GALOIS THEORY ON THE LINE IN NONZERO
CHARACTERISTIC

SHREERAM S. ABHYANKAR

Dedicated to Walter Feit, J-P. Serre, and e-mail

1. WHAT IS GALOIS THEORY?

Originally, the equation $Y^2 + 1 = 0$ had no solution. Then the two solutions i and $-i$ were created. But there is absolutely no way to tell who is i and who is $-i$.[1] That is Galois Theory.

Thus, Galois Theory tells you how far we cannot distinguish between the roots of an equation. This is codified in the Galois Group.

2. GALOIS GROUPS

More precisely, consider an equation

$$Y^n + a_1 Y^{n-1} + \cdots + a_n = 0$$

and let $\alpha_1, \ldots, \alpha_n$ be its roots, which are assumed to be distinct. By definition, the Galois Group G of this equation consists of those permutations of the roots which preserve all relations between them. Equivalently, G is the set of all those permutations σ of the symbols $\{1, 2, \ldots, n\}$ such that $\phi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$ for every n-variable polynomial ϕ for which $\phi(\alpha_1, \ldots, \alpha_n) = 0$. The coefficients of ϕ are supposed to be in a field K which contains the coefficients $a_1, \ldots, a_n$ of the given polynomial

$$f = f(Y) = Y^n + a_1 Y^{n-1} + \cdots + a_n.$$

We call G the Galois Group of f over K and denote it by $\mathrm{Gal}_Y(f, K)$ or $\mathrm{Gal}(f, K)$. This is Galois' original concrete definition.

According to the modern abstract definition, the Galois Group of a normal extension L of a field K is defined to be the group of all K-automorphisms of L and is denoted by $\mathrm{Gal}(L, K)$. Note that a normal extension L of a field K is a field obtained by adjoining to K all the roots of a bunch of univariate polynomials with coefficients in K. To relate the two definitions, let $L = K(\alpha_1, \ldots, \alpha_n)$ and note that we get an isomorphism of $\mathrm{Gal}(L, K)$ onto

---

[1]Only the physicist can tell the difference by declaring that i is up and $-i$ is down. But then, what is up and what is down? What I am saying is that intrinsically there is no way to distinguish, in an abstractly given copy of the complex numbers, between the two square-roots of minus one. However, practically everyone has their own favorite concrete model of $\mathbb{C}$, perhaps $\mathbb{R} \times \mathbb{R}$, perhaps $\mathbb{R}[Y]/(Y^2 + 1)$, and then there is no problem in pointing to say $(0, 1)$ in the first case or $[Y]$ in the second and calling that i.

Gal(f, K) by sending any $\tau \in \mathrm{Gal}(L, K)$ to that $\sigma \in \mathrm{Gal}(f, K)$ for which $\tau(\alpha_i) = \alpha_{\sigma(i)}$ for $1 \le i \le n$.

3. PERMUTATION GROUPS

The above concrete definition brings out the close connection between group theory and theory of equations. To wit, the Galois Group $\mathrm{Gal}(f, K)$ is now a subgroup of S_n where, as usual, S_n denotes the symmetric group of degree n, i.e., the group of all permutations of n symbols; note that the order of S_n is $n!$. Quite generally, a subgroup of S_n is called a (permutation) group of degree n. Here the use of the word degree is meant to remind us that potentially it comes from an equation of degree n. To convert this potentiality into actuality, in various situations, constitutes Inverse Galois Theory. To further bring out the parallelism between group theory and the theory of equations, we note that.

(1) f is irreducible iff $\mathrm{Gal}(f, K)$ is transitive.

Here, a permutation group G "acting"[2] on the set $\Omega = \{1, 2, \ldots, n\}$ is *transitive* if for all i, j in Ω, there exists $\sigma \in G$ such that $\sigma(i) = j$. Likewise, G is 2-transitive (or doubly transitive) if for all $i \ne i'$ and $j \ne j'$ in Ω, there exists $\sigma \in G$ such that $\sigma(i) = j$ and $\sigma(i') = j'$. Quite generally, G is *l-transitive* for a positive integer $l \le n$, if for all pairwise distinct elements $i_1, i_2, \ldots, i_l$ in Ω and pairwise distinct elements $j_1, j_2, \ldots, j_l$ in Ω, there exists $\sigma \in G$ such that $\sigma(i_e) = j_e$ for $1 \le e \le l$. This brings us to MTR, i.e., the method of

4. THROWING AWAY ROOTS

Assuming f to be irreducible in $K[Y]$, let us "throw away" a root of f, say α_1, and get

$$f_1 = f_1(Y) = \frac{f(Y)}{(Y - \alpha_1)} = Y^{n-1} + b_1 Y^{n-2} + \cdots + b_{n-1} \in K(\alpha_1)[Y].$$

In continuation of (1), we see that.

(2) f and f_1 are irreducible in $K[Y]$ and $K(\alpha_1)[Y]$ respectively iff $\mathrm{Gal}(f, K)$ is 2-transitive.

It may be noted that, assuming f to be irreducible, it does not matter which root of f we throw away; for instance, the irreducibility of f_1 in $K(\alpha_1)[Y]$ and, up to isomorphism, the Galois group $\mathrm{Gal}(f_1, K(\alpha_1))$ are independent of which root we call α_1.

Likewise, by throwing away s roots of $f_0 = f$ we get

$$f_s = f_s(Y) = \frac{f(Y)}{(Y - \alpha_1) \cdots (Y - \alpha_s)}$$
$$= Y^{n-s} + d_1 Y^{n-s-1} + \cdots + d_{n-s} \in K(\alpha_1, \ldots, \alpha_s)[Y]$$

and then:

(3) f_s is irreducible in $K(\alpha_1, \ldots, \alpha_s)[Y]$ for $0 \le s < l$ iff $\mathrm{Gal}(f, K)$ is *l*-transitive.

5. CLASSIFICATION THEOREMS

Now you would have thought that you could (easily or possibly) construct a polynomial $f = f_0$, say of degree 20, such that $f_0, f_1, \ldots, f_9$ are irreducible

---

[2]Self-advice: Don't be so scared of the term "acting." It is simply the modern substitute for "permuting."

whereas f_{10} is reducible. But No! And that is the surprise of the century. You cannot!! So says the CT, i.e., the recently established Classification Theorem of Finite Simple Groups, which was a magnificent piece of "team work". According to the staggering statistics as reported by Coach Gorenstein [G3], the CT took 30 years (1950–1980), 100 authors, 500 papers, and 15000 pages! Yet several hundred more pages are required to prove the implications

$$\text{CT} \Rightarrow \text{CDT} \Rightarrow \text{CTT} \Rightarrow \text{CQT} \Rightarrow \text{CFT} \Rightarrow \text{CST}$$

where CDT (resp: CTT, CQT, CFT, and CST) stands for the Classification Theorem of Doubly (resp: Triply, Quadruply, Fivefold, and Sixfold) transitive permutation groups.[3] Promising to come back to CDT to CFT in a moment, let us state CST. It simply says that the symmetric group S_n for $n \geq 6$ and the alternating group A_n for $n \geq 8$ are the only sixfold transitive groups!! Vis-a-vis equations, what we are saying is that if f is an irreducible polynomial of degree $n > 7$ such that f_1, f_2, f_3, f_4 and f_5 are irreducible then so are $f_6, f_7, \ldots, f_{n-3}$.[4]

To take a first shot at CT, in addition to permutation groups, we should also consider groups of matrices over the (Galois) Field GF(q) of q elements where q is a power of a prime. So let

$$\begin{aligned} \text{GL}(m, q) = {} & \text{the } \textit{general linear group} \text{ of degree } m \text{ over GF}(q) \\ = {} & \text{the group of all nonsingular } m \text{ by } m \text{ matrices} \\ & \text{with entries in GF}(q). \end{aligned}$$

Here the multiplicative group GF(q)* comes in two ways. Firstly, thinking of scalar matrices, GF(q)* becomes a normal subgroup (and, in fact, the center) of GL(m, q). Secondly, taking determinants we get a surjective homomorphism GL(m, q) → GF(q)*. This motivates the definitions

$$\begin{aligned} \text{PGL}(m, q) = {} & \text{the } \textit{projective general linear group} \text{ of degree } m \\ & \text{over GF}(q) \\ = {} & \text{GL}(m, q)/\text{GF}(q)^* \end{aligned}$$

and

$$\begin{aligned} \text{SL}(m, q) = {} & \text{the } \textit{special linear group} \text{ of degree } m \text{ over GF}(q) \\ = {} & \ker \text{GL}(m, q) \rightarrow \text{GF}(q)^*. \end{aligned}$$

Combining these two roles of GF(q)* we get

$$\begin{aligned} \text{PSL}(m, q) = {} & \text{the } \textit{projective special linear group} \text{ of degree } m \\ & \text{over GF}(q) \\ = {} & \text{SL}(m, q)/(\text{SL}(m, q) \cap \text{GF}(q)^*). \end{aligned}$$

---

[3]This is an expanded version of a lecture given at Walter Feit's 60th birthday conference in Oxford, England. In addition to Walter Feit, the audience included the group theorists Peter Cameron, Michael Collins, Sandy Green, Graham Higman, Peter Neumann, Ron Solomon, and John Thompson; my talking group theory in this meet of topnotch group theorists was like carrying coal to Newcastle, or bringing holy water to the Ganges!!

[4]Self-Challenge = challenge to the extollers of high school algebra: prove that by high school algebra if you can! Of course we can simply decree CT be high school algebra!!

In group theory parlance[5]

$$L_m(q) = \text{ the } \textit{linear group} \text{ of degree } m \text{ over } \mathrm{GF}(q)$$
$$= \mathrm{PSL}(m, q).$$

In yet another notation

$$A_n(q) = L_{n+1}(q) = \mathrm{PSL}(n+1, q).$$

With these preliminaries,

CT essentially says that A_n and $A_n(q)$ are the only (finite) simple groups.

Here we have to exclude "small" cases; namely, from the alternating group A_n exclude $n \leq 4$, and from $A_n(q)$ exclude $n = 1$ and $q \leq 3$ (we define $A_n(q)$ only for $n \geq 1$). Moreover, "essentially" means that with $A_n(q)$ we have to include its relatives and incarnations, to be discussed later. Finally, in addition to these infinite families, there are 26 "sporadics", again to be discussed later.[6]

6. Brief thirty year history

First, in the fifties, there was the fundamental work of Brauer [B] and Chevalley [Ch]. In 1962 this was followed by the path-breaking odd order paper of Feit and Thompson [FT]. Then came the large team coached by Gorenstein [G4]. At any rate, we are meeting here to felicitate our friend Walter Feit on the occasion of his forthcoming sixtieth birthday.[7]

7. Primitive groups

As another example of the parallelism between group theory and theory of equations, let us note that a permutation group G is said to be primitive if it is transitive, and the *one-point stabilizer* G_1 of G is a maximal subgroup of G. Here we are assuming G to be a subgroup of the symmetric group S_n acting on $\{1, 2, \ldots, n\}$, and then by definition, $G_1 = G \cap S_{n-1}$ with $S_{n-1} = \{\sigma \in S_n : \sigma(1) = 1\}$. Just as it did not matter which root of the irreducible equation we threw away, so in the present situation, if G is transitive then we may replace G_1 by any $G_i = \{\sigma \in G : \sigma(i) = i\}$, which is called the *stabilizer* of i in G. Clearly.

(4) If f is irreducible and $G = \mathrm{Gal}(f, K)$ then $G_1 = \mathrm{Gal}(f_1, K(\alpha_1))$.
Moreover;

(5) $\mathrm{Gal}(f, K)$ is primitive iff f is irreducible and there is no field between K and $K(\alpha_1)$.

Not to get completely lost in group theory, let us revert to algebraic geometry by talking about

8. Fundamental groups

In my 1957 paper on "Coverings of Algebraic Curves" in the American Journal [A3], I considered the *algebraic fundamental group* $\pi_A(C)$ of a nonsingular

---

[5]In learning group theory, I am following the traditional Indian method: memorize things by heart and the meaning will eventually be revealed to you. Moreover, every subject has its lingo. Thus GL, SL and PSL are the Tom, Dick, and Harry of group theory.

[6]Does the number 26 vindicate the spread of the English language which has exactly that many letters?

[7]My fondest memory of Walter is that in 1957, when we were both at Cornell, we decided to go on a diet together and the one who lost more weight was to get a quarter. At the end of one month, Walter gained one pound and I gained two. Who lost and who won?

curve C. Here C is allowed to be "open", i.e., it may consist of a projective algebraic curve minus a finite number of points. We assume that C is irreducible and defined over an algebraically closed ground field k. By $\pi_A(C)$ we mean the family of Galois groups $\mathrm{Gal}(L/k(C))$ as L varies over all finite normal extensions of the function field $k(C)$ of C such that no point of C (equivalently, no valuation of $k(C)/k$ having center on C) is *ramified* in L.

In case C is the (affine) line L_k over k, or more generally if $C = L_{k,r} = $ the line L_k minus r points $\lambda_1, \ldots, \lambda_r$ (with $\lambda_i \neq \lambda_j$ in k for $1 \leq i < j \leq r$) then this amounts to considering $\mathrm{Gal}(F, k(X))$ where

$$F = F(X, Y) = Y^n + \phi_1(X)Y^{n-1} + \cdots + \phi_n(X)$$

is a bivariate polynomial with coefficients $\phi_1(X), \ldots, \phi_n(X)$ in $k[X]$ such that F is unramified at all (finite) values of X other than $\lambda_1, \ldots, \lambda_r$, i.e., such that for every λ in k different from $\lambda_1, \ldots, \lambda_r$ we have

$$F(X + \lambda, Y) = \prod_{i=1}^{n}(Y - \eta_\lambda^{(i)}(X))$$

with $\eta_\lambda^{(i)}(X)$ in the (formal) power series ring $k[[X]]$. We may call F an *unramified covering* of $L_{k,r}$.

For any group G, let G_h denote the family of finite homomorphic images of G. Let $\mathscr{F}_r$ be the free group on r generators, and let J_r be the family of all finite groups generated by r generators, and note that then $J_r = \mathscr{F}_{rh}$. By the Riemann Existence Theorem etc., we see that if $k = $ the field of complex numbers $\mathbb{C}$, then for any (irreducible) nonsingular curve C over k we have $\pi_A(C) = \pi_1(C)_h$ where, as usual, $\pi_1(C)$ denotes the (topological) fundamental group of C; see Serre [S1]. Hence in particular $\pi_A(L_{\mathbb{C},r}) = \pi_1(L_{\mathbb{C},r})_h$, and clearly $\pi_1(L_{\mathbb{C},r}) = \mathscr{F}_r$. Therefore $\pi_A(L_{\mathbb{C},r}) = J_r$.

