (\alpha - \zeta_d^i u^m), a_1 = -t, a_q = d_m \zeta_d^{i(q-1)} u^{-mq+n}, a_{q+1} = d_m u^{-n(q+1)m} \zeta_d^{-iq}\). For a general \(\alpha\) the expression \(a^q a_{q+1} - a_1 a_q\) has valuation 1. For each \(i\) let \(L_{\alpha,i}\) be the field generated by the positively valued roots of \(Q_i\), and let \(L_\alpha\) be the field obtained.
by adjoining to \( K((t)) \) the coordinates of the intersection of \( X \) with \( \ell_\alpha \). The field \( L_\alpha \) is the compositum of \( L_{\alpha,i} \) for \( i = 1, \ldots, d \). Let \( H(\alpha) \) be the Galois group of the extension \( L_{\alpha}/K((t)) \). Lemma 3.2 implies that for a general \( \beta \in K \) the image of \( H(\beta) \) in \( \text{Sym}(A_j) \) is \( \text{AGL}_1(q) \) for all \( i \). Fix one such \( \beta \neq 0 \) and let \( H := H(\beta) \).

We now compute the action of \( H(\alpha) \) on \( B \) for \( \alpha \neq 0 \). The elements of \( B \) are the roots of \( Q(x) = x^n - (t + x^{n-m})x^m + ct \) that reduce to 0 modulo \( t \). The Newton polygon of \( Q(x) \) contains only one segment of positive slope, it connects \((0,1) \) and \((m,0) \). Since the slope is \( 1/m \) and \( m \) is prime to \( p \), the elements of \( B \) are permuted cyclically by the group \( H(\alpha) \) for every \( \alpha \neq 0 \). Let \( h \in H \) be an element that surjects onto a generator of \( \text{Gal}(K((t))/K((t))) \). Since the field extension obtained by adjoining \( B \) to \( K((t)) \) is \( K((t^{1/m})) \), the element \( h \) acts on \( B \) through a cyclic permutation. The field \( L_{\alpha,i} \) has ramification index \( q(q-1) \) and therefore contains \( K((t^{1/q}) \). Hence the action of \( h \) on \( A_i \) has order \( q-1 \), so \( h \) acts on each \( A_i \) by fixing one point and permuting the rest cyclically.

Let \( L_i \) denote the field \( L_{\zeta_i^m} \). Let \( H_i \) be the Galois group of \( L_i \) over \( K((t^{1/LCM(m,q-1)})) \).

Then \( H_i \) fixes \( B \). When \( \alpha = \zeta_i^m \) the power series \( Q_i \) has root 0. The positive slope part of the Newton polygon of \( Q_i/x_i \) is a single segment from \((0,1) \) to \((q-1,0) \). Therefore \( H_i \) fixes \( A_i \). For \( j \neq i \) the positive slope part of the Newton polygon of \( Q_j \) is a segment from \((0,1) \) to \((q,0) \), therefore \( H_i \) acts transitively on \( A_j \) for \( j \neq i \).

\[ \square \]

**Theorem 5.4.** Suppose \( m \) and \( n \) are relatively prime integers satisfying \( m \leq n/2 \). Let \( G \) be the Galois group of the polynomial \( P(x) := x^n + ax^m + b \) over \( K(a,b) \).

1. If \( m = 1 \) and \( n = p^d \), then \( G = \text{AGL}_1(p^d) \).
2. If \( m = 1 \), \( n = 6 \), and \( p = 2 \), then \( G = \text{PSL}_2(5) \).
3. If \( m = 1 \), \( n = 12 \), and \( p = 3 \), then \( G = M_{11} \).
4. If \( m = 1 \), \( n = 24 \), and \( p = 2 \), then \( G = M_{24} \).
5. If \( m = 2 \), \( n = 11 \), and \( p = 3 \), then \( G = M_{11} \).
6. If \( m = 3 \), \( n = 23 \), and \( p = 2 \), then \( G = M_{23} \).
7. Let \( q := p^k \) for some \( k \). If \( n = (q^d-1)/(q-1) \), \( m = (q^s-1)/(q-1) \) for some \( s,d \), then \( G = \text{PGL}_d(q) \).
8. If none of the above holds, then \( A_n \subset G \).

**Proof.** We break the proof into cases corresponding to the cases of Proposition 5.2. The case \( n = 2 \) is trivial. In what follows we assume \( n > 2 \) so that \( m < n/2 \) since \( m, n \) are relatively prime.