By taking $r = 0$ or 1 in the last equation, we get $\pi_A(L_\mathbb{C}) = J_0 = \{1\}$ and $\pi_A(L_{\mathbb{C},1}) = J_1 = $ the family of all finite cyclic groups. These two facts can also be proved purely algebraically, by the genus formula due to Hurwitz–Riemann–Zeuthen; see Serre [S2]. The said genus formula actually shows that

$$\pi_A^*(L_k) = J_0 = \{1\}$$

and

$$\pi_A^*(L_{k,1}) = J_1[\mathrm{char}\ k]^*$$
$$= \text{the family of all finite cyclic groups with order}$$
$$\text{nondivisible by char } k,$$

where char k is the characteristic of k and where for any (irreducible) nonsingular curve C over any algebraically closed field k we define

$$\pi_A^*(C) = \text{the } \textit{globally tame fundamental group} \text{ of } C$$
$$= \text{the family of all the members of } \pi_A(C) \text{ whose order is}$$
$$\text{nondivisible by char } k$$

and for any nonnegative integer m and any family of finite groups J we put

$$J[m]^* = \text{the family of all the members of } J \text{ whose order is nondivisible by } m.$$

9. QUASI p-GROUPS

Given any prime number p we put

$$Q(p) = \text{the family of all quasi } p\text{-groups},$$

where by a *quasi p-group* we mean a finite group which is generated by all of its p-Sylow subgroups, and for any finite group G we put

$p(G) = $ the (normal) subgroup of G generated by all of its p-Sylow subgroups

and for any family of finite groups J we put

$$J(p) = \text{the family of all finite groups } G \text{ such that } G/p(G) \in J$$

and we note that then $J_0(p) = Q(p)$ and for every nonnegative integer r we have

$$J_r(p) = J_r[p]^*(p)$$
$$= \text{the family of all finite groups } G \text{ such that } G/p(G) \text{ is generated}$$
$$\text{by } r \text{ generators}$$

and

$$\{p(G) : G \in J_r(p)\} = Q(p).$$

10. CONJECTURES

For any algebraically closed field k of characteristic $p \neq 0$, in the above cited 1957 paper, I conjectured that $\pi_A(L_{k,r}) = \pi_A(L_{\mathbb{C},r})(p)$, i.e., equivalently,

General Conjecture. For every nonnegative integer r we have $\pi_A(L_{k,r}) = J_r(p)$. Hence in particular

Quasigroup Conjecture. $\pi_A(L_k) = Q(p)$.

Now a (finite) simple group whose order is divisible by p is obviously a quasi p-group, and therefore QC (= the Quasigroup Conjecture) subsumes the

Simple Group Conjecture. $\pi_A(L_k)$ contains every simple group whose order is divisible by p.

In particular

Alternating Group Conjecture. For every integer $n \geq p$ we have $A_n \in \pi_A(L_k)$ except when $p = 2 < n < 5$.

Here, as usual, A_n denotes the alternating group of degree n, i.e., the group of all even permutations on n symbols, and we note that the order of A_n is $n!/2$ or 1 according as $n > 1$ or $n = 1$. As proved by Galois, A_n is a simple group for every $n > 4$, and hence AGC (= the Alternating Group Conjecture) is a special case of SGC (= the Simple Group Conjecture) except when $(p, n) = (3,4)$; in this exceptional case, A_n is obviously a quasi p-group and so we can directly fall back upon QC. The symmetric group S_n of degree n is obviously a quasi 2-group for every n, and hence QC subsumes the

Even Prime Symmetric Group Conjecture. If $p = 2$ then for every integer $n \geq 2$ we have $S_n \in \pi_A(L_k)$.

To match up with EPSGC (= the Even Prime Symmetric Group Conjecture), let us divide AGC into EPAGC and OPAGC, i.e., into the following two conjectures respectively.

Even Prime Alternating Group Conjecture. If $p = 2$ then for every integer $n \geq 2$ except when $2 < n < 5$ we have $A_n \in \pi_A(L_k)$.

Odd Prime Alternating Group Conjecture. If $p > 2$ then for every integer $n \geq p$ we have $A_n \in \pi_A(L_k)$.

11. AGAIN SOME HISTORY

Let $0 \neq a \in k =$ an algebraically closed field of characteristic $p \neq 0$, and let n, s, t be positive integers such that $t \not\equiv 0(p)$. Now in support of the above conjectures, in the above cited 1957 paper, I had written down the following two examples of unramified coverings of L_k :

$$\widehat{F}_n = Y^n - aX^sY^t + 1 \quad \text{with } n = p + t$$

and

$$\widetilde{F}_n = Y^n - aY^t + X^s \text{ with } t < n \equiv 0(p) \text{ and } \text{GCD}(n, t) = 1 \text{ and } s \equiv 0(t)$$

and had suggested that their Galois groups $\widehat{G}_n = \text{Gal}(\widehat{F}_n, k(X))$ and $\widetilde{G}_n = \text{Gal}(\widetilde{F}_n, k(X))$ should be calculated.

Now, after a gap of thirty years, with Serre's encouragement and with the help of CT, I can calculate these Galois groups, and the answers are as follows.

(I)

(I.1) If $t = 1$, then $\widehat{G}_n = \text{PSL}(2, p) = \text{PSL}(2, n - 1)$.

(I.2) If $t = 2$ and $p = 7$, then $\widehat{G}_n = \text{PSL}(2, 8) = \text{PSL}(2, n - 1)$.

(I.3) If $t = 2$ and $p \neq 7$, then $\widehat{G}_n = A_n$.

(I.4) If $t > 2$ and $p \neq 2$, then $\widehat{G}_n = A_n$.

(I.5) If $p = 2$, then $\widehat{G}_n = S_n$.

(II)

(II.1) If $1 < t < 4$ and $p \neq 2$, then $\widetilde{G}_n = A_n$.

(II.2) If $1 < t < n - 3$ and $p \neq 2$, then $\widetilde{G}_n = A_n$.

(II.3) If $1 < t = n - 3$ and $p \neq 2$ and $11 \neq p \neq 23$, then $\widetilde{G}_n = A_n$.

(II.4) If $1 < t < 4 < n$ and $p = 2$, then $\widetilde{G}_n = A_n$ or S_n.

(II.5) If $1 < t < n - 3$ and $p = 2$, then $\widetilde{G}_n = A_n$ or S_n.

Actually, $\widehat{F}_n$ is a slight generalization of the original equation

$$\overline{F}_n = Y^n - XY^t + 1 \quad \text{with } n = p + t$$

written down in the 1957 paper. This equation $\overline{F}_n$ was discovered by taking a section of a surface extracted from my 1955 paper "Ramification of Algebraic Functions" in the American Journal [A1], which was the second part of my Ph.D. Thesis written under the able guidance of Oscar Zariski. In the 1956 paper in the Annals of Mathematics [A2], which was the first part of my Ph.D Thesis, I proved resolution of singularities of algebraic surfaces in nonzero characteristic. In the 1955 American Journal paper, I was showing why Jung's method of surface resolution in the complex case does not generalize to nonzero characteristic, because the local fundamental group, above a normal crossing of the branch locus, in the former case is abelian whereas in the latter case it can

even be unsolvable. It was a surface constructed for this purpose whose section I took in the 1957 paper.

Although the second equation $\widetilde{F}_n$ is also a slight generalization of an equation occuring in the 1957 paper but, amusingly, it got rediscovered in 1989 as a variation of the first equation $\widehat{F}_n$.

Now (I.1) was originally proved by Serre and when he told me about it in September 1988, that is what started off my calculations after a thirty year freeze! As a slight generalization of (I.1), in the case of $t = 1$, I can also calculate the Galois group $\widehat{G}_{n,q} = \mathrm{Gal}(\widehat{F}_{n,q}, k(X))$ of the unramified covering of L_k given by

$$\widehat{F}_{n,q} = Y^n - aX^{-s}Y^t + 1 \quad \text{with } n = q + t,$$

where q is any positive power of p, and it turns out that

(III)

(III.1) If $t = 1$, then $\widehat{G}_{n,q} = \mathrm{PSL}(2, q) = \mathrm{PSL}(2, n - 1)$.

Again, $\widehat{F}_{n,q}$ is a slight generalization of the equation

$$\overline{F}_{n,q} = Y^n - XY^t + 1 \quad \text{with } n = q + t,$$

which also occurs in the 1957 paper. Note that then

$$\overline{F}_n = \overline{F}_{n,p}.$$

12. Using MRT

Applying MRT (= method of removing tame ramification through cyclic compositums = so called Abhyankar's Lemma) to the one-point stabilizer of $\widehat{F}_{n+1}$ we get the monic polynomial of degree n in Y with coefficients in $k(X)$ given by

$$\widehat{F}'_n = h(Y)(Y + b)^p - aX^{-s}Y^t \quad \text{with } 0 \neq b \in k,$$

where $h(Y)$ is the monic polynomial of degree $n - p$ in Y with coefficients in k given by

$$h(Y) = \frac{(Y + n + 1)^{n+1-p} - Y^{n+1-p}}{(n + 1)^2}$$

and we let $\widehat{G}'_n = \mathrm{Gal}(\widehat{F}'_n, k(X))$. As an immediate consequence of (I) we now get

(IV)

Assuming that $n + 1 \not\equiv 0(p)$, in the following cases $\widehat{F}'_n$ gives an unramified covering of L_k with the indicated Galois group.

(IV.1) If $n + 1 - p = t > 2 \neq p$ and $b = t$ and $s \equiv 0(p - 1)$ and $s \equiv 0(t)$, then $\widehat{G}'_n = A_n$.

(IV.2) If $n + 1 - p = t = 2$ and $p \neq 7$ and $b = t$ and $s \equiv 0(p - 1)$, then $\widehat{G}'_n = A_n$.

(IV.3) If $n = p + 1$ and $p > 5$, then t can be chosen so that $1 < t < \frac{p+1}{2}$ and $\mathrm{GCD}(p + 1, t) = 1$, and for any such t, upon assuming $b = \frac{t}{t-1}$ and $s \equiv 0(t(p + 1 - t))$, we have $\widehat{G}'_n = A_n$.

(IV.4) If $n + 1 - p = t$ and $p = 2$ and $b = t$ and $s \equiv 0(t)$, then $\widehat{G}'_n = S_n$.

13. UNRAMIFIED COVERINGS

We have the following four corollaries of calculations (I) through (IV).

In Calculations (I) through (IV), we use a lot of Ramification Theory, or, equivalently, CS (= Cycle Structure). In addition to CS + MTR + MRT, in the proofs of Calculations (I) to (IV) we also use CT. In our original version of these proofs, the use of CT was heavy. Gradually the use of CT decreased, but could not be removed completely. However, by traversing a delicate path through calculations (I) through (IV), we have arranged a proof of the First and the Second Corollaries independent of CT.

First Corollary. *OPAGC is true. Equivalently, for any $n \geq p > 2$, there exists an unramified covering of the affine line in characteristic p whose Galois group is the alternating group A_n of degree n.*

Second Corollary. *EPSGC is true. Equivalently, for any $n \geq p = 2$, there exists an unramified covering of the affine line in characteristic p whose Galois group is the symmetric group S_n of degree n.*

Third Corollary. *Unramified coverings of the affine line in characteristic p with a few more Galois groups have been constructed.*

Definition-Remark. By the *minimal index* of a finite group G we mean the smallest number d such that G has a subgroup of index d which does not contain any nonidentity normal subgroup of G.[8] Now QC is obviously equivalent to saying that for every integer $d \geq p$ the following is true.

QC(d). *Every quasi p-group of minimal index d belongs to $\pi_A(L_k)$, i.e., occurs as the Galois group of an unramified covering of the affine line in characteristic p.*

Therefore it is interesting to point out that as a corollary of the above results we have the following:

Fourth Corollary. *QC$(p + 1)$ is true for every p which is not a Mersenne prime[9] and which is different from 11 and 23. More generally, if G is a quasi p-group containing a subgroup H of index $p + 1$ such that H does not contain any nonidentity normal subgroup of G, and if p is not a Mesenne prime and p is different from 11 and 23, then there exists an unramified covering of the affine line in characteristic p having G as the Galois group.*

The proofs of the above four Corollaries and the four claims (I) to (IV) will be completely given in this paper with the exception that the proof of claim (I.2)

---

[8]In other words, we are minimizing the index over subgroups of G which do not contain any minimal normal subgroup of G, where we recall that a *minimal normal subgroup* of a group G is a nonidentity normal subgroup N of G such that N does not contain any nonidentity normal subgroup of G other than N itself.

[9]A *Mersenne prime* is a prime p of the form $p = 2^\mu - 1$ for some positive integer μ. Note that then μ is necessarily prime, because otherwise by factoring $\mu = \mu'\mu''$ with $\mu' > 1$ and $\mu'' > 1$, we would get a factorization $2^\mu - 1 = l'l''$ with $l' = 2^{\mu'} - 1 > 1$ and $l'' = 1 + 2^{\mu'} + 2^{2\mu'} + \cdots + 2^{\mu'(\mu'' - 1)} > 1$.

will be completed in my forthcoming paper [A7]. In connection with (II.4), it may be noted that the case of $p = 11$ or 23 is still open.[10]

14. History of a pilgrimage

When I said that "Now...I can calculate these Galois groups", what I really meant was that, from September 1988 to August 1989, I undertook a pilgrimage (physical as well as mental)[11] to seek the help of lots of mathematicians, and then I simply collated the help so obtained. In chronological order, these mathematicians were. Serre (oh yes, very much Serre), Kantor, Feit, Cameron, Sathaye, Eakin, Stennerson, Gorenstein, O'Nan, Mulay, and Neumann.

The pilgrimage started when in September and October of 1988, Serre sent me one after another four long letters briefly saying that

"*In your* 1957 *paper you suggested that the Galois group of* $\overline{F}_n$ *should be calculated. I can now prove that for* $t = 1$ *it is* PSL$(2, p)$. *Can you calculate it for other values of* t? *Also, the conjectures in your paper include AGC. Can you now prove AGC?*"

Fortunately, in his last letter, Serre added a sentence saying that "my e-mail is...."

15. Multiply transitive groups

Having already commented on the significance of transitivity for Galois theory, before proceeding further with calculations of Galois groups, let us give a brief review of multiply transitive groups.

So let G be a permutation group, say of degree n, i.e., let G act on $\Omega = \{1, 2, \ldots, n\}$. In analogy with the concept of transitivity introduced in §3, we say that G is λ-*antitransitive* (or λ-fold antitransitive) for a positive integer $\lambda \leq n$, if for all pairwise distinct elements $i_1, i_2, \ldots, i_\lambda$ in Ω we have that the identity is the only member of G which keeps them fixed.[12] Moreover, for positive integers $l \leq \lambda \leq n$, we say that G is (l, λ)-*transitive* if G is l-transitive and λ-antitransitive; we may express this by simply saying that G is (l, λ).[13] Finally, G is *sharply* l-*transitive* means G is (l, l). Now if G is l-transitive, with $l > 1$, then the one-point stabilizer of G is obviously $(l - 1)$-transitive as a permutation group of degree $n - 1$, acting on the "remaining" $n - 1$ elements; conversely, if G is transitive and its one-point stabilizer is $(l - 1)$-transitive then G is l-transitive. Similarly, if G is λ-antitransitive, with $\lambda > 1$, then the one-point stabilizer of G is $(\lambda - 1)$-antitransitive as a permutation group of degree $n - 1$, acting on the "remaining" $n - 1$ elements; conversely, if G is transitive and its one-point stabilizer is $(l - 1)$-antitransitive then G is l-antitransitive. Thus, to classify all (l, λ) groups, we can make induction and each time increase l, λ, and n by one. So we start with $(1, 1)$.

By definition, G is *regular* means G is $(1, 1)$. Now the classification of $(1, 1)$ groups is either obvious or impossible. Obvious because it is so easy

---

[10]As will become apparent later, the reason for this, as well as for the exclusion of these values of p from the Fourth Corollary, is the existence of the "Mathieu Groups".

[11]mental = e-mail + s-mail. s-mail = snail mail = usual mail.

[12]That is, if $\sigma \in G$ is such that $\sigma(i_e) = i_e$ for $1 \leq e \leq \lambda$ then we must have $\sigma = 1$.

[13]Note that if G is l-transitive and m-antitransitive for positive integers $l \leq n$ and $m \leq n$, then automatically $l \leq m$. Also note that if G is l-transitive for some positive integer $l \leq n$ then G is l'-transitive for every positive integer $l' \leq l$. Likewise, if G is λ-antitransitive for a positive integer λ then G is λ'-antitransitive for every positive integer $\lambda' \geq \lambda$ with $\lambda' \leq n$.

to define what is $(1, 1)$. Indeed, the usual proof of the usual theorem which says that every finite group is a permutation group, amounts to representing the given group as a regular permutation group.[14] Hence impossible because it would amount to classifying all finite groups.

G is *Frobenius* means G is $(1, 2)$ but not $(1, 1)$. A prototype of a Frobenius group is the group of all affine linear transformations $ax + b$ with a, b in a finite field, or more generally in a finite near-field. Zassenhaus [Z2], in his 1936 Thesis written under Artin, proved that the converse is true for $(2, 2)$ groups.

Zassenhaus' Theorem. G *is* $(2, 2) \Leftrightarrow G = \text{AGLNF}(1, \Psi)$ *for some finite near-field* Ψ.

Here, by $\text{AGLNF}(1, \Psi)$ we are denoting the group of all affine linear transformations of degree 1 over the near-field Ψ, where "near-field" is a generalization of "field" obtained by weakening the distributive law. Namely, a *near-field* is an additive abelian group Ψ in which the nonzero elements form a multiplicative group such that for all a, b, c in Ψ we have $a(b + c) = ab + ac$. Thus we are not assuming the other distributive law $(b + c)a = ba + bc$ which is not a consequence of the first distributive law because the multiplication is not required to be commutative. It can easily be seen that, as in the case of a field, the number of elements in any finite near-field is a power of a prime number. By an affine linear transformation of degree 1 over the near-field Ψ we mean a map $\Psi \to \Psi$ given by $x \mapsto ax + b$ with a, b in Ψ and $a \neq 0$. It can easily be seen that distinct (a, b) give distinct maps $\Psi \to \Psi$. A proof of Zassenhaus' Theorem is given in 9.10 on page 424 of volume III of Huppert-Blackburn [HB].[15] In the proof of this Theorem, as well as in the proofs of various other theorems on multitransitive groups, an important role is played by the following Theorem of Frobenius (1901) [Fr] for a proof of which we refer to 8.2 on page 496 of volume I of Huppert–Blackburn [HB].

Frobenius' Theorem. *A Frobenius group* G *always has a* $(1, 1)$ *normal subgroup. More precisely, the subset of* G *consisting of the identity together with those elements* σ *which fix no letter (i.e.,* $\sigma(i) \neq i$ *for* $i = 1, 2, \ldots, n$*) forms a regular normal subgroup of* G.

In the notation $\text{AGLNF}(1, \Psi)$, the letters NF are meant to remind us of a near-field. In case $\Psi =$ a field Φ, we may write $\text{AGL}(1, \Phi)$ instead of $\text{AGLNF}(1, \Psi)$.

To put the notation $\text{AGL}(1, \Phi)$ in proper perspective, first we remark that for a field Φ and a positive integer m the groups $\text{GL}(m, \Phi)$, $\text{PGL}(m, \Phi)$, $\text{SL}(m, \Phi)$, and $\text{PSL}(m, \Phi)$ are defined by replacing $\text{GF}(q)$ by Φ in §5.[16] Note that $Z(\text{GL}(m, \Phi)) =$ the set of all scalar matrices, and $Z(\text{SL}(m, \Phi)) = \text{SL}(m, \Phi) \cap Z(\text{GL}(m, \Phi))$, where the *center* of any group Γ is denoted by

---

[14]By making G act on itself by right or left (but not both) multiplication.

[15]Although Dickson found all finite near-fields, it was left to Zassenhaus to prove that there were no more. E. H. Moore [Mo] of the newly opened University of Chicago classified finite fields, around 1895, and then, around 1905, his students Wedderburn [W] and Dickson [D2] studied skew fields and near-fields respectively.

[16]Writing q for $\text{GF}(q)$ is justified because for any prime power q, up to isomorphism, there is exactly one field with q elements.

$Z(\Gamma)$, i.e., $Z(\Gamma)$ is the normal subgroup of Γ given by putting $Z(\Gamma) = \{a \in \Gamma : ab = ba$ for all $b \in \Gamma\}$. Now a nonsingular m by m matrix $\alpha \in \mathrm{GL}(m, \Phi)$ corresponds to the bijection $\Phi^m \to \Phi^m$ which sends any 1 by m matrix $\xi \in \Phi^m$ to the matrix product $\xi\alpha \in \Phi^m$. In this manner, the group $\mathrm{GL}(m, \Phi)$, and hence also the subgroup $\mathrm{SL}(m, \Phi)$, may be regarded as a permutation group on Φ^m. Let $\mathscr{P}(\Phi^m)$ be the $(m - 1)$-dimensional *projective space* over Φ, where we think of $\mathscr{P}(\Phi^m)$ as the set of all one-dimensional subspaces of Φ^m. Now the bijection $\Phi^m \to \Phi^m$ corresponding to any $\alpha \in \mathrm{GL}(m, \Phi)$ clearly induces a bijection $\mathscr{P}(\Phi^m) \to \mathscr{P}(\Phi^m)$; moreover, if $\alpha^* \in \mathrm{GL}(m, \Phi)$ differs from α by a scalar matrix, then α and α^* induce the same bijection $\mathscr{P}(\Phi^m) \to \mathscr{P}(\Phi^m)$. Thus the group $\mathrm{PGL}(m, \Phi)$, and hence also the subgroup $\mathrm{PSL}(m, \Phi)$, becomes a permutation group on $\mathscr{P}(\Phi^m)$. Members of $\mathrm{PGL}(m, \Phi)$ are called *projective transformations* of $\mathscr{P}(\Phi^m)$. Note that for any $\gamma \in \mathrm{PGL}(m, \Phi)$ and $\zeta \in \mathscr{P}(\Phi^m)$ we have $\gamma(\zeta) \in \mathscr{P}(\Phi^m)$.

Now the *affine general linear group* $\mathrm{AGL}(m, \Phi)$ of degree m over Φ may be introduced as the *semidirect product* $\Phi^m \rtimes \mathrm{GL}(m, \Phi)$ of Φ^m by $\mathrm{GL}(m, \Phi)$ with the obvious action of $\mathrm{GL}(m, \Phi)$ on Φ^m, where we recall that a group Γ is said to be the (internal) semidirect product of a normal subgroup Θ by a subgroup Δ provided $\Gamma = \Theta\Delta$ and $\Theta \cap \Delta = 1$, and we note that in this case Δ acts on Θ by conjugation. Concretely, $\mathrm{AGL}(m, \Phi)$ may be regarded as the set of all m by $m + 1$ matrices whose entries are in the Φ and whose m by m piece is nonsingular; in other words, we think of $\mathrm{AGL}(m, \Phi)$ as the set of all pairs (α, β) with $\alpha \in \mathrm{GL}(m, \Phi)$ and $\beta \in \Phi^m$, where multiplication is defined by $(\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \beta\alpha' + \beta')$.[17] To $(\alpha, \beta) \in \mathrm{AGL}(m, \Phi)$ there corresponds the bijection $\Phi^m \to \Phi^m$ which sends every $\xi \in \Phi^m$ to $\xi\alpha + \beta \in \Phi^m$.[18] Thus $\mathrm{AGL}(m, \Phi)$ also becomes a permutation group on Φ^m. Members of $\mathrm{AGL}(m, \Phi)$ are called *affine transformations* of Φ^m.[19]

To make another example of a semidirect product, let $\mathrm{Aut}\,\Phi$ be the *group of all automorphisms* of the field Φ. For every matrix γ with entries in Φ and for every $g \in \mathrm{Aut}\,\Phi$, let γ^g be the matrix obtained by applying g to each entry of γ. This gives an action of $\mathrm{Aut}\,\Phi$ on $\mathrm{GL}(m, \Phi)$. The semidirect product $\mathrm{GL}(m, \Phi) \rtimes \mathrm{Aut}\,\Phi$ is denoted by $\Gamma\mathrm{L}(m, \Phi)$ and members of $\Gamma\mathrm{L}(m, \Phi)$ are called *semilinear transformations* of Φ^m. A member of $\Gamma\mathrm{L}(m, \Phi)$ may be thought of as a pair (g, α) with $g \in \mathrm{Aut}\,\Phi$ and $\alpha \in \mathrm{GL}(m, \Phi)$, and the corresponding bijection $\Phi^m \to \Phi^m$ sends every $\xi \in \Phi^m$ to $\xi^g\alpha \in \Phi^m$. The multiplication in $\Gamma\mathrm{L}(m, \Phi)$ is given by $(g, \alpha)(g', \alpha') = (gg', \alpha^{g'}\alpha')$. Thus

---

[17]This is an example of an "external" semidirect product. For further elucidation see Suzuki [Su2], Huppert-Blackburn [HB], and Wielandt [Wi]. A lot of the group theory background, required in this paper, I learned in the last two years from these nice books. I highly recommend them. It may be noted that a Frobenius group G is the semidirect product of the Frobenius kernel of G by a Frobenius complement of G, where by the *Frobenius kernel* of G we mean the $(1, 1)$ normal subgroup of G, and by a *Frobenius complement* of G we mean a 1-point stabilizer of G.

[18]In the above case of $m = 1$, this reduces to $x \mapsto ax + b$ by taking $x = \xi \in \Phi$, $0 \neq a = \alpha \in \Phi$, and $b = \beta \in \Phi$.

[19]Transformations, or substitutions, of the type $x' = ax + by + c$ and $y' = a'x + b'y + c'$ are familiar to us from high school. By adding "points at infinity" to the ordinary plane we get the projective plane. To distinguish between the ordinary plane and the projective plane, the ordinary plane is called the affine plane and the above transformations are called affine transformations of the plane Φ^2. To know that they can be redefined in terms of semidirect products should help to make this notion friendly.

$\Gamma L(m, \Phi)$, which may be called the *semilinear group* of degree m over Φ, acts on Φ^m. With this action we can form the semidirect product $A\Gamma L(m, \Phi) = \Phi^m \rtimes \Gamma L(m, \Phi)$ and call it the *affine semilinear group* of degree m over Φ. A member of $A\Gamma L(m, \Phi)$ is called an *affine semilinear transformation* of Φ^m and it may be represented as a triple (g, α, β) with $g \in \operatorname{Aut}\Phi$, $\alpha \in GL(m, \Phi)$, $\beta \in \Phi^m$; the corresponding bijection $\Phi^m \to \Phi^m$ sends every $\xi \in \Phi^m$ to $\xi^g \alpha + \beta \in \Phi^m$, and the multiplication in $A\Gamma L(m, \Phi)$ is given by $(g, \alpha, \beta)(g', \alpha', \beta') = (gg', \alpha^{g'}\alpha', \beta^{g'}\alpha' + \beta')$. Thus $A\Gamma L(m, \Phi)$ is a permutation group on Φ^m, and in a natural manner we have

$$SL(m, \Phi) \lhd GL(m, \Phi) \lhd \Gamma L(m, \Phi) < A\Gamma L(m, \Phi)$$

and

$$GL(m, \Phi) < AGL(m, \Phi) < A\Gamma L(m, \Phi),$$

where $<$ and $\lhd$ denote *subgroup* and *normal subgroup* respectively.

To construct one more example of a semidirect product, we note that the action of $\operatorname{Aut}\Phi$ on $GL(m, \Phi)$ obviously induces an action of $\operatorname{Aut}\Phi$ on the factor group $PGL(m, \Phi)$. With this induced action we form the semidirect product $P\Gamma L(m, \Phi) = PGL(m, \Phi) \rtimes \operatorname{Aut}\Phi$ and call it the *projective semilinear group* of degree m over Φ. A member of $P\Gamma L(m, \Phi)$ is called a *projective semilinear transformation* of $\mathscr{P}(\Phi^m)$ and it may be represented by a pair (γ, g) with $\gamma \in PGL(m, \Phi)$ and $g \in \operatorname{Aut}\Phi$; the corresponding bijection $\mathscr{P}(\Phi^m) \to \mathscr{P}(\Phi^m)$ sends every $\zeta \in \mathscr{P}(\Phi^m)$ to $\gamma(\zeta^g) \in \mathscr{P}(\Phi^m)$ where $\zeta^g \in \mathscr{P}(\Phi^m)$ is given by $\zeta^g = \{\xi^g : \xi \in \zeta\}$. Thus $P\Gamma L(m, \Phi)$ becomes a permutation group on $\mathscr{P}(\Phi^m)$, and in a natural manner we have

$$PSL(m, \Phi) \lhd PGL(m, \Phi) \lhd P\Gamma L(m, \Phi).$$

Although we have spoken of $SL(m, \Phi)$, $GL(m, \Phi)$, $\Gamma L(m, \Phi)$, $AGL(m, \Phi)$, $A\Gamma L(m, \Phi)$ as permutation groups on Φ^m, and $PSL(m, \Phi)$, $PGL(m, \Phi)$, $P\Gamma L(m, \Phi)$ as permutation groups on $\mathscr{P}(\Phi^m)$, this is relevant mainly when $\Phi = GF(q)$ for some prime power q and in that case we may write $SL(m, q)$, $GL(m, q)$, $\Gamma L(m, q)$, $AGL(m, q)$, $A\Gamma L(m, q)$, $PSL(m, q)$, $PGL(m, q)$, and $P\Gamma L(m, q)$ for $SL(m, \Phi)$, $GL(m, \Phi)$, $\Gamma L(m, \Phi)$, $AGL(m, \Phi)$, $A\Gamma L(m, \Phi)$, $PSL(m, \Phi)$, $PGL(m, \Phi)$, and $P\Gamma L(m, \Phi)$ respectively.

Henceforth by a *permutation group* we shall again mean a permutation group on a finite set.

16. ZASSENHAUS GROUPS

Having talked about $(1, 1)$, $(1, 2)$, and $(2, 2)$ groups, let us now discuss $(2, 3)$ groups which are not $(2, 2)$. Basically they fall into the following three classes.

(i) A *Feit group* is defined to be a $(2, 3)$ group which is not $(2, 2)$ but has a $(1, 1)$ normal subgroup. As a prototype we have the group $A\Gamma L(1, 2^p)$ where p is a prime number. This consists of all transformations $x \mapsto ax^g + b$ with $0 \neq a \in GF(2^p)$ and $b \in GF(2^p)$ and $g \in \operatorname{Aut} GF(2^p)$. Now $|GF(2^p)| = 2^p$ and $|\operatorname{Aut} GF(2^p)| = p$ where $|\ |$ denotes cardinality. Thus $A\Gamma L(1, 2^p)$ is a permutation group of degree 2^p and order $2^p(2^p - 1)p$.

(ii) A *sharp Zassenhaus group* is defined to be a $(3, 3)$ group; such a group is clearly a $(2, 3)$ group; moreover, it is a $(2, 2)$ group only when its degree

is 3 and in that case it is simply S_3. The Fundamental Theorem of Projective Geometry says that, on the projective line over a field Φ, any three points can be sent to any other three points by one and only one projective transformation. In case, $\Phi = GF(q)$, where q is a prime power,[20] this amounts to saying that the group $PGL(2, q)$ is a $(3, 3)$ group, where we regard $PGL(2, q)$ as a permutation group of degree $q + 1$;[21] it is easily seen that $PGL(2, q)$ has no $(1, 1)$ normal subgroup; clearly the order of $PGL(2, q)$ is $(q + 1)q(q - 1)$.[22] It can be shown that, if q is an even power of an odd prime, $P\Gamma L(2, q)$ has exactly one 3-transitive subgroup, which we denote by $PML(2, q)$, such that $PML(2, q) \neq PGL(2, q)$ and $PSL(2, q)$ is a subgroup of $PML(2, q)$ of index 2. Now $PML(2, q)$ is also a $(3, 3)$ group, where we again regard it as a permutation group of degree $q + 1$; it is easily seen that $PML(2, q)$ has no $(1, 1)$ normal subgroup provided $q \geq 4$; clearly the order of $PML(2, q)$ is $(q + 1)q(q - 1)$; we call $PML(2, q)$ the *projective mock linear group* of degree 2 over $GF(q)$. For further discussion about $PML(2, q)$ see page 163 of volume III of Huppert-Blackburn [HB] where it is denoted by $M(q)$.