1. Assume \( p \nmid nm(n-m) \). By Proposition 5.2 the curve \( X_{m,n} \) is nonstrange and the Gauss map is either birational or purely inseparable of degree two. In any case Lemma 3.3 implies that \( G \) contains a transposition; hence \( G = S_n \).
2. Assume \( p \mid n \). Consider the specialization of \( x^n + ax^m + b \) to the polynomial \( P(x) := x^n + t^{-1}x^m + 1 \) over the field \( K((t)) \). The Newton polygon of \( P \) consists of two segments: one from \((0,0) \) to \((m,-1) \) and one from \((m,-1) \) to \((n,0) \). Since \( n-m \) and \( m \) are relatively prime and are both prime to \( p \), the group \( G \) contains an \( m \)-cycle and an \( (n-m) \)-cycle. If \( m \neq 1 \), then \( A_n \subset G \) by Theorem 3.1. If \( m = 1 \) and \( A_n \not\subset G \), then Theorem 3.1 implies that one of the following holds
   1. \( n = p^d \). In this case the Galois group is \( \text{AGL}_1(p^d) \), see Rat87 Example 2.17.
(2) \( n = \ell + 1 \) for some prime \( \ell \) and \( G = \text{PSL}_2(\ell) \) or \( G = \text{PGL}_2(\ell) \). Write \( n = qd \) for \( d \) prime to \( p \) and a power \( q \) of \( p \). Proposition 5.2 states that in this case the Gauss map has inseparable degree \( q \) and separable degree \( d \). If \( d = 1 \), then \( n \) is a power of \( p \), which is precisely the case \([1]\) above. Assume \( d > 1 \). Lemma 5.3 applies in this case with \( B = \emptyset \). The group \( H_1 \) surjects onto \( \text{AGL}_1(q) \) and therefore has order divisible by \( p \). Take an element \( g_1 \in H_1 \) of order \( p \), so that it acts as a nontrivial product of cycles of length \( p \) and fixes \( A_1 \). Since no element of \( \text{PGL}_2(\ell) \) can fix three points, \( \# A_1 = q = 2 \). The element \( g_1 \) fixes two points and acts as a product of transpositions. There is a unique such element, namely multiplication by \(-1\). In particular \( g_1 \) acts as a transposition on \( A_i \) for \( i > 1 \). Take an element \( g_2 \in H \) that acts on \( A_1 \) as a transposition. If \( d \geq 4 \), then either \( g_2 \) or \( g_1g_2 \) fixes at least four points, contradiction. If \( d = 2 \), then \( g_1 \) acts a transposition and so \( G = S_n \). If \( d = 3 \), then \( \ell = 5 \) (and \( q = 2 \)). Suppose \( \ell = 5 \), \( q = 2 \). There is a factorization

\[
x^6 + ax + b = \left(x^3 + cx^2 + c^2\alpha x + \frac{a}{c^2} + \alpha c^3\right) \left(x^3 + cx^2 + (c^2\alpha + c^2)x + \frac{a}{c^2} + (\alpha + 1)c^3\right),
\]

where \( \alpha \in K \) satisfies \( \alpha^2 + \alpha + 1 = 0 \) and \( c \) is a root of \( y^{10} + ay^5 + a^2 + b \). So \( P(x) \) decomposes into product of two cubic polynomials after a degree 10 extension. If \( A_6 \subset G \), then the minimal degree of the extension over which \( P(x) \) splits into a product of two cubic polynomials is

\[
\frac{\# S_6}{\#(S_3 \times S_3)} = \frac{\# A_6}{\#((S_3 \times S_3) \cap A_6)} = 20.
\]

Therefore \( G \not\supset A_6 \). The cubic polynomials appearing in the factorization are conjugate to each other over the field \( K(a,b)(c) \) via an automorphism that fixes \( c \) and sends \( \alpha \) to \( 1 + \alpha \). Therefore the total degree of the extension is at most \( 10\#S_3 = 60 \). Thus \( G = \text{PSL}_2(5) \).

(3) \( n = 12 \). If \( p = 3 \), then \( G = M_{11} \), see \([Uch70, \text{Example 3}]\). Assume \( p = 2 \). In this case either \( G \) is one of the Mathieu groups \( M_{11}, M_{12} \) or \( G \) contains \( A_9 \). Let \( \hat{G} \) denote the Galois group of \( P(x) \) over \( \mathbb{F}_2(a,b) \). Then \( G \) is a normal subgroup of \( \hat{G} \). Over \( \mathbb{F}_2 \) the polynomial \( x^{12} + x + 1 \) factorizes into a product of irreducibles of degrees 3, 4 and 5. Therefore \( \hat{G} \) is a 2-transitive group containing a 4-cycle and thus \( \hat{G} = S_{12} \). Since \( G \) is a normal subgroup of \( \hat{G} \), the group \( G \) contains \( A_{12} \).