(iii) A *strict Zassenhaus group* is defined to be a $(2, 3)$ group which is neither $(2, 2)$ nor $(3, 3)$ and does not have any $(1, 1)$ normal subgroup.[23] It can easily be seen that, for any odd prime power q, the group $PSL(2, q)$ is a strict Zassenhaus group of degree $q + 1$. To find the order of this group, we might as well start by calculating the order of $GL(m, q)$ for any positive integer m and any prime power q which need not be odd. Now the number of ways of choosing the first column of an element of $GL(m, q)$ equals $|GF(q)^m| - 1 = q^m - 1$. The number of multiples of the first column is q and hence, having chosen the first column, the number of ways of choosing the second column equals $|GF(q)^m| - |GF(q)| = q^m - q$. More generally, the first i columns generate an i-dimensional vector space over $GF(q)$ and hence, having chosen the first i columns, the number of ways of choosing the $(i + 1)$th columns equals $|GF(q)^m| - |GF(q)^i| = q^m - q^i$. Therefore

$$|GL(m, q)| = (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}).$$

Consequently

$$|AGL(m, q)| = |GF(q)^m||GL(m, q)| = q^m(q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}).$$

Now $|GF(q)^*| = q - 1$, where $GF(q)^*$ is the multiplicative group of nonzero elements of $GF(q)$, and we have obvious exact sequences of finite groups $1 \rightarrow SL(m, q) \rightarrow GL(m, q) \rightarrow GF(q)^* \rightarrow 1$ and $1 \rightarrow GF(q)^* \rightarrow GL(m, q) \rightarrow$

---

[20]That is q is a positive integral power of a prime number. Clearly then q is an odd prime power or an even prime power according as the corresponding prime number is even or odd. When q is an odd prime power, it can be an even power of an odd prime or an odd power of an odd prime.

[21] $PGL(2, q)$ acts on the projective line over $GF(q)$ which has $q + 1$ points on it, out of which q are at "finite distance" and one is the point at "infinity".

[22]Obviously the order of any (l, l) group of degree n is $n(n - 1) \cdots (n - l + 1)$.

[23]In Gorenstein's book [G1] every $(2, 3)$ group which is not $(2, 2)$ is called a Zassenhaus group. In Huppert and Blackburn's book [HB] every $(2, 3)$ group which is not $(2, 2)$ and does not have any $(1, 1)$ normal subgroup is called a Zassenhaus group. We are calling the groups mentioned in (i) Feit groups because they were completely characterized by Feit [F] in 1960.

$\mathrm{PGL}(m, q) \to 1$, and hence

$$|\mathrm{PGL}(m, q)| = |\mathrm{SL}(m, q)| = |\mathrm{GL}(m, q)|/(q - 1)$$
$$= (q^m - 1)(q^m - q) \cdots (q^m - q^{m-2})q^{m-1}.$$

Let

$$Z_\nu = \text{the cyclic group of order } \nu \text{ where } \nu \text{ is either a positive}$$
$$\text{integer or } \infty.$$

Now clearly

$$\mathrm{Aut}\, \mathrm{GF}(q) = Z_\mu \text{ where } q = p^\mu \text{ with } p = \mathrm{char}\, k$$

and hence

$$|\Gamma\mathrm{L}(m, q)|/|\mathrm{GL}(m, q)| = |A\Gamma\mathrm{L}(m, q)|/|A\mathrm{GL}(m, q)|$$
$$= |P\Gamma\mathrm{L}(m, q)|/\mathrm{PGL}(m, q)| = \mu.$$

Let $\mathrm{SL}(m, q)^*$ be the group of all m by m scalar matrices whose entries are in $\mathrm{GF}(q)$ and whose determinant is 1. Then $\mathrm{SL}(m, q)^*$ is isomorphic to the group of all mth roots of 1 in $\mathrm{GF}(q)$ and hence $|\mathrm{SL}(m, q)^*| = \mathrm{GCD}(m, q - 1)$. Also we have an obvious exact sequence of finite groups $1 \to \mathrm{SL}(m, q)^* \to \mathrm{SL}(m, q) \to \mathrm{PSL}(m, q) \to 1$ and hence

$$|\mathrm{PSL}(m, q)| = |\mathrm{SL}(m, q)|/\mathrm{GCD}(m, q - 1)$$
$$= |\mathrm{PGL}(m, q)|/\mathrm{GCD}(m, q - 1).$$

So in particular

$$|\mathrm{PSL}(2, q)| = (q + 1)q(q - 1)/2 \quad \text{or} \quad (q + 1)q(q - 1)$$

according as q is odd or even i.e., according as $q - 1$ is or is not divisible by 2. If q is even then we cannot divide $q - 1$ by 2, and so we do the best we can; namely, assuming q to be a square of a proper odd power[24] of 2, in the expression $(q + 1)q(q - 1)/2$ we replace $(q - 1)/2$ by $(q^{1/2} - 1)$ to get the expression $(q+1)q(q^{1/2}-1)$, and now to get rid of the fractional power we write q in place of $q^{1/2}$. For every q which is a proper odd power of 2, the resulting expression $(q^2 + 1)q^2(q - 1)$ is the order of a certain strict Zassenhaus group $\mathrm{Sz}(q)$ of degree $q^2 + 1$; this group $\mathrm{Sz}(q)$ is isomorphic[25] to a certain subgroup of $\mathrm{GL}(4, q)$ and, since it was discovered by Suzuki [Su1] in 1962, it is called the *Suzuki group* over $\mathrm{GF}(q)$. We may think of $\mathrm{Sz}(q)$ as ersatz $\mathrm{PSL}(2, q^2)$; we have just given a heuristic reason for its existence and a mnemonic device for remembering its order; to recapitulate

$$|\mathrm{Sz}(q)| = (q^2 + 1)q^2(q - 1) \quad \text{if } q \text{ is any odd power of 2.}$$

As hinted in the above order formula, the definition of the Suzuki group $\mathrm{Sz}(q)$ can be extended so as to include the case of $q = 2$; in this case we still get a 2-transitive permutation group of degree $q^2 + 1$ and of the above order, which is however not a strict Zassenhaus group; indeed, as a permutation group, $\mathrm{Sz}(2)$ is isomorphic to the $(2, 2)$ group $\mathrm{AGL}(1, 5)$.

The following theorem of Zassenhaus [Z1], Feit [F], and Suzuki [Su1] says that the above examples of $(2, 3)$ groups which are not $(2, 2)$ are exhaustive; for a proof see 1.1 and 11.16 on pages 161 and 286 of volume III of Huppert-Blackburn [HB].

---

[24]That is with an odd exponent > 1.

[25]Not as a permutation group.

Zassenhaus-Feit-Suzuki Theorem. *For a permutation group G we have the following.*

    (1) G *is Feit* $\Leftrightarrow G = A\Gamma L(1, 2^p)$ *for some prime* p.

    (2) G *is sharp Zassenhaus* $\Leftrightarrow G = PGL(2, q)$ *for some prime power* q, *or* $G = PML(2, q)$ *for some even power* q *of an odd prime.*

    (3) G *is strict Zassenhaus* $\Leftrightarrow G = PSL(2, q)$ *for some odd prime power* q, *or* $G = Sz(q)$ *for some proper odd power* q *of* 2.

Moreover, this gives an exhaustive and mutually exclusive listing of $(2, 3)$ *groups which are not* $(2, 2)$, *with the proviso that the group* $PSL(2, 2) = S_3$ *is included in item* (2) *even though it is a* $(2, 2)$ *group in addition to being a* $(3, 3)$, *and hence a* $(2, 3)$, *group.*

17. MORE ABOUT CLASSIFICATION THEOREMS

By analyzing the Suzuki group $Sz(q)$, a certain analogous 2-transitive permutation group $R_1(q)$ of degree q^3+1, for every odd power q of 3, was discovered by Ree [R] in 1964; although $R_1(q)$ is 2-transitive, it is not 3-antitransitive; the group $R_1(q)$ is defined in terms of some 7 by 7 matrices over $GF(q)$ and is called the Ree group over $GF(q)$; the order of $R_1(q)$ is given by

$$|R_1(q)| = (q^3 + 1)q^3(q - 1) \quad \text{if } q \text{ is any odd power of 3.}$$

For every odd power q of 2, in terms of certain matrices over $GF(q)$, Ree defined a group $R_2(q)$ which is also called the Ree group over $GF(q)$; the order is now given by

$$|R_2(q)| = q^{12}(q^6 + 1)(q^4 - 1)(q^3 + 1)(q - 1)$$

if q is any odd power of 2. All the Suzuki groups and all the Ree groups turn out to be a simple groups except: $Sz(2)$ is solvable; $R_1(3)$ is isomorphic to $P\Gamma L(2, 8)$ and hence the simple group $PSL(2, 8)$ may be regarded as a normal subgroup of $R_1(3)$ of index 3 and then $PSL(2, 8)$ is the unique minimal normal subgroup of $R_1(3)$; the commutator subgroup $R_2(2)'$ of $R_2(2)$ is a (normal) subgroup of $R_2(2)$ of index 2, and the said commutator subgroup $R_2(2)'$ is actually a simple group called the Tits group. Thus we have the following three infinite families of finite simple groups deduced from matrices over $GF(q)$.

Suzuki and Ree groups. $Sz(q)$ for every proper odd power q of 2. $R_1(q)$ for every proper odd power q of 3. $R_2(q)$ for every proper odd power q of 2, together with the commutator subgroup $R_2(2)'$.

Just before Suzuki and Ree found these groups, Steinberg [St], in 1959, discovered that some known groups together with some further ones suggested by them could be organized into four other infinite families of finite simple groups which are defined in terms of matrices over $GF(q^2)$ and which are now labeled as follows.

Steinberg groups. $^2A_n(q), {}^2D_n(q), {}^3D_4(q)$, and $^2E_6(q)$. Here n is any positive integer and q is any prime power except: in case of $^2A_n(q)$ exclude $(n, q) = (1, 2), (1, 3), (2, 2)$, and in case of $^2D_n(q)$ exclude $n = 1$.

These $3 + 4 = 7$ families are the "twisted incarnations" of the original nine infinite families of "relatives" of $A_n(q)$. These nine infinite families of finite

simple groups defined in terms of matrices over $GF(q)$ were systematized by Chevalley [Ch] in 1955, and they are labeled as follows.[26]

Chevalley groups. $A_n(q)$, $B_n(q)$, $C_n(q)$, $D_n(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, and $G_2(q)$. Again here n is any positive integer and q is any prime power except: in case of $A_n(q)$ exclude $(n, q) = (1, 2), (1, 3)$; in case of $B_n(q)$ and $C_n(q)$ exclude $(n, q) = (1, 2), (1, 3), (2, 2)$; in case of $D_n(q)$ exclude $n < 4$; and in case of $G_2(q)$ exclude $q = 2$.

Thus we have $7 + 9 = 16$ infinite families of finite simple groups defined in terms of matrices over finite fields. It may be noted that, just as the group $A_n(q) = \mathrm{PSL}(n + 1, q)$ is obtained by projectivizing the special linear group $\mathrm{SL}(n + 1, q)$, the group $C_n(q) = \mathrm{PSp}(2n, q)$ is obtained by projectivizing the "symplectic group" $\mathrm{Sp}(2n, q)$, and the groups $B_n(q) = \mathrm{P\Omega}(2n + 1, q)$ and $D_n(q) = \mathrm{P\Omega}^+(2n, q)$ are obtained by projectivizing the "commutator groups" $\Omega(2n + 1, q)$ and $\Omega^+(2n, q)$ of the "orthogonal groups" $O(2n+1, q)$ and $O^+(2n, q)$ respectively. The groups $A_n(q)$, $B_n(q)$, $C_n(q)$, $D_n(q)$ are collectively called "classical groups", and the remaining Chevalley groups $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$ are collectively called "exceptional groups."

Likewise, amongst the Steinberg groups, the group $^2A_n(q) = \mathrm{PSU}(n + 1, q)$ is obtained by projectivizing the "special unitary group" $\mathrm{SU}(n + 1, q)$, and the group $^2D_n(q) = \mathrm{P\Omega}^-(2n, q)$ is obtained by projectivizing the "commutator group" $\Omega^-(2n, q)$ of the "orthogonal group" $O^-(2n, q)$. The Suzuki and Ree groups have the alternative labels $\mathrm{Sz}(q) = {}^2B_2(q)$, $R_1(q) = {}^2G_2(q)$, and $R_2(q) = {}^2F_4(q)$. The groups $^2A_n(q)$, $^2B_2(q)$, $^2D_n(q)$, $^3D_4(q)$ may collectively be called the "twisted classical groups", and the groups $^2E_6(q)$, $^2F_4((q)$, $^2G_2(q)$ may collectively be called the "twisted exceptional groups."

Now the projective mock linear group $\mathrm{PML}(2, q)$ may also be called the *premathieu linear group* of degree 2 over $GF(q)$. The reason for this nomenclature is that, around 1865, Mathieu [Mat] found a transitive extension of $\mathrm{PML}(2, 9)$ which is denoted by M_{11}. By a *transitive extension* of a permutation group of degree n we mean a transitive permutation group of degree $n + 1$ having the given group as a one-point stabilizer. Note that M_{11} is a $(4, 4)$ group of degree 11 and hence its order is $11 \cdot 10 \cdot 9 \cdot 8$. Mathieu also found a transitive extension of M_{11} which we denote by M_{12}. Clearly M_{12} is a $(5, 5)$ group of degree 12 and hence its order is $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$. The permutation groups M_{11} and M_{12} are called *Mathieu groups* of degree 11 and 12 respectively. It can be shown that M_{12} has a noninner automorphism α of order 2 such that $\alpha(M_{11})$ is 3-transitive of degree 12. The permutation group $\alpha(M_{11})$ may be regarded as an *incarnation* of the Mathieu group M_{11} and we may denote it by $\widehat{M}_{11}$. To recapitulate

$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \qquad \text{and} \qquad |\widehat{M}_{11}| = |M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8.$$

To introduce the remaining three groups discovered by Mathieu, let us first note that for any positive integer m and any prime power q we have $|GF(q)^m|$

---

[26]When $q = $ a prime p, many of these were already studied by Jordan [J1] in the last century. For general q, some of them were discussed by Dickson [D1] at the turn of the century. Likewise the first two families of Steinberg groups were already known to Jordan and Dickson, while the last two were independently found by Tits.