(4) \( n = 24 \). In this case either \( G = M_{24} \) or \( G \supset A_{24} \). If \( p = 2 \), then we can apply Serre’s linearization method \([\text{Abh93a}]\). We will find an additive polynomial that is divisible by \( x^{24} + ax + b \). Consider the following sequence of equalities in \( K(a,b)[x]/(x^{24} + ax + b) \):

\[
0 = x^{32} + ax^9 + bx^8 = x^{256} + a^8x^{72} + b^8x^{64}
\]

\[
= x^{256} + a^8(ax + b)^3 + b^8x^{64} = x^{256} + b^8x^{64} + a^{11}x^3 + a^{10}bx^2 + a^9b^2x + a^8b^3
\]

\[
= x^{2048} + b^8x^{512} + a^{88}x^{24} + a^{80}b^8x^{16} + a^{72}b^8x^8 + a^{64}b^{24} = x^{2048} + b^8x^{512} + a^{80}b^8x^{16} + a^{72}b^8x^8 + a^{64}x + a^{88}b + a^{64}b^{24}
\]
The last polynomial in this chain of equalities is an additive polynomial up to a constant. Therefore the group \( G \) is a subquotient of \( AGL_{11}(2) \), thus \( G \) cannot contain \( A_{24} \) since \( 23 \nmid \#AGL_{11}(2) \). Hence \( G = M_{24} \).

Suppose \( p = 3 \). Let \( \hat{G} \) denote the Galois group of \( P(x) \) over \( \mathbb{F}_9(a,b) \). Then \( \hat{G} \) contains \( G \) as a normal subgroups, and therefore \( \hat{G} \) is also a primitive group containing an \( n \)-cycle. From Theorem 3.1 it follows that \( \hat{G} \) is either one of the groups \( PGL_2(23), PGL_2(23), M_{24} \) or \( G \supset A_{24} \). Let \( c \in \mathbb{F}_9 \) be a root of the polynomial \( y^2 - y - 1 \). The polynomial \( x^{24} - x + c \) factors over \( \mathbb{F}_9 \) into a product of irreducible polynomials of degrees 1, 2, 3, 4, 6 and 8. Therefore \( \hat{G} \) contains an element \( g \) with cycle type 1, 2, 3, 4, 6, 8. Since \( g^8 \) fixes at least 15 points, \( \hat{G} \notin PGL_2(23) \). The group \( M_{24} \) has no elements with the cycle type of \( g \) (see Appendix A). Therefore \( \hat{G} \supset A_n \). Since \( G \) is a normal subgroup of \( \hat{G} \), the group \( G \) contains \( A_{24} \).

(3) Assume \( p|m \). Consider the specialization of \( x^n + ax^m + b \) to the polynomial \( P(x) = x^n + t \) over \( K((t)) \). The Galois group of this polynomial is cyclic and we deduce that \( G \) contains an \( n \)-cycle. Theorem 3.1 gives a finite list of possibilities for \( G \). Consider the specialization to the polynomial \( Q(x) = x^n + tx^m + t^2 \) over \( K((t)) \). The Newton polygon of this polynomials has two slopes \( 1/(n - m) \) and \( 1/m \). Since \( p|m \) the roots of \( Q \) span a wildly ramified extension. Any element of the wild inertia will fix at least \( n - m > n/2 \) points. No group from the case (1) of Theorem 3.1 can have nontrivial elements fixing at least half of the points.

(4) Assume \( p|n - m \). Consider the specialization \( x^n + t \) over \( K((t)) \). Since \( n,m \) are relatively prime, the specialized polynomial is separable with cyclic Galois group. Assume \( A_n \notin G \). Since \( G \) contains an \( n \)-cycle, Theorem 3.1 produces a list of possibilities for \( G \). We analyze each case separately.