$= q^m$ and hence for the corresponding $(m-1)$-dimensional projective space we have

$$|\mathscr{P}(\mathrm{GF}(q)^m)| = (q^m - 1)/(q - 1) = q^{m-1} + q^{m-2} + \cdots + q + 1.$$

So in particular $|\mathscr{P}(\mathrm{GF}(4)^3)| = 21$ and hence $\mathrm{PSL}(3, 4)$, which acts on $\mathscr{P}(\mathrm{GF}(4)^3)$, is a permutation group of degree 21; it can easily be seen that it is 2-transitive but not 3-transitive; by the above order formula we also get

$$|\mathrm{PSL}(3, 4)| = (4^3 - 1)(4^3 - 4)4^2 / \mathrm{GCD}(3, 3) = 21 \cdot 20 \cdot 48.$$

Mathieu obtained a transitive extension M_{22} of $\mathrm{PSL}(3, 4)$, a transitive extension M_{23} of M_{22}, and a transitive extension M_{24} of M_{23}. Clearly M_{22} is a 3-transitive but not 4-transitive permutation group of degree 22, M_{23} is a 4-transitive but not 5-transitive permutation of degree 23, and M_{24} is a 5-transitive but not 6-transitive permutation group of degree 24. These groups are called *Mathieu groups* of degree 22, 23, 24 respectively, and obviously their orders are[27] $|M_{22}| = 22 \cdot 21 \cdot 20 \cdot 48$; $|M_{23}| = 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$, and $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. Note the striking similarity between the numbers $(2, 9)$ occuring in the "parent group" $\mathrm{PML}(2, 9)$ of M_{11} and M_{12}, and the numbers $(3, 4)$ occuring in the "parent group" $\mathrm{PSL}(3, 4)$ of M_{22}, M_{23}, and M_{24}. All of the five Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, and M_{24} turn out to be simple groups. One hundred years after their discovery, during 1965 to 1975, twenty-one other finite simple *sporadic groups*, i.e., those which do not naturally fit in any infinite family, were discovered by various people; the largest of the $21 + 5 = 26$ sporadic groups is called the *monster* and its order is

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71;$$

for details see Gorenstein [G1]. We are now ready to state, of course without proof, the Classification Theorem of Finite Simple Groups.[28]

CT. *The following is a complete list of finite simple groups.*

(1) *The cyclic group Z_p for every prime p.*

(2) *The alternating group A_n for every integer $n \geq 5$.*

(3) *The sixteen infinite families of "matrix" groups mentioned above.*[29]

(4) *The twenty-six sporadics including the five Mathieus.*

Just as $\mathrm{PSL}(m, q)$ is the typical example of a finite simple group, so $\mathrm{PGL}(2, q)$ is the quintessential example of a 3-transitive permutation group. As obvious variations of this, additional 3-transitive permutation groups are obtained by taking into account all the groups between $\mathrm{PGL}(2, q)$ and $\mathrm{P\Gamma L}(2, q)$ for every prime power q, and all the groups between $\mathrm{PML}(2, q)$ and $\mathrm{P\Gamma L}(2, q)$ for every even power q of an odd prime; both these types have degree $q + 1$. All these arise out of the fact that, by a projective transformation, any 3 points of a projective line can be sent to any other 3. Going to higher dimensions, by

---

[27]For a transitive permutation group G of degree n we clearly have $|G| = n|G_1|$ where G_1 is a one-point stabilizer of G.

[28]See Gorenstein [G2] or Aschbacher [As]. At least one part of this extremely long proof, namely Mason's paper on quasi-thin groups [Mas], is still to see the light of day!

[29]I am using the more friendly term "matrix groups" instead of the awe inspiring "Lie type groups."

a projective transformation, any 4 points of a projective plane can be sent to
any other 4, and any 5 points of a projective 3-space can be sent to any other
5, and so on. This would give rise to 4-transitives, 5-transitives, and so on.
But there is a flaw. 3 collinear points in a projective plane, or in a projective
3-space, cannot be sent to 3 noncollinear points. 4 coplanar points in a projec-
tive 3-space cannot be sent to 4 noncoplanar points. And so on. Thus, because
of questions of linear independence, for every integer $m > 1$ and every prime
power q, the group $\mathrm{PGL}(m, q)$, instead of being $(m + 1)$-transitive, is only
2-transitive, unless every line contains only 2 distinct points, in which case it
would be 3-transitive. Well, for $q = 2$, a line should contain only 2 points. But
even that is so only in the affine case because then we don't have the point at
infinity. Thus, it is not $\mathrm{PGL}(m, 2)$ which is 3-transitive, but $\mathrm{AGL}(m, 2)$. We
can see that $\mathrm{AGL}(m, 2)$ is, however, not 4-transitive unless $m = 2$ in which
case we actually have $\mathrm{AGL}(2, 2) = S_4$.

Now

$$\mathrm{AGL}(m, 2) = \mathrm{GF}(2)^m \rtimes \mathrm{GL}(m, 2) = 2^m \cdot L_m(2),$$

where a dot stands for the semidirect product symbol $\rtimes$, and 2^m stands for
$(Z_2)^m$, i.e., for the direct product $Z_2 \times Z_2 \times \cdots \times Z_2$ of m copies of Z_2. By
the order formula we have

$$|L_4(2)| = (2^4 - 1)(2^4 - 2)(2^4 - 4)(2^4 - 8) = 8!/2 = |A_8|.$$

Hence, by the philosophical principle that *two finite simple groups of equal order
are usually isomorphic*, we expect that $L_4(2) \approx A_8$ where $\approx$ stands for isomor-
phism, and this can, in fact, be easily proved. Note that $L_4(2) = \mathrm{GL}(4, 2)$
is a 1-point stabilizer of $\mathrm{AGL}(4, 2)$ and hence in this incarnation A_8 is only
2-transitive;[30] let us denote this *incarnation* by $\widehat{A_8}$.[31] In a natural manner, A_7
may be regarded as a subgroup of A_8 and then it turns out that the image of
A_7 under the said isomorphism is also only 2-transitive; let us denote the said
image by $\widehat{A_7}$.[32] The corresponding subgroup of $2^4 \cdot \widehat{A_8} = \mathrm{AGL}(4, 2)$ may be
denoted by $2^4 \cdot \widehat{A_7}$; this is a 3-transitive but not 4-transitive permutation group
of degree 2^4 and order $2^3 \cdot 7!$.[33]

As a consequence of CT, it can be shown that there are no more 3-transitive
permutation groups other than those we have already listed. In other words
we have the following detailed version of CTT, i.e., the Classification Theo-
rem of Triply Transitive Permutation Groups; this theorem was compiled from
conversations with Cameron, Neumann, and O'Nan.

CTT or Refined Fundamental Theorem of Projective Geometry. *The following is
a complete list of 3-transitive permutation groups.*

(1) *For every prime power q, each group between $\mathrm{PGL}(2, q)$ and
$\mathrm{P\Gamma L}(2, q)$ is a 3-transitive permutation group of degree $q + 1$, and we*

---

[30]By taking the stabilizer at the origin, $\mathrm{GL}(m, q)$ becomes the 1-point stabilizer of $\mathrm{AGL}(m, q)$
for every integer $m > 1$ and every prime power q. Likewise, by taking the stabilizer at the point
at infinity, $\mathrm{AGL}(1, q)$ may be regarded as the 1-point stabilizer of $\mathrm{PGL}(2, q)$ for every prime
power q.

[31]That is, as a permutation group, $\widehat{A_8} = \mathrm{GL}(4, 2) = \mathrm{PGL}(4, 2) \subset S_{15}$.

[32]In other words, $\widehat{A_7}$ is the image of A_7 under some injective group homomorphism $A_7 \to$
$\widehat{A_8} = \mathrm{GL}(4, 2) \subset S_{15}$, and $\widehat{A_7}$ is a 2-transitive but not 3-transitive permutation group of degree
15.

[33]As permutation groups, $\widehat{A_7}$ and $2^4 \cdot \widehat{A_7}$ are independent of the injective group homomorphism
$A_7 \to \widehat{A_8}$ we choose for defining $\widehat{A_7}$.

have $|\mathrm{PGL}(2, q)| = |\mathrm{P\Gamma L}(2, q)|/\mu = (q + 1)q(q - 1)$ where $q = p^{\mu}$ with $p = \mathrm{char}\,\mathrm{GF}(q)$. Among these, $\mathrm{PGL}(2, 3)$ and $\mathrm{P\Gamma L}(2, 4)$ are the only groups which are 4-transitive, and for them we actually have $\mathrm{PGL}(2, 3) = S_4$ and $\mathrm{P\Gamma L}(2, 4) = S_5$.

(2) *For every even power q of an odd prime, each group between $\mathrm{PML}(2, q)$ and $\mathrm{P\Gamma L}(2, q)$ is a 3-transitive but not 4-transitive permutation group of degree $q + 1$, and we have $|\mathrm{PML}(2, q)| = |\mathrm{P\Gamma L}(2, q)|/\mu = (q + 1)q(q - 1)$ where $q = p^{\mu}$ with $p = \mathrm{char}\,\mathrm{GF}(q)$.*

(3) *For every integer $m > 1$, the group $\mathrm{AGL}(m, 2)$ is a 3-transitive permutation group of degree 2^m and order $2^m(2^m - 1)(2^m - 2) \cdots (2^m - 2^{m-1})$. This is 4-transitive only for $m = 2$, and in that case we actually have $\mathrm{AGL}(2, 2) = S_4$.*

(4) *The group $2^4 \cdot \widehat{A}_7$ is a 3-transitive but not 4-transitive permutation group of degree 2^4 and order $2^4 \cdot 7!$, and as a permutation group it is a subgroup of $2^4 \cdot \widehat{A}_8 = \mathrm{AGL}(4, 2)$.*

(5) *The reincarnated Mathieu group $\widehat{M}_{11}$ is a 3-transitive but not 4-transitive permutation group of degree 12 and order $11 \cdot 10 \cdot 9 \cdot 8 = 12 \cdot 11 \cdot 10 \cdot 6$.*

(6) *The Mathieu group M_{22} and its automorphism group $\mathrm{Aut}\,M_{22}$ are 3-transitive but not 4-transitive permutation groups of degree 22 with $|M_{22}| = |\mathrm{Aut}\,M_{22}|/2 = 22 \cdot 21 \cdot 20 \cdot 48$.*

(7) *The Mathieu groups M_{11} and M_{23} are 4-transitive but not 5-transitive permutation groups of degree 11 and 23 and order $11 \cdot 10 \cdot 9 \cdot 8$ and $23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ respectively.*

(8) *The Mathieu groups M_{12} and M_{24} are 5-transitive but not 6-transitive permutation groups of degree 12 and 24 and order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ and $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ respectively.*

(9) *For every integer $n \geq 5$, the alternating group A_n is an $(n-2)$-transitive but not $(n-1)$-transitive permutation group of degree n and order $n!/2$.*

(10) *For every integer $n \geq 3$, the symmetric group S_n is an n-transitive but not $(n + 1)$-transitive permutation group of degree n and order $n!$.*

The above formulation of CTT obviously subsumes CQT, CFT, and CST. In turn the CTT is of course subsumed under the CDT which is given by Cameron [C] and Kantor [K2] and which, in addition to heavily using the CT, is based on the previous work of Curtis-Kantor-Seitz [CKS], O'Nan [O], and others. The following weaker version of CDT, dealing mainly with the degrees of 2-transitive permutation groups which are not 3-transitive, was communicated to me by Cameron.

Weak CDT. *Concerning the degrees of 2-transitive permutation groups we have the following.*

(1) *For every integer $m > 1$ and every prime power q, each group between $\mathrm{PSL}(m, q)$ and $\mathrm{P\Gamma L}(m, q)$ is a 2-transitive permutation group of degree $|\mathscr{P}(\mathrm{GF}(q)^m)| = (q^m - 1)/(q - 1)$. Out of these, only the groups listed in items (1) and (2) of CTT are 3-transitive. In case of $m > 2$, for each group between $\mathrm{PSL}(m, q)$ and $\mathrm{P\Gamma L}(m, q)$, by considering the action on "hyperplanes" in $\mathscr{P}(\mathrm{GF}(q)^m)$, we get a second representation as a 2-transitive but not 3-transitive permutation group of degree $(q^m - 1)/(q - 1)$.*

(2) *For every integer $m > 2$, the group $\mathrm{Sp}(2m, 2)$ has 2-transitive but not 3-transitive permutation representations of degrees $2^{2m-1} + 2^{m-1}$ and $2^{2m-1} - 2^{m-1}$.*

(3) *For every prime power $q = p^\mu > 2$ with prime p, each group between $\mathrm{PSU}(3, q)$ and its automorphism group $\mathrm{Aut}\,\mathrm{PSU}(3, q)$ has a 2-transitive but not 3-transitive permutation representation of degree q^3+1, and moreover $\mathrm{PSU}(3, q)$ is a normal subgroup of index $[\mathrm{GCD}(3, q + 1)]2\mu$ in $\mathrm{Aut}\,\mathrm{PSU}(3, q)$.[34]*

(4) *For every proper odd power $q = 2^\mu$ of 2, each group between the Suzuki group $\mathrm{Sz}(q)$ and its automorphism group $\mathrm{Aut}\,\mathrm{Sz}(q)$ has a 2-transitive but not 3-transitive permutation group of degree $q^2 + 1$, and moreover $\mathrm{Sz}(q)$ is a normal subgroup of index μ in $\mathrm{Aut}\,\mathrm{Sz}(q)$.*

(5) *For every odd power $q = 3^\mu$ of 3, each group between the Ree group $R_1(q)$ and its automorphism group $\mathrm{Aut}\,R_1(q)$ has a representation as a 2-transitive but not 3-transitive permutation group of degree $q^3 + 1$, and moreover $R_1(q)$ is a normal subgroup of index μ in $\mathrm{Aut}\,R_1(q)$.*

(6) *The group $\mathrm{PSL}(2, 11)$ has two distinct 2-transitive but not 3-transitive permutation representations of degree 11.[35]*

(7) *The alternating group A_7 has two distinct 2-transitive but not 3-transitive permutation representations of degree 15; both are equivalent to isomorphisms $A_7 \to \widehat{A_7} \subset S_{15}$.*

(8) *The "Higman-Sims" sporadic group HS has two different 2-transitive but not 3-transitive permutation representations of degree 176.*

(9) *The "third Conway" sporadic group Co_3 has a 2-transitive but not 3-transitive permutation representation of degree 276.*

The above items (1) to (9) contain a complete list of 2-transitive but not 3-transitive permutation groups having a nonabelian minimal normal subgroup. The degree of a 2-transitive but not 3-transitive permutation group G having an abelian minimal normal subgroup is necessarily some power p^m of some prime p; the said minimal normal subgroup is isomorphic to $(Z_p)^m$ and a 1-point stabilizer of the group G itself is isomorphic to a subgroup of $\mathrm{GL}(m, p)$; moreover: in the case $m = 1$ we must have $G = \mathrm{AGL}(1, p)$, whereas, in the case $m = a$ prime number and $p = 2$ we must have $G = \mathrm{AGL}(1, 2^m)$ or $\mathrm{A\Gamma L}(1, 2^m)$, and finally, in the case $m = 2$ and $p = 3$ we must have $G = \mathrm{AGL}(1, 9)$ or $\mathrm{A\Gamma L}(1, 9)$ or $\mathrm{AML}(1, 9)$ or $\mathrm{AGL}(2, 3)$ or $\mathrm{ASL}(2, 3)$, where we have put $\mathrm{AML}(1, 9) = $ the 1-point stabilizer of $\mathrm{PML}(2, 9)$,[36] and $\mathrm{ASL}(2, 3) = (\mathrm{GF}(3))^2 \rtimes \mathrm{SL}(2, 3)$.

In connection with the above statement, we note the following Theorem of Burnside which is really the starting point of the classification of 2-transitive permutation groups. Although most modern proofs of this make use of Frobe-

---

[34]A *centerless* group G, i.e., a group G whose center is the identity, may be identified with its inner automorphism group and hence may be regarded as a normal subgroup of its automorphism group $\mathrm{Aut}\,G$.

[35]Two permutation representations $G \to S_n$ and $G \to S_{n'}$ of a (finite) group G are *equivalent* if they differ by an isomorphism $S_n \to S_{n'}$ induced by a bijection between the underlying sets of S_n and $S_{n'}$; note that then automatically $n = n'$. Two representations are *distinct* if they are not equivalent.