1. \( C_t \subset G \subset AGL_1(\ell), n = \ell \geq 5 \) is prime. Consider the specialization \( x^n + t^{-1}x^m + 1 \) over \( K((t)) \). The Newton polygon of this trinomial consists of two segments with slopes \( m \) and \( m - n \). Since \( p|(n - m) \) the extension is wildly ramified. Any element from the wild inertia subgroup fixes at least \( m \) roots. Therefore \( m = 1 \). In this case Lemma 5.3 applies with \( \#B = 1 \). The stabilizer of \( B \) in \( G \subset AGL_1(\ell) \) is abelian and has \( AGL_1(q) \) as a subquotient, thus \( q = 2 \). Since \( \ell \geq 5 \) the group \( H_1 \) has an element \( g \neq id \). The element \( g \) fixes at least two points, contradiction.

2. \( PGL_r(\ell) \subset G \subset PGL_r(\ell), n = \#\mathbb{F}^{r-1}(\mathbb{F}_\ell) = (\ell^{r-1} - 1)/(\ell - 1) \). We will prove that \( \ell \) is necessarily a power of \( p \) and that \( m = \#\mathbb{F}^{r'}(\mathbb{F}_\ell) \) for some \( r' < r \).

We can assume that \( PGL_r(\ell) \nsubseteq A_n \). We call a point blue if it is in the set \( B \) and azure if it is in one of the \( A_i \)’s. Lemma 5.3 implies that for every pair of points \( P,Q \in A_i \) there is an element of \( G \) that fixes all blue points and moves \( P \) to \( Q \). Our goal is to show that \( p|\ell \) and \( B \) forms a projective subspace of \( \Omega \). To this end we examine the Galois action on lines that contain blue points.

Consider a line \( l \) in \( \mathbb{P}^r(\mathbb{F}_\ell) \) that contains at least 3 blue points; identify this line with \( \mathbb{P}^1(\mathbb{F}_\ell) \). Any element of \( G \) that fixes all blue points is a power of the Frobenius when restricted to \( l \). Since any azure point can be moved by an element of \( G \) that fixes all blue points, the set of blue points of \( l \) is the set \( l(\mathbb{F}_\ell) \) for some subfield \( \mathbb{F}_t \subset \mathbb{F}_\ell \). There is a subgroup of \( H \) that fixes all blue points and acts transitively on \( A_i \) for every \( i \). Thus if \( l \) contains a point from \( A_i \), then it contains
the whole set $A_i$. Assume $A_i, A_j \subset l$ for some $i \neq j$. The group $H_i$ fixes all 
blue points and $A_i$, and acts transitively on the rest of the line. Therefore $A_i$ 
eq 1 
eq q + t$. Similarly $A_j$ equals \ $l(F_{q^k}) \setminus l(F_t)$, contradiction. Thus $l$ contains points only from one group $A_i$. Since the subgroup of $G$ that fixes $B$ acts transitively on $A_i$, the extension $F_t/F_\ell$ is such that the 
Frobenius acts with only one orbit. There is only one such extension $F_4/F_2$. So 
either $\ell = 4, q = 2$ or every line containing at least three blue points consists 
entirely of blue points. Suppose $\ell = 4, q = 2$. If $r = 2$, then $\text{PGL}_2(4) = A_5$, 
contradiction. Therefore $r > 2$. Suppose $m > 3$. Take a blue point $Q$ not on 
l and let $P \in l$ be an azure point $P \in A_i$. Then $A_i \subset l$. Consider the line 
connecting $Q$ and $P$. If this line contains a blue point $R \neq Q$, then an element 
of $H$ that induces a transposition on $A_i$ does not preserve the collinearity of 
P, $Q$, and $R$. If this line contains an azure point $R \in A_j$, then an element of 
$H_j$ that induces a transposition on $A_i$ does not preserve the collinearity of $P, Q$ 
and $R$, contradiction. Suppose $m = 3, \ell = 4, q = 2, r > 2$. Consider blue points 
P, $Q \in l$ and an azure point $R_1 \in A_i, R_1 \not\in l$ (as in Figure 1). Let $R_2$ denote 
the point of $A_i \setminus \{R_1\}$. The line $l'$ connecting $P$ and $R_1$ does not contain any blue 
points except $P$, therefore there is a point $S \in l', S \in A_j$ for some $j \neq i$. Let 
g \in $H_j$ be an element that maps $R_1$ to $R_2$. Since $g$ fixes $S$ and $P$, $g$ preserves 
l' and therefore $R_2 \in l'$ and $P, R_1, R_2$ are collinear. Similarly $Q, R_1$ and $R_2$ are 
collinear, contradiction. Therefore every line containing at least three blue points 
consists entirely of blue points.

Consider a line $l$ containing exactly two blue points $P$ and $Q$ (if it exists). 
Consider a point $R \in A_i \cap l$. Since the pointwise stabilizer of $B$ in $G$ acts 
transitively on $A_i$, the whole set $A_i$ lies on $l$. We conclude that $q|\ell - 1$. Suppose 
m > 2, so there is a blue point $S \not\in l$ (as in Figure 2). Let $l'$ denote the line 
connecting $S$ and $R$. Since $A_i \subset l$, there is a point $T \in (A_j \cup B) \cap l'$ for some $j \neq i$. 
Take an element $g \in H_j$ that moves $R$ to a different point on $l$. Then $g$ fixes $S$ 
and $T$, and therefore fixes $l'$ but moves $R$ to a point not on $l'$, contradiction. If 
m = 2 and $r > 2$, there exists a line containing exactly one blue point. Therefore, 
assuming that $l$ exists, $q|\ell - 1$ and either $r = 2$ or there exists a line containing 
extactly one blue point.

Assume that there exists a line $l$ that passes through exactly one blue point. If 
all azure points on this line are from the same group $A_i$, take two azure points
Assume that it is not the case that $q \nmid \ell$. Thus we proved that $q \nmid \ell$.

We have proved the following statements.

- Every line that contains at least three blue point is entirely blue.
- If a line containing exactly two blue points exists, then $q \nmid \ell - 1$ and either $r = m = 2$ or a line containing exactly one blue point exists.
- If a line containing exactly one blue point exists, then $p \nmid \ell$.

Assume that it is not the case that $r = m = 2$. Then if a line containing two blue points exists, then $q \nmid \ell - 1$ and a different line passes through exactly one blue point, which in turn implies $p \nmid \ell$, contradiction. Therefore there are no lines that contain exactly two blue points. So every line that contains two blue points, contains at least three, thus is entirely blue. Take a line through a blue and an azure point. It must have exactly one blue point. Therefore $p \nmid \ell$ and the blue points form a projective subspace.

Now we show that the case $r = m = 2$ is impossible. Suppose $r = m = 2$. Then $n = \ell + 1$ must be odd, therefore $\ell = 2^k$. Since $n = qd + 2$, both $q$ and $d$ are odd. Suppose $d = 1$. If $q \neq 3$, then $h^2$ has exactly three fixed points, so $h^2$ is the degree 2 Frobenius. A nontrivial orbit of the degree 2 Frobenius on $\mathbb{A}^1(\mathbb{F}_{2^k})$ has size at most $k$. Since $h^2$ has two nontrivial orbits and two fixed points $2 + 2k \geq 2^k$. We conclude that $k \leq 3$. Since the Frobenius must have two nontrivial orbits, $k$ is equal to 3. Then $q = 6$ which is absurd. If $d = 1$ and $q = 3$, then $G \subset \text{PGL}_2(4) = A_5$, contradiction. Thus we can assume that $d \neq 1$ and, since $d$ is odd, $d \geq 3$. In this case the element $h$ has exactly $d$ fixed points, thus $h$ is a power of the Frobenius, so $d - 1$ is a power of 2. Suppose $q \neq 3$. Since $h$ has a unique orbit of length 2, $h$ is the degree 2 Frobenius and the number of fixed points of $h$ is $3 = \#\mathbb{P}^1(\mathbb{F}_2) = d$. The group $H_1$ fixes $q + 2 > 3$ points, therefore $H_1$ is generated by a power of the Frobenius and $q + 1$, which is the number of fixed points of $H_1$ on $\mathbb{A}^1$, is a power of 2. Therefore $q \equiv -1 \pmod{4}$ hence $2^k = \ell = qd + 1 = 3q + 1 \equiv 2 \pmod{4}$. Thus $\ell = 2$, $n = 3$. But if $\ell = 2$, then $G \supset \text{PGL}_2(2) = S_3$, contradiction. Finally we have to consider the case $q = 3$. Write $d = 2^a + 1$, then $3(2^a + 1) = qd = n - 2 = 2^k - 1$. The last equation can be satisfied modulo 8 only if $d = 5$, $n = 17$. The group $H_1$ has $q + m = 5$ fixed points, and is therefore generated by the degree 4 Frobenius. The degree 4 Frobenius on $\mathbb{P}^1(\mathbb{F}_{16})$ acts with orbits of size 1 and 2, so it cannot act transitively on $A_2$. Contradiction.

Thus we proved that $\ell$ is a power of $p$, $n = 1 + \ell + \ldots + \ell^{r-1}$ and $m = 1 + \ell + \ldots + \ell^{s-1}$.