[36]In other words, $\mathrm{AML}(1, 9)$ is the 2-point stabilizer of the Mathieu group M_{11}.

nius' Theorem (1901) [Fr],[37] it is clear that Burnside's original proof did not, since it is already given as Theorem IX on page 192 of the first edition of [Bu] published in 1897. In the second edition of [Bu] published in 1911, it occurs as Theorem XIII on page 202, and there Burnside gives two proofs of it, one using Frobenius and the other without.[38] Thus Burnside gives an "elementary" proof of the following Theorem without using "character theory."[39]

Burnside's Theorem. *A 2-transitive permutation group has a unique minimal normal subgroup. The said subgroup is either an elementary abelian group[40] or a nonabelian simple group.*

As a consequence of CTT and Weak CDT, and in view of a simple numerical lemma, we have the following.

Special CDT. *Given any prime p and any positive integer μ, concerning 2-transitive but not 3-transitive permutation groups of degree $q + 1$, where $q = p^\mu$, we have the following. If $\mu = 1$ and p is a Mersenne prime, then $\mathrm{PSL}(2, p)$, $\mathrm{AGL}(1, p + 1)$ and $\mathrm{A\Gamma L}(1, p + 1)$ are the only such groups. If $\mu = 1$ but p is not a Mersenne prime, then $\mathrm{PSL}(2, p)$ is the only such group, except that for $p = 2$ this group is "accidentally" 3-transitive because it coincides with S_3. If $\mu > 1$ then, in addition to the relevant groups listed in items (1), (3), (4), (5) of Weak CDT, the only other such groups are the groups $\mathrm{AGL}(1, 9)$, $\mathrm{A\Gamma L}(1, 9)$, $\mathrm{AML}(1, 9)$, $\mathrm{AGL}(2, 3)$, and $\mathrm{ASL}(2, 3)$, which occur when $(\mu, p) = (3, 2)$, and the group $\mathrm{AGL}(1, q + 1)$ which occurs when $q + 1$ is a Fermat prime.[41]*

Here is the said

Simple Numerical Lemma. *Given any primes p and π and any positive integers μ and u, such that $p^\mu + 1 = \pi^u$, we have the following. If $p > 2$, then $\mu = 1$ and $\pi = 2$ and $u = $ a prime number, and so p must be a Mersenne prime. If $p = 2$ and $u > 1$, then $\mu = 3$ and $\pi = 3$ and $u = 2$. If $p = 2$ and $u = 1$, then $\mu = $ a power of 2, and so π must be a Fermat prime.*

To see this, first suppose that $p > 2$; now p is odd and hence $p^\mu + 1$ is even and hence $\pi = 2$; since p is odd, we have $p \equiv 1(4)$ or $p \equiv 3(4)$ and hence $p^2 \equiv 1(4)$, and therefore if μ is even then $2^u = p^\mu + 1 \equiv 2(4)$ and this would imply $u = 1$ which would be absurd; on the other hand, if μ is odd then $2^u = p^\mu + 1 = (p + 1)(p^{\mu-1} - p^{\mu-2} + \cdots + 1)$ where the second parenthesis contains an odd number of odd terms and hence its value is odd, but since that value divides 2^u, it must be 1, and this gives $p^\mu + 1 = p + 1$ which implies

---

[37]For Frobenius' Theorem there is no "character free" proof. As examples of modern proofs of Burnside's Theorem which seem to use Frobenius' Theorem, see 12.4 on page 32 of Wielandt [Wi] and 7.12 on page 233 of volume III of Huppert-Blackburn [HB].

[38]In Burnside's classical style of writing, Theorem x means Theorem x together with the discussion around it. In other words, although everything is proved, only some of the conclusions are called theorems. This "classical" style is quite different from the so called "Landau Style" of Satz-Beweis-Bemerkung. In the classical style, you first discuss things and then suddenly say that you have proved such and such; in other words, the proof precedes the statement of a theorem.

[39]And certainly without using CT!

[40]A group is *elementary abelian* if it is isomorphic to $(Z_p)^m$ for some positive integer m and some prime p.

[41]A *Fermat prime* is a prime of the form $2^\mu + 1$ for some positive integer μ. It follows then that μ must be a power of 2, because otherwise $\mu = \mu'\mu''$ where μ' is even and $\mu'' > 1$ is odd and this would give the nontrivial factorization $2^\mu + 1 = (2^{\mu'} + 1)(2^{\mu'(\mu''-1)} - 2^{\mu'(\mu''-2)} + \cdots + 1)$.

$\mu = 1$. Next suppose that $p = 2$ and $u > 1$; now π must be odd, and if u is also odd then $2^{\mu} = \pi^{u} - 1 = (\pi - 1)(\pi^{u-1} + \pi^{u-2} + \cdots + 1)$ where the second parenthesis consists of u positive odd terms and hence its value is an odd number $\geq u$ and, since it divides 2^{μ}, it must be 1 which is absurd; on the other hand, if u is even then $2^{\mu} = \pi^{u} - 1 = (\pi^{u/2} - 1)(\pi^{u/2} + 1)$ and hence $\pi^{u/2} - 1$ and $\pi^{u/2} + 1$ are both powers of 2 whose difference is 2 and therefore they must be equal to 2 and 4, and this gives $\mu = 3$ and $\pi = 3$ and $u = 2$. Finally, if $p = 2$ and $u = 1$, then by the last footnote we see that μ must be a power of 2, and π must be a Fermat prime.

Here is another consequence of CDT.

Uniqueness Theorem for Transitive Extensions. *Any two transitive extensions of a transitive permutation group are isomorphic as permutation groups, with only one exception.*[42] *The exception is that* PSL$(2, 7)$ *and* $A\Gamma L(1, 8)$ *have a common 1-point stabilizer; note that both these are 2-transitive but not 3-transitive permutation groups of degree 8.*

As an immediate corollary of the above theorem we have the following.

Uniqueness Theorem for Transitive Extensions of 2-Transitive Groups. *Any two transitive extensions of a 2-transitive permutation group are isomorphic as permutation groups. In particular, the Mathieu groups* M_{11}, M_{12}, M_{22}, M_{23}, *and* M_{24} *are the unique transitive extensions of* PML$(2, 9)$, M_{11}, PSL$(3, 4)$, M_{22}, *and* M_{23} *respectively.*

To end this review of group theory, we note that by the *rank* of a transitive permutation group is meant the number of orbits of its 1-point stabilizer; the lengths of these orbits, excluding the obvious one point orbit, are called *subdegrees* of the group; so the number of subdegrees is one less than the rank, and the sum of the subdegrees is one less than the degree. Thus a 2-transitive group is simply a transitive group of rank 2. Now CT has also been used by Kantor-Liebler [KL], Liebeck [L], and others, to give CR3 = classification of transitive groups of rank 3, which although much longer than CDT, should be quite useful for Galois theory. Here is an amusing sample from CR3 which does not use CT and which can be found in Kantor [K1].

Sample from CR3. *For any integer* $n > 1$ *and any prime power* q, *the groups* PSp$(2n, q)$ *and* O$(2n+1, q)$ *are the only transitive permutation groups of rank 3 whose subdegrees are* $q(q^{2n-2} - 1)/(q - 1)$ *and* q^{2n-1}. *A rank 3 transitive permutation group* G *with subdegrees* $q(q + 1)^2$ *and* q^4 *for a prime power* $q > 1$, *is a subgroup of* Aut PSL$(4, q)$; *moreover, if* $q > 2$ *then* G *contains* PSL$(4, q)$.

18. A TYPE OF DERIVATIVE

To continue with the calculation of Galois groups, let me explain how to throw away a root $\alpha = \alpha_1$ of a polynomial

---

[42]If we don't assume the given group to be transitive, then there are numerous exceptions. For example every finite group, in its standard representation as a regular permutation group, is a transitive extension of the identity group. Since for increasing l, there are fewer and fewer l-transitive permutation groups, it follows that "most" transitive permutation groups have no transitive extensions.

$$f = f(Y) = Y^n + a_1 Y^{n-1} + \cdots + a_n = \prod_{i=1}^{n}(Y - \alpha_i)$$

by using a type of derivative. Now the coefficients $a_1, \ldots, a_n$ belong to a field K, and we want to find the polynomial

$$f_1 = f_1(Y) = \frac{f(Y)}{(Y - \alpha)} = Y^{n-1} + b_1 Y^{n-2} + \cdots + b_{n-1} \in K(\alpha)[Y].$$

To this end, first recall the three basic transformations of equations described in any old book. For instance, we may quote the following three relevant articles (= sections) from Burnside-Panton's 1904 book on the theory of equations [BP].[43]

Art 31. To multiply the roots by a given quantity. For any $u \neq 0$, the polynomial $g = g(Y)$ whose roots are u times the roots of f is given by

$$g(Y) = u^n f\left(\frac{Y}{u}\right) = Y^n + c_1 Y^{n-1} + \cdots + c_n = \prod_{i=1}^{n}(Y - u\alpha_i)$$

with $c_i = u^i a_i$.

Art 32. To reciprocate the roots. In case $\alpha_i \neq 0$ for $1 \leq i \leq n$, i.e., in case $a_n \neq 0$, the polynomial $g = g(Y)$ whose roots are the reciprocals of the roots of f is given by

$$g(Y) = \frac{Y^n}{a_n} f\left(\frac{1}{Y}\right) = \frac{1}{a_n}(1 + a_1 Y + \cdots + a_n Y^n) = \prod_{i=1}^{n}\left(Y - \left(\frac{1}{\alpha_i}\right)\right).$$

Art 33. To decrease the roots by a given quantity. For any u, the polynomial $g = g(Y)$ whose roots are $-u$ plus the roots of f is given by

$$g(Y) = f(Y + u) = Y^n + c_1 Y^{n-1} + \cdots + c_n = \prod_{i=1}^{n}(Y - (\alpha_i - u))$$

with $c_1 = a_1 + nu, \ldots, c_n = f(u)$.

Now in the first and the third cases provided $u \in K$, and in the second case without any proviso, we have $g(Y) \in K[Y]$ and, assuming the roots $\alpha_1, \ldots, \alpha_n$ to be pairwise distinct, we have $\mathrm{Gal}(g, K) = \mathrm{Gal}(f, K)$ as permutation groups, and so for Galois theory purposes we may conveniently modify f by one or more of these three transformations.

For example, sometimes it may be easier to compute the polynomial $g_1(Y)$ obtained by decreasing the roots of f_1 by α. In view of what we have just said, we get $\mathrm{Gal}(g_1, K(\alpha)) = \mathrm{Gal}(f_1, K(\alpha))$ and hence, assuming f to be irreducible in $K[Y]$, for the one-point stabilizer G_1 of $G = \mathrm{Gal}(f, K)$ we get $G_1 = \mathrm{Gal}(g_1, K(\alpha))$.

---

[43]For the last forty years I had happily assumed that this Burnside of the theory of equations [BP] was the same as the Burnside of the theory of groups of finite order [Bu]. To my dismay, at the Oxford Conference in April 1990, Peter Neumann told me that, although both were named William and both obtained a D.Sc. from Dublin around 1890, the equations Burnside was William Snow whereas the group theory Burnside was simply William. Strangely, I first learnt group theory from William Snow's book on the theory of equations.

Clearly g_1 can also be obtained by first decreasing the roots of f by α to get the polynomial $g = g(Y) = f(Y + \alpha)$, and then throwing away the root $Y = 0$ of g; this gives $g_1(Y) = g(Y)/Y$, and now remembering that $f(\alpha) = 0$ we get

$$g_1(Y) = \frac{f(Y + \alpha) - f(\alpha)}{Y}.$$

According to the calculus definition, by taking the "limit" of the RHS as Y tends to 0, we get $f'(\alpha)$. This motivates the following definition according to which g_1 *turns out to be the twisted Y-derivative of f at α*.

Definition. For any polynomial $\theta = \theta(Y)$ in an indeterminate Y with coefficients in a field L and for any element β in L, we call $(\theta(Y + \beta) - \theta(\beta))/Y$ the *twisted Y-derivative* of θ at β.

For a moment let us denote the twisted Y-derivative of θ at β by θ'. Then clearly $\theta' = \theta'(Y)$ is a polynomial in Y with coefficients in L, and if $\theta \in L$ then $\theta' = 0$, whereas: if $\theta \notin L$ then $\theta' \neq 0$ and the Y-degree of θ' is 1 less than the Y-degree of θ, and the two polynomials θ and θ' have the same leading coefficient, and hence in particular, if θ is monic then so in θ'.

Next we note that this is *L-linear* because for any $\delta = \delta(Y) \in L[Y]$ and $\lambda, \mu \in L$ we have

$$(\lambda\delta + \mu\theta)' = \frac{\lambda\delta(Y + \beta) + \mu\theta(Y + \beta) - \lambda\delta(\beta) - \mu\theta(\beta)}{Y} = \lambda\delta' + \mu\theta'.$$

However, the usual product rule is to be replaced by a *twisted product rule* because by the standard trick of adding and subtracting the same quantity we get

$$(\delta\theta)' = \frac{\delta(Y + \beta)\theta(Y + \beta) - \delta(Y + \beta)\theta(\beta)}{Y}$$
$$+ \frac{\delta(Y + \beta)\theta(\beta) - \delta(\beta)\theta(\beta)}{Y}$$
$$= \delta^*\theta' + \delta'\theta^\sharp$$

where δ^* is the *Y-translation* of δ by β and $\theta^\sharp$ is the *evaluation* of θ at β, i.e., $\delta^* = \delta^*(Y) = \delta(Y + \beta)$ and $\theta^\sharp = \theta(\beta)$.

Finally, for any positive integer m we have the *power rule*

$$(Y^m)' = Y^{m-1} + m\beta Y^{m-2} + \cdots + \binom{m}{i}\beta^i Y^{m-i-1} + \cdots + m\beta^{m-1}$$

and, in case $\operatorname{char} L \neq 0$, for any power q of $\operatorname{char} L$ we have the *prime power rule* $(Y^q)' = Y^{q-1}$ and combining this with the product rule, we get the *power product rule*

$$[Y^q\theta(Y)]' = (Y + \beta)^q\theta'(Y) + Y^{q-1}\theta(\beta).$$

The reason for explicitly mentioning Y in all this is that there may be other indeterminates present; for instance, if $\psi = \psi(X, Y)$ is a polynomial in indeterminates X and Y, and β is an element in a field which contains X as well as all the coefficients of ψ, then the twisted Y-derivative of ψ at β is given by $(\psi(X, Y) - \psi(X, \beta))/Y$.

Reverting to the original situation by taking $\beta = \alpha$ and $L = K(\alpha)$ in the above set-up, we conclude with the following.

Summary about the twisted derivative. If $f = f(Y)$ is a nonconstant monic irreducible polynomial in an indeterminate Y with coefficients in a field K such that f has no multiple root in any overfield of K, and if α is a root of f in some overfield of K, then by letting $f' = f'(Y)$ to be the twisted Y-derivative of f at α we have that the Galois group $\mathrm{Gal}(f', K(\alpha))$ is the one-point stabilizer of the Galois group $\mathrm{Gal}(f, K)$.

Now without assuming f to be irreducible and without any precondition about multiple roots, suppose the degree of f is $n > 2$ and suppose for every root α of $f(Y)$ in a splitting field of K we have that the twisted Y-derivative of $f(Y)$ at α is irreducible in $K(\alpha)[Y]$, then $f(Y)$ must be devoid of multiple roots; namely, if $f(Y) = \prod_{i=1}^{n}(Y - \alpha_i)$ and $\alpha_1 = \alpha_2$ and $f'(Y)$ is the twisted Y-derivative of $f(Y)$ at $\alpha = \alpha_1$, then $f'(Y)$ is reducible in $K(\alpha)[Y]$ because its degree is $n - 1 > 1$ and it has $(Y - \alpha_2)$ as a factor in $K(\alpha)[Y]$. Thus we have the following.