Assume $n = 1 + \ell + \ldots + \ell^{r-1}$ and $m = 1 + \ell + \ldots + \ell^{s-1}$, for some power $\ell$ of the characteristic. We claim that for such $n, m$ the group $G$ is $\text{PGL}_r(\ell)$. Consider the equation $x^n + ax^m + b$. Let $y = x^{\ell - 1}$. The equation becomes $y^{\ell^{r-1}} + ay^{\ell^{s-1}} + b$. Multiplying by $y$ gives $y^{\ell^r} + ay^{\ell^s} + by$. The roots of the latter form an $\mathbb{F}_\ell$.
vector space, so its Galois group is a subgroup of $GL_r(\ell)$. Since the roots of $x^n + ax^m + b$ correspond to lines in the space of roots of $y^e + ay^c + by$, $G$ is contained in $PGL_r(\ell)$. Since $G$ contains an $n$-cycle and $n \neq 11, 23$, Theorem 3.1 implies that either $PGL_s(t) \subset G \subset PGL_d(t)$ for some prime power $t$ or $n$ is prime and $C_n \subset G \subset AGL_1(n)$. From the case (1) of this proof we deduce that $PGL_s(t) \subset G \subset PGL_d(t)$. From the case (2) we deduce that $t$ is the largest power of the characteristic that divides $n - 1$; hence $t = \ell$. Therefore $G = PGL_d(\ell)$.

(4) $n = 11$ and $G = M_{11}$ or $G = PSL_2(11)$. In this case $m$ can be any number from 1 to 5. Assume that $\hat{G}$ is the Galois group of $P$ over some $F(a, b)$ for some finite field $F$. The group $\hat{G}$ is a normal subgroup of $G$. Since $\hat{G}$ contains an $n$-cycle, it is equal to one of $M_{11}, PSL_2(11), A_{11}, S_{11}$. Hence to show, that $A_{11} \subset G$ it suffices to show that $\hat{G} \neq M_{11}, PSL_2(11)$. To show that $\hat{G} \neq M_{11}, PSL_2(11)$ it is enough to find a specialization of $P(x)$ over a finite field, whose factorization pattern contradicts the possible cycle types of $M_{11}$ and $PSL_2(11)$. We do so in Table 2 of Appendix B (in every case the factorization shows that $\hat{G}$ has a cycle of length 2, 3 or 5 contradicting Theorem 3.1).

The only case remaining is that of the polynomial $x^{11} + ax^2 + b$ when $p = 3$. But in this case Uchida [Uch70, Example 4] proved that $G = M_{11}$.

(5) $n = 23$ and $G = M_{23}$. Similarly to the previous case, for all but one possible pair $(p, m)$ we can find a trinomial over a finite field with factorization pattern that is impossible for $G = M_{23}$. The results are summarized in Table 2 of Appendix B. The only case not covered in Table 2 is that of the polynomial $x^{23} + ax^3 + b$ for $p = 2$. The polynomial $x^{23} + tx^3 + 1$ over $\mathbb{F}_2(t)$ has Galois group $M_{23}$, as proved by Abhyankar using the linearization method [Abh93a]. Consider the field $L = K(a, b)(b^{1/23})$. Let $\alpha := b^{1/23}$ and $\beta := a\alpha^{-20}$. Then $L$ is isomorphic to the field of rational functions $K(\alpha, \beta)$. Over $L$ the equation $x^{23} + ax^3 + b = 0$ can be simplified. Let $x = \alpha y$, then the equation becomes $y^{24} + \beta y^3 + 1 = 0$.

Since $K(\alpha, \beta)/K(\alpha)$ is a purely transcendental extension, the Galois group of $y^{23} + \beta y^3 + 1$ over $K(\alpha, \beta)$ is equal to the Galois group of the same equation over $K(\beta)$, which is equal to $M_{23}$. Since $L/K(a, b)$ is a cyclic extension, $G \neq A_{23}$, thus $G = M_{23}$.

\[ \square \]

Remark 5.5. Theorem 5.4 does not distinguish between the cases $G = A_n$ and $G = S_n$, but it is possible to do so. When $p$ is odd this is discussed in Remark 4.5. If $p = 2$ and $n$ is even, then $G \subset A_n$ by [AOS94, Proposition 2.24]. If $p = 2$ and $n$ is odd, then $G \subset A_n$ if and only if $m = 2$ by [AOS94, Proposition 2.23].

Acknowledgements

I would like to thank my advisor Bjorn Poonen for careful reading of the paper and insightful conversations. I thank Dmitri Kubrak for many helpful suggestions.

Appendix A. Cycle types of Mathieu groups

The following table describes cycle types of Mathieu groups in their standard multiply transitive actions; see [WWT+].
| Group | Number of points | Cycle types |
|-------|-----------------|-------------|
| $M_{11}$ | 11 | $2^4, 3^3, 4^2, 5^2, (2, 3, 6), (2, 8), 11$ |
| $M_{11}$ | 12 | $2^4, 3^3, (2^2, 4^2), 5^2, (2, 3, 6), (4, 8), 11$ |
| $M_{12}$ | 12 | $2^6, 2^4, 3^3, 3^4, (2^2, 4^2), 4^2, 5^2, 6^2, (2, 3, 6), (4, 8), (2, 8), (2, 10), 11$ |
| $M_{23}$ | 23 | $2^8, 3^6, (2^2, 4^4), 5^4, (2^2, 3^2, 6^2), 7^3, (2, 4, 8^2), 11^2, (2, 7, 14), (3, 5, 15), 23$ |
| $M_{24}$ | 24 | $2^8, 2^{12}, 3^6, 3^8, (2^4, 4^4), (2^2, 4^4), 4^6, 5^4, (2^2, 3^2, 6^2), 6^4, 7^3, (2, 4, 8^2), 2^2, 10^2, 11^2, (2, 4, 6, 12), 12^2, (2, 7, 14), (3, 5, 15), (2, 21), 23$ |

Table 1. Cycle types of Mathieu groups
### Appendix B. Factors of trinomials over finite fields

| Polynomial     | Field | Degrees of irreducible factors |
|----------------|-------|---------------------------------|
| $x^{11} + x + 1$ | $\mathbb{F}_2$ | $2 \times 9$                   |
| $x^{11} - x - 1$ | $\mathbb{F}_5$ | $1 \times 3 \times 7$          |
| $x^{11} + x^3 + 1$ | $\mathbb{F}_2$ | $5 \times 6$                    |
| $x^{11} + x^4 + 1$ | $\mathbb{F}_7$ | $1 \times 1 \times 2 \times 7$ |
| $x^{11} + x^5 + 1$ | $\mathbb{F}_3$ | $1 \times 3 \times 7$          |
| $x^{11} + x^5 + 1$ | $\mathbb{F}_2$ | $3 \times 8$                    |
| $x^{23} + x + 1$ | $\mathbb{F}_2$ | $2 \times 8 \times 13$         |
| $x^{23} + x + 1$ | $\mathbb{F}_{11}$ | $1 \times 2 \times 5 \times 15$ |
| $x^{23} + x^2 + 1$ | $\mathbb{F}_3$ | $1 \times 2 \times 20$         |
| $x^{23} + x^2 + 1$ | $\mathbb{F}_7$ | $2 \times 7$                    |
| $x^{23} + x^3 + 1$ | $\mathbb{F}_5$ | $1 \times 22$                   |
| $x^{23} + 3x^4 + 1$ | $\mathbb{F}_9$ | $1 \times 1 \times 1 \times 4 \times 7 \times 9$ |
| $x^{23} + x^5 + 1$ | $\mathbb{F}_3$ | $1 \times 2 \times 5 \times 7 \times 8$ |
| $x^{23} + cx^5 + 1$ | $\mathbb{F}_4$ | $1 \times 9 \times 13$         |
| $x^{23} + x^6 + 1$ | $\mathbb{F}_{17}$ | $2 \times 3 \times 9 \times 9$ |
| $x^{23} + x^7 + 1$ | $\mathbb{F}_2$ | $2 \times 10 \times 11$        |
| $x^{23} + x^8 + 1$ | $\mathbb{F}_3$ | $1 \times 3 \times 19$         |
| $x^{23} + x^8 + 1$ | $\mathbb{F}_5$ | $1 \times 4 \times 5 \times 13$ |
| $x^{23} + x^9 + c$ | $\mathbb{F}_4$ | $1 \times 2 \times 20$         |
| $x^{23} + x^9 + 1$ | $\mathbb{F}_7$ | $4 \times 19$                   |
| $x^{23} + x^{10} + 1$ | $\mathbb{F}_{13}$ | $1 \times 1 \times 4 \times 6 \times 11$ |
| $x^{23} + x^{11} + 1$ | $\mathbb{F}_2$ | $5 \times 6 \times 12$        |
| $x^{23} + x^{11} + 1$ | $\mathbb{F}_3$ | $1 \times 3 \times 19$         |