Twisted Derivative Criterion. *If $f(Y)$ is a nonconstant monic polynomial of degree > 2 in an indeterminate Y with coefficients in a field K such that for every root α of $f(Y)$ in a splitting field of K we have that the twisted Y-derivative of $f(Y)$ at α is irreducible in $K(\alpha)[Y]$, then $f(Y)$ has no multiple roots in any overfield of K.*

19. CYCLE LEMMA

As another tool for calculating Galois groups, let us make note of a "cycle lemma".

Let K be a field and consider a monic polynomial

$$f = f(Y) = Y^n + a_1 Y^{n-1} + \cdots + a_n = \prod_{i=1}^{n}(Y - \alpha_i)$$

of degree n in an indeterminate Y with coefficients $a_1, \ldots, a_n$ in K having pairwise distinct roots $\alpha_1, \ldots, \alpha_n$ in some overfield of K. Now by conveniently enlarging the said overfield and moving it by a K-isomorphism, it can be construed to contain any preassigned overfield K^* of K, and this gives us the following obvious but basic principle of computational Galois theory.

Basic Extension Principle. *For any given overfield K^* of K, the Galois group $\mathrm{Gal}(f, K^*)$, as a permutation group of degree n, acting on the roots $\{\alpha_1, \ldots, \alpha_n\}$, may be regarded as a subgroup of the Galois group $\mathrm{Gal}(f, K)$.*

Given any overfield K^* of K and any factorization

$$f(Y) = \prod_{j=1}^{m} e_j(Y) \quad \text{where } e_j(Y) = Y^{n_j} + a_{j1}Y^{n_j-1} + \cdots + a_{jn_j}$$

with $a_{j1}, \ldots, a_{jn_j}$ in K^* we can relabel the roots $\alpha_1, \ldots, \alpha_n$ as $\alpha_{11}, \ldots, \alpha_{1,n_1}, \ldots, \alpha_{m1}, \ldots, \alpha_{mn_m}$ so that

$$e_j = e_j(Y) = \prod_{i=1}^{n_j}(Y - \alpha_{ji}) \quad \text{for } 1 \le j \le m$$

and we can identify the direct product $S_{n_1} \times \cdots \times S_{n_m}$, where S_{n_j} is the symmetric group acting on $\alpha_{j1}, \ldots, \alpha_{jn_j}$, with a subgroup of the symmetric group

S_n acting on $\alpha_1, \ldots, \alpha_n$. As a second obvious but basic principle we then have the following.

Basic Projection Principle. *For the Galois group* $\mathrm{Gal}(f, K^*) \subset S_n$ *we have* $\mathrm{Gal}(f, K^*) \subset S_{n_1} \times \cdots \times S_{n_m}$, *and for* $1 \le j \le m$, *the Galois group* $\mathrm{Gal}(f, K^*)$ *maps onto the Galois group* $\mathrm{Gal}(e_j, K^*) \subset S_{n_j}$ *under the natural projection* $S_{n_1} \times \cdots \times S_{n_m} \to S_{n_j}$.

Recall that a *ν-cycle* is a permutation σ, say in S_n, such that for some ν distinct elements $\alpha_{i_1}, \ldots, \alpha_{i_\nu}$ in $\{\alpha_1, \ldots, \alpha_n\}$ we have $\sigma(\alpha_{i_1}) = \alpha_{i_2}, \ldots, \sigma(\alpha_{i_{\nu-1}}) = \alpha_{i_\nu}$, $\sigma(\alpha_{i_\nu}) = \alpha_{i_1}$ and $\sigma(\alpha_j) = \alpha_j$ for all $j \notin \{i_1, \ldots, i_\nu\}$. Now if $e_1(Y)$ is irreducible in $K^*[Y]$ and if either n_1 is prime or $\mathrm{Gal}(e_1, K^*)$ is cyclic, then clearly $\mathrm{Gal}(e_1, K^*)$ contains an n_1-cycle τ_1, and by the Projection Principle τ_1 is the projection of some $\tau \in \mathrm{Gal}(f, K^*)$, and if also $|\mathrm{Gal}(e_j, K^*)|$ and n_1 are coprime for $2 \le j \le m$ then upon letting μ to be the product of $|\mathrm{Gal}(e_2, K^*)|, \ldots, |\mathrm{Gal}(e_m, K^*)|$ we see that $\tau^\mu \in \mathrm{Gal}(f, K^*)$ is an n_1-cycle. Therefore in view of the Extension Principle we get the following.

Cycle Prelemma. *If* $|\mathrm{Gal}(e_j, K^*)|$ *and* n_1 *are coprime for* $2 \le j \le m$, *and* $e_1(Y)$ *is irreducible in* $K^*[Y]$, *and either* n_1 *is prime or* $\mathrm{Gal}(e_1, K^*)$ *is cyclic, then* $\mathrm{Gal}(f, K)$ *contains an* n_1-*cycle.*

To convert the Cycle Prelemma into the Cycle Lemma, let v be a (real discrete) *valuation*[44] of K, i.e., v is a map of K onto the set of all integers together with the symbol ∞ such that for all a, b in K we have $v(a) = \infty \Leftrightarrow a = 0$, and $v(ab) = v(a) + v(b)$, and $v(a + b) \ge \min(v(a), v(b))$. Recall that $\{a \in K : v(a) \ge 0\}$ is called the *valuation ring* of v, and this ring modulo the unique maximal ideal $\{a \in K : v(a) > 0\}$ in it is called the *residue field* of v. Also recall that v is said to be *trivial* on a subfield k of K, or v is said to be a valuation of K/k, if $v(a) = 0$ for all $0 \ne a \in k$. Let $\widehat{K}$ be a finite algebraic field extension of K and let $\hat{v}_1, \ldots, \hat{v}_h$ be the extensions of v to $\widehat{K}$, i.e., $\hat{v}_1, \ldots, \hat{v}_h$ are those valuations of $\widehat{K}$ whose valuation rings intersected with K give the valuation ring of v; we may also say that v *splits* in $\widehat{K}$ into $\hat{v}_1, \ldots, \hat{v}_h$. By $\bar{r}(\hat{v}_j : v)$ we denote the *reduced ramification exponent*[45] of $\hat{v}_j$ over v, i.e., $\bar{r}(\hat{v}_j : v)$ is the unique positive integer such that for all $a \in K$ we have $\hat{v}_j(a) = \bar{r}(\hat{v}_j : v)v(a)$. By $\bar{d}(\hat{v}_j : v)$ we denote the *residue degree* of $\hat{v}_j$ over v, i.e., $\bar{d}(\hat{v}_j : v)$ is the field degree of the residue field of $\hat{v}_j$ over the residue field of v. Note that *if either $\widehat{K}/K$ is separable, or v is trivial over a subfield k of K such that K/k is finitely generated of transcendence degree 1, then*

$$(\dagger) \qquad \sum_{j=1}^{h} \bar{r}(\hat{v}_j : v)\bar{d}(\hat{v}_j : v) = [\widehat{K} : K].$$

Also note that $\hat{v}_j$ is *unramified* over v, or over K, means that $\bar{r}(\hat{v}_j : v) = 1$ and the residue field of $\hat{v}_j$ is separable over the residue field of v; $\hat{v}_j$ is *ramified* over v, or over K, means that $\hat{v}_j$ is not unramified over v; v is *unramified* in $\widehat{K}$ means that $\hat{v}_j$ is unramified over v for $1 \le j \le h$; and finally, v is

---

[44]In this paper, by a valuation we shall mean a real discrete valuation.

[45]Also called the reduced ramification index.

ramified in $\widehat{K}$ means that v is not unramified in $\widehat{K}$. Now it is well known that if $f(Y)$ is irreducible in $K[Y]$, $\widehat{K} = K(\alpha_1)$, K^* = the completion of K with respect to v, and $e_j(Y)$ is irreducible in $K^*[Y]$ for $1 \leq j \leq m$, then $h = m$ and, after a suitable relabelling, $\bar{r}(\hat{v}_j : v)\bar{d}(\hat{v}_j : v) = n_j$ for $1 \leq j \leq h$; for instance see §2 of [A2]. Moreover, by Newton's Theorem, if the residue field of v is an algebraically closed field of the same characteristic as K, and if $n_j \not\equiv 0(\text{char } K)$ for some j, then for that j the Galois group $\text{Gal}(e_j, K^*)$ is cyclic; for a proof of Newton's Theorem based on Shreedharacharya's method of completing the square, see my new book on algebraic geometry for scientists and engineers [A6]. Therefore by the Cycle Prelemma we get the

Cycle Lemma. *If $f(Y)$ is irreducible in $K[Y]$ and there exists a valuation v of K such that the residue field of v is an algebraically closed field of the same characteristic as K and such that for the extensions $\hat{v}_1, \ldots, \hat{v}_h$ of v to a root field[46] of $f(Y)$ over K we have that $\bar{r}(\hat{v}_j : v)$ and $\bar{r}(\hat{v}_1 : v)$ are coprime and $\bar{r}(\hat{v}_j : v) \not\equiv 0(\text{char } K)$ for $1 < j \leq h$, and either $\bar{r}(\hat{v}_1 : v)$ is prime or $\bar{r}(\hat{v}_1 : v) \not\equiv 0(\text{char } K)$, then the Galois group $\text{Gal}(f, K)$ contains an $\bar{r}(\hat{v}_1 : v)$-cycle.*

The Basic Extension Principle can be refined thus.

Refined Extension Principle. *Given any field extensions $K \subset K' \subset K^*$, by the Basic Extension Principle we may regard $\text{Gal}(f, K^*) < \text{Gal}(f, K') < \text{Gal}(f, K) < S_n$, and assuming K^* to be a finite normal extension of K we have that $\text{Gal}(f, K^*) \lhd \text{Gal}(f, K)$ and the factor group $\text{Gal}(f, K)/\text{Gal}(f, K^*)$ is a homomorphic image of $\text{Gal}(K^*, K)$.*[47]

To see this, let $L = K(\alpha_1, \ldots, \alpha_n)$ and $L^* = K^*(\alpha_1, \ldots, \alpha_n)$. Now L is a (finite) Galois extension of K, and given any $\sigma \in \text{Gal}(f, K)$, we view σ as a permutation of $\{1, 2, \ldots, n\}$ such that for some (actually unique) $\tau \in \text{Gal}(L, K)$ we have $\tau(\alpha_i) = \alpha_{\sigma(i)}$ for $1 \leq i \leq n$. Likewise, L^* is a (finite) Galois extension of K^*, and given any $\sigma^* \in \text{Gal}(f, K^*)$, we view σ^* as a permutation of $\{1, 2, \ldots, n\}$ such that for some (actually unique) $\tau^* \in \text{Gal}(L^*, K^*)$ we have $\tau^*(\alpha_i) = \alpha_{\sigma^*(i)}$ for $1 \leq i \leq n$. Obviously, $\sigma = \sigma^* \Leftrightarrow \tau = \tau^*|L$ where $\tau^*|L$ denotes the restriction of τ^* to L. Thus we get the commutative diagram

$$
\begin{array}{ccc}
\text{Gal}(f, K^*) & \longrightarrow & \text{Gal}(f, K) \\
\downarrow & & \downarrow \\
\text{Gal}(L^*, K^*) & \xrightarrow{\;\delta\;} & \text{Gal}(L, K)
\end{array}
$$

where the left arrow is the isomorphism $\sigma^* \mapsto \tau^*$, the right arrow is the isomorphism $\sigma \mapsto \tau$, the top arrow is the inclusion $\text{Gal}(f, K^*) \subset \text{Gal}(f, K)$, and the bottom arrow δ is the injection $\tau^* \mapsto \tau^*|L$. Therefore our assertion is equivalent to saying that $\text{im } \delta$ is a normal subgroup of $\text{Gal}(L, K)$ and

---

[46]A *root field* of $f(Y)$ over K is a field obtained by adjoining a root of $f(Y)$ to K, for instance the field $K(\alpha_1)$.

[47]That is, $\text{Gal}(f, K)/\text{Gal}(f, K^*) \approx \text{Gal}(K^*, K)/N$ for some normal subgroup N of $\text{Gal}(K^*, K)$. Note that for any finite normal extension K^* of a field K, without assuming K^* to be separable over K, the Galois group $\text{Gal}(K^*, K)$ is defined to be the group of all K-automorphisms of K^*.

$\mathrm{Gal}(L, K)/\mathrm{im}\,\delta \approx \mathrm{Gal}(K^*, K)/N$ for some normal subgroup N of $\mathrm{Gal}(K^*, K)$. To prove this new version of the assertion, let $K_0 = L \cap K^*$, let K_0^* be the maximal separable algebraic field extension of K_0 in K^*, let $L_0^* = K_0^*(\alpha_1, \ldots, \alpha_n)$, and let us depict all this in the following Hasse diagram.
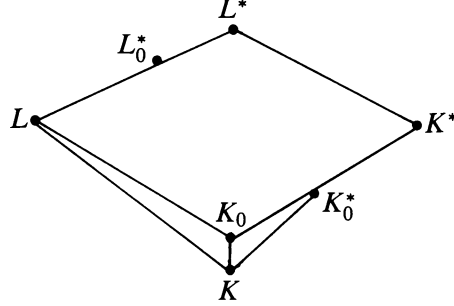
Referring to the lower quadrilateral in the above diagram, L_0^*/K_0 is a finite Galois extension, the field L_0^* is a compositum of the fields L and K_0^* with $L \cap K_0^* = K_0$, and the four sides of the said quadrilateral represent the finite Galois extensions L/K_0, K_0^*/K_0, L_0^*/L, and L_0^*/K_0^*; hence by the Fundamental Theorem of Galois Theory, the group $\mathrm{Gal}(L_0^*, K_0)$ is the internal direct product of the two normal subgroups[48] $\mathrm{Gal}(L_0^*, L)$ and $\mathrm{Gal}(L_0^*, K_0^*)$, and $\lambda^* \mapsto \lambda^*|L$ gives a surjection $\mathrm{Gal}(L_0^*, K_0) \to \mathrm{Gal}(L, K_0)$ whose kernel is $\mathrm{Gal}(L_0^*, L)$ and whose restriction to $\mathrm{Gal}(L_0^*, K_0^*)$ is an isomorphism $\mathrm{Gal}(L_0^*, K_0^*) \xrightarrow{\theta} \mathrm{Gal}(L, K_0)$. By applying the Fundamental Theorem of Galois Theory to the left triangle in the above diagram, i.e., by noting that L/K, L/K_0, and K_0/K are Galois extensions, we see that $\mathrm{Gal}(L, K_0)$ is a normal subgroup of $\mathrm{Gal}(L, K)$ and $\mathrm{Gal}(L, K)/\mathrm{Gal}(L, K_0) \approx \mathrm{Gal}(K_0, K)$. Upon letting $\mathrm{Gal}(L, K_0) \xrightarrow{\theta^*} \mathrm{Gal}(L, K)$ be the natural inclusion $\mathrm{Gal}(L, K_0) \subset \mathrm{Gal}(L, K)$, we see that the composition $\mathrm{Gal}(L_0^*, K_0^*) \xrightarrow{\theta} \mathrm{Gal}(L, K_0) \xrightarrow{\theta^*} \mathrm{Gal}(L, K)$ coincides with the injection $\mathrm{Gal}(L_0^*, K_0^*) \xrightarrow{\delta_0} \mathrm{Gal}(L, K)$ given by $\lambda^* \mapsto \lambda^*|L$, and hence

$$\mathrm{im}\,\delta_0 = \mathrm{Gal}(L, K_0) \triangleleft \mathrm{Gal}(L, K)$$

and

$$\mathrm{Gal}(L, K)/\mathrm{im}\,\delta_0 \approx \mathrm{Gal}(K_0, K).$$

By applying the Fundamental Theorem of Galois Theory to the right triangle in the above diagram, i.e., by noting that K_0^*/K, K_0^*/K_0, and K_0/K are finite Galois extensions, we see that

$$\mathrm{Gal}(K_0^*, K_0) \triangleleft \mathrm{Gal}(K_0^*, K) \quad \text{and} \quad \mathrm{Gal}(K_0^*, K)/\mathrm{Gal}(K_0^*, K_0) \approx \mathrm{Gal}(K_0, K).$$

Therefore, upon letting $N = \mathrm{Gal}(K_0^*, K_0)$, we conclude that

$$\mathrm{im}\,\delta_0 \triangleleft \mathrm{Gal}(L, K) \quad \text{and} \quad \mathrm{Gal}(L, K)/\mathrm{im}\,\delta_0 \approx \mathrm{Gal}(K_0^*, K)/N$$

for some

$$N \triangleleft \mathrm{Gal}(K_0^*, K).$$

---

[48]That is, the intersection of the two normal subgroups is the identity and they generate the whole group.