Table 2. Factorization of trinomials; $c^2 = c + 1$
References

[Abh92] Shreeram Shankar Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. **27** (1992), no. 1, 68 – 133. MR1118002 (94a:12004)

[ASP92] Shreeram Shankar Abhyankar, Wolfgang K. Seiler, and Herbert Popp, *Miehus group coverings of the affine line*, Duke Math. J. **68** (1992), no. 2, 301 – 311. MR1191563 (93j:14018)

[Abh93a] Shreeram Shankar Abhyankar, *Mathieu group coverings in characteristic two*, C. R. Acad. Sci. Paris Sér. I Math. **316** (1993), no. 3, 267–271. MR1205196 (94g:14013)

[Abh93b], *Alternating group coverings of the affine line for characteristic greater than two*, Math. Ann. **296** (1993), no. 1, 63–68. MR1298962 (95h:14020)

[Abh94], *Nice equations for nice groups*, Israel J. Math. **88** (1994), no. 1-3, 1 – 23. MR1303488

[AOS94] Shreeram Shankar Abhyankar, Jun Oun, and Avinash Sathaye, *Alternating group coverings of the affine line for characteristic two*, Discrete Math. **133** (1994), no. 1-3, 25 – 46. MR1298962 (95h:14018)

[BWT+] Robert Wilson, Peter Walsh, Jonathan Tripp, Ibrahim Suleiman, Richard Parker, Simon Norton, Simon Nickerson, Steve Linton, John Bray, and Abbott Abbott, *ATLAS of finite group representations – version 3. available at [http://brauer.maths.qmul.ac.uk/Atlas/v3/].

[BC00] Edoardo Ballico and Antonio Cossidente, *Curves of the projective 3-space, tangent developables and partial spreads*, Bull. Belg. Math. Soc. **7** (2000), 387–394. MR1788144 (2001j:51022)

[Coh80] Stephen Cohen, *The Galois group of a polynomial with two indeterminate coefficients*, Pacific J. Math. **90** (1980), no. 1, 63–76. Correction in Pacific J. Math. **97** (1981), no. 2, 483–486. MR0599320 (83j:12020a)

[Con99] J.H. Conway, *Three lectures on exceptional groups*, Sphere Packings, Lattices and Groups, Springer, New York, 1999, pp. 267–298.

[DM96] John D. Dixon and Brian Mortimer, *Permutation Groups*, Graduate Texts in Math., vol. 163, Springer-Verlag, New York – Heidelberg – Berlin, 1996. MR1409812 (98m:20003)

[EH82] David Eisenbud and Joe Harris, *Curves in projective space*, Les presses de l’Université de Montréal, 1982. notes du cours de Monsieur Joe Harris á la dix-neuvieme session du Seminaire de Mathematiques superieures.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)

[Hef89] Abramo Hefez, *Non-reflexive curves*, Compositio Math. **69** (1989), no. 1, 3–35.

[Jon14] Gareth A. Jones, *Primitive permutation groups containing a cycle*, Bull. Amer. Math. Soc. **89** (2014), no. 1, 159–165. MR3163014

[Kaj89] Hajime. Kaji, *On the Gauss maps of space curves in characteristic p*, Compositio Math. **70** (1989), no. 2, 177–197. MR0996326 (90c:14032)

[Kat73] Nicholas M. Katz, *Pinceaux de Lefschetz: théorème d’existence*, Groupes de monodromie en géométrie algébrique. II, Springer-Verlag, Berlin. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II); Dirigé par P. Deligne et N. Katz, Lecture Notes in Mathematics, Vol. 340, Exposé XVII, 1973, pp. 212–253.

[Rat87] Jürgen Rathmann, *The uniform position principle for curves in characteristic p*, Mathematische Annalen **267** (1987), no. 4, 565–579. MR0879536 (89g:14026)

[Smi77] John Howard Smith, *General trinomials having symmetric Galois group*, Proc. Amer. Math. Soc. **63** (1977), no. 2, 208–212. MR0437508 (55 #10433)

[Smi84], *Sur le groupe de Galois d’un polynôme dont les coefficients sont indépendants*, Sem. Théor. Nombres Bordeaux (1984), 1-11. MR0848379 (87i:12010)

[Uch70] Kôji Uchida, *Galois group of an equation x^n – ax + b = 0*, Tohoku Math. J. (2) **22** (1970), no. 4, 670-678. MR0277505 (43 # 3238)