Finally, referring to the modified diagram obtained by deleting the three lines emanating from K_0 in the above diagram, L/K and K_0^*/K are finite Galois extensions; K^*/K is a finite normal extension; K^*/K_0^* is pure inseparable; L_0^* is a compositum of L and K_0^*; and L^* is a compositum of L_0^* and K^*. Consequently $\lambda \mapsto \lambda|K_0^*$ gives an isomorphism $\mathrm{Gal}(K^*, K) \to \mathrm{Gal}(K_0^*, K)$, whereas $\lambda' \mapsto \lambda'|L_0^*$ gives an isomorphism

$$\mathrm{Gal}(L^*, K^*) \xrightarrow{\delta'} \mathrm{Gal}(L_0^*, K_0^*)$$

such that $\delta_0(\mathrm{im}\,\delta') = \mathrm{im}\,\delta$; therefore by the next to last display we conclude that

$$\mathrm{im}\,\delta \lhd \mathrm{Gal}(L, K) \quad \text{and} \quad \mathrm{Gal}(L, K)/\mathrm{im}\,\delta \approx \mathrm{Gal}(K^*, K)/N$$

for some $N \lhd \mathrm{Gal}(K^*, K)$.

For applying to specific situations, here are some

Corollaries of the Refined Extension Principle. *Given any finite algebraic field extension K' of K, by the Basic Extension Principle we may regard $\mathrm{Gal}(f, K') < \mathrm{Gal}(f, K) < S_n$, and then upon letting K^* be a least normal extension of K containing K', we have the following.*

(1.1) *There exists $N \lhd \mathrm{Gal}(K^*, K)$ and $M \lhd \mathrm{Gal}(f, K)$ with $M < \mathrm{Gal}(f, K')$ such that $\mathrm{Gal}(f, K)/M \approx \mathrm{Gal}(K^*, K)/N$.*

(1.2) *If $\mathrm{Gal}(K^*, K)$ is solvable, then there exists $M \lhd \mathrm{Gal}(f, K)$ with $M < \mathrm{Gal}(f, K')$ such that $\mathrm{Gal}(f, K)/M$ is solvable.*

(1.3) *If $\mathrm{Gal}(K^*, K)$ is solvable, and $\mathrm{Gal}(f, K) = S_n$, and $3 \neq n \neq 4$, then $\mathrm{Gal}(f, K') = S_n$ or A_n.*

(1.4) *If $\mathrm{Gal}(K^*, K)$ is cyclic and $\mathrm{Gal}(f, K) = S_n$, then $\mathrm{Gal}(f, K') = S_n$ or A_n.*

(1.5) *If $\mathrm{Gal}(K^*, K)$ is cyclic of odd order and $\mathrm{Gal}(f, K) = S_n$, then $\mathrm{Gal}(f, K') = S_n$.*

(1.6) *If there is no nonidentity group which is a homomorphic image of $\mathrm{Gal}(f, K)$ as well as $\mathrm{Gal}(K^*, K)$, then $\mathrm{Gal}(f, K') = \mathrm{Gal}(f, K)$.*

(1.7) *If $\mathrm{Gal}(f, K)$ is a simple group which is not a homomorphic image of $\mathrm{Gal}(K^*, K)$, then $\mathrm{Gal}(f, K') = \mathrm{Gal}(f, K)$.*

(1.8) *If $\mathrm{Gal}(K^*, K)$ is solvable and $\mathrm{Gal}(f, K)$ is nonabelian simple, then $\mathrm{Gal}(f, K') = \mathrm{Gal}(f, K)$.*

(1.9) *If $\mathrm{Gal}(K^*, K)$ is solvable, and $\mathrm{Gal}(f, K) = A_n$, and $3 \neq n \neq 4$, then $\mathrm{Gal}(f, K') = A_n$.*

(1.10) *If $\mathrm{Gal}(K^*, K)$ is cyclic, and $\mathrm{Gal}(f, K) = A_n$, and $n = 4$, then $\mathrm{Gal}(f, K') = A_n$ or $(Z_2)^2$.*

(1.11) *If $\mathrm{Gal}(K^*, K)$ is cyclic, and $\mathrm{Gal}(f, K) = A_n$, and $n = 3$, then $\mathrm{Gal}(f, K') = A_n$ or Z_1.*

(1.12) *If $\mathrm{Gal}(K^*, K)$ is cyclic of order nondivisible by 3 and $\mathrm{Gal}(f, K) = A_n$, then $\mathrm{Gal}(f, K') = A_n$.*

(1.13) *If $\mathrm{Gal}(K^*, K)$ is solvable and $\mathrm{Gal}(f, K) = \mathrm{PSL}(2, q)$ for a prime power $q > 3$, then $\mathrm{Gal}(f, K') = \mathrm{PSL}(2, q)$.*

(1.14) *If $\mathrm{Gal}(K^*, K)$ is cyclic of order nondivisible by $\mathrm{char}\,k$ and $\mathrm{Gal}(f, K) = \mathrm{PSL}(2, q)$ with $1 < q = n - 1 = $ a power of $\mathrm{char}\,k$, then $\mathrm{Gal}(f, K') = \mathrm{PSL}(2, q)$.*

(1.1) follows by taking $M = \mathrm{Gal}(f, K^*)$ in the Refined Extension Principle.

The implication $(1.1) \Rightarrow (1.2)$ follows from the fact that a homomorphic image of a finite solvable group is solvable. In view of (1.1), the implication $(1.2) \Rightarrow (1.3)$ follows from the facts that if $n \geq 5$ then S_n is nonsolvable, and A_n and S_n are the only nonidentity normal subgroups of S_n, and there are no other subgroups of S_n between A_n and S_n, whereas if $n \leq 2$ then A_n and S_n are the only subgroups of S_n. In view of (1.1), the implication $(1.3) \Rightarrow (1.4)$ follows from the fact that S_3 and S_4 are noncyclic; A_3 is the only nonidentity normal subgroup of S_3, for the factor group we have $S_3/A_3 = Z_2$, and the only nonidentity normal subgroup of S_4 other than A_4 is the Klein group $(Z_2)^2$ consisting of the four permutations (1), $(12)(34)$, $(13)(24)$, $(14)(23)$, and the factor group of S_4 by the Klein group is isomorphic to S_3. In view of (1.1), the implication $(1.4) \Rightarrow (1.5)$ follows from the fact that $S_n/A_n = Z_2$ or Z_1. The implications $(1.1) \Rightarrow (1.6) \Rightarrow (1.7)$ are obvious. The implication $(1.7) \Rightarrow (1.8)$ follows from the fact that a homomorphic image of a finite solvable group is solvable. In view of (1.1), the implication $(1.8) \Rightarrow (1.9)$ follows from the facts that if $n \geq 5$ then A_n is nonabelian simple, whereas if $n \leq 2$ then $A_n = Z_1$. The implication $(1.1) \Rightarrow (1.10)$ follows from the facts that A_4 is not cyclic, and the Klein group $(Z_2)^2$ is the only nonidentity normal subgroup of A_4, and the factor group by the Klein group is Z_3. The implication $(1.1) \Rightarrow (1.11)$ follows from the fact that $A_3 = Z_3$. In view of (1.1), (1.10), and (1.11), the implication $(1.9) \Rightarrow (1.12)$ follows from the fact that $A_4/(Z_2)^2 = Z_3 = A_3$. The implication $(1.8) \Rightarrow (1.13)$ follows from the fact that $\mathrm{PSL}(2, q)$ is nonabelian simple for every prime power $q > 3$. Finally, in view of (1.1), and what we have said about S_3 and A_4, the implication $(1.13) \Rightarrow (1.14)$ follows from the facts that $\mathrm{PSL}(2, 2) = S_3$ and $\mathrm{PSL}(2, 3) = A_4$.

As a consequence of the Refined Extension Principle we have the

Substitutional Principle. *Assume that $K = $ the field $k(X)$ of rational functions in an indeterminate X with coefficients in a field k, i.e., $a_i = a_i(X) \in k(X)$ for $1 \leq i \leq n$. Given any $\chi(X) \in k(X) \setminus k$, let*

$$f_\chi = f_\chi(Y) = Y^n + a_1(\chi(X))Y^{n-1} + \cdots + a_n(\chi(X)) \in k(X)[Y] = K[Y]$$

and let $K' = k(V)$ where V is an indeterminate. Then the k-homomorphism $X \mapsto \chi(V)$ gives an embedding $K = k(X) \subset k(V) = K'$, and by sending Y to Y it gives an embedding $K[Y] = k(X)[Y] \subset k(V)[Y] = K'[Y]$, and this sends f to f_χ with X changed to V. Therefore, f_χ has no multiple roots in any field extension of $k(X)$ and, upon letting $K^* = $ a least normal extension of $k(X)$ containing $k(V)$, by the Basic Extension Principle we may regard $\mathrm{Gal}(f, K^*) < \mathrm{Gal}(f, k(V)) = \mathrm{Gal}(f_\chi, k(X)) < \mathrm{Gal}(f, k(X)) < S_n$, and now by the Refined Extension Principle $\mathrm{Gal}(f, K^*) \triangleleft \mathrm{Gal}(f, k(X))$ and $\mathrm{Gal}(f, k(X))/\mathrm{Gal}(f, K^*) \approx \mathrm{Gal}(K^*, k(X))/N$ for some $N \triangleleft \mathrm{Gal}(K^*, k(X))$.[49]

Here are the corresponding

Corollaries of the Substitutional Principle. *Letting the situation be as in the Substitutional Principle, and remembering that $K^* = $ a finite normal extension of $k(X)$ and $\mathrm{Gal}(f_\chi, k(X)) < \mathrm{Gal}(f, k(X)) < S_n$, we have the following.*

---

[49]Note that by writing $\chi(X) = \chi'(X)/\chi''(X)$, where $\chi'(X)$ and $\chi''(X)$ are coprime nonzero polynomials in X with coefficients in k, we have $K^* = $ a splitting field of $\chi'(Y) - X\chi''(Y)$ over $k(X)$, and if the said splitting field coincides with a root field of $\chi'(Y) - X\chi''(Y)$ over $k(X)$, then we have $\mathrm{Gal}(f, K^*) = \mathrm{Gal}(f, k(V)) = \mathrm{Gal}(f_\chi, k(X))$.

(2.1) *There exists* $N \triangleleft \operatorname{Gal}(K^*, k(X))$ *and* $M \triangleleft \operatorname{Gal}(f, k(X))$ *with* $M < \operatorname{Gal}(f_\chi, k(X))$ *such that* $\operatorname{Gal}(f, k(X))/M \approx \operatorname{Gal}(K^*, k(X))/N$.

(2.2) *If* $\operatorname{Gal}(K^*, k(X))$ *is solvable, then there exists* $M \triangleleft \operatorname{Gal}(f, k(X))$ *with* $M < \operatorname{Gal}(f_\chi, k(X))$ *such that* $\operatorname{Gal}(f, k(X))/M$ *is solvable.*

(2.3) *If* $\operatorname{Gal}(K^*, k(X))$ *is solvable, and* $\operatorname{Gal}(f, k(X)) = S_n$, *and* $3 \neq n \neq 4$, *then* $\operatorname{Gal}(f_\chi, k(X)) = S_n$ *or* A_n.

(2.4) *If* $\operatorname{Gal}(K^*, k(X))$ *is cyclic and* $\operatorname{Gal}(f, k(X)) = S_n$, *then* $\operatorname{Gal}(f_\chi, k(X)) = S_n$ *or* A_n.

(2.5) *If* $\operatorname{Gal}(K^*, k(X))$ *is cyclic of odd order and* $\operatorname{Gal}(f, k(X)) = S_n$, *then* $\operatorname{Gal}(f_\chi, k(X)) = S_n$.

(2.6) *If there is no nonidentity group which is a homomorphic image of* $\operatorname{Gal}(f, k(X))$ *as well as* $\operatorname{Gal}(K^*, k(X))$, *then* $\operatorname{Gal}(f_\chi, k(X)) = \operatorname{Gal}(f, k(X))$.

(2.7) *If* $\operatorname{Gal}(f, k(X))$ *is a simple group which is not a homomorphic image of* $\operatorname{Gal}(K^*, k(X))$, *then* $\operatorname{Gal}(f_\chi, k(X)) = \operatorname{Gal}(f, k(X))$.

(2.8) *If* $\operatorname{Gal}(K^*, k(X))$ *is solvable and* $\operatorname{Gal}(f, k(X))$ *is nonabelian simple, then* $\operatorname{Gal}(f_\chi, k(X)) = \operatorname{Gal}(f, k(X))$.

(2.9) *If* $\operatorname{Gal}(K^*, k(X))$ *is solvable, and* $\operatorname{Gal}(f, k(X)) = A_n$, *and* $3 \neq n \neq 4$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$.

(2.10) *If* $\operatorname{Gal}(K^*, k(X))$ *is cyclic, and* $\operatorname{Gal}(f, k(X)) = A_n$, *and* $n = 4$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$ *or* $(Z_2)^2$.

(2.11) *If* $\operatorname{Gal}(K^*, k(X))$ *is cyclic, and* $\operatorname{Gal}(f, k(X)) = A_n$, *and* $n = 3$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$ *or* Z_1.

(2.12) *If* $\operatorname{Gal}(K^*, k(X))$ *is cyclic of order nondivisible by* 3 *and* $\operatorname{Gal}(f, k(X)) = A_n$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$.

(2.13) *If* $\operatorname{Gal}(K^*, k(X))$ *is solvable and* $\operatorname{Gal}(f, k(X)) = \operatorname{PSL}(2, q)$ *for a prime power* $q > 3$, *then* $\operatorname{Gal}(f_\chi, k(X)) = \operatorname{PSL}(2, q)$.

(2.14) *If* $\operatorname{Gal}(K^*, k(X))$ *is cyclic of order nondivisible by* char k *and* $\operatorname{Gal}(f, k(X)) = \operatorname{PSL}(2, q)$ *with* $1 < q = n - 1 = $ *a power of* char k, *then* $\operatorname{Gal}(f_\chi, k(X)) = \operatorname{PSL}(2, q)$.

The proof of (2.1) to (2.14) follows from the above proof of (1.1) to (1.14) by changing "Refined Extension Principle" to "Substitutional Principle" and by changing (1.i) to (2.i) for $1 \leq i \leq 14$.

Stated in a form more suitable for applying to the specific equations described earlier, here are some further

Corollaries of the Substitutional Principle. *Letting the situation be as in the Substitutional Principle, and remembering that* $\operatorname{Gal}(f_\chi, k(X)) < \operatorname{Gal}(f, k(X)) < S_n$, *and assuming that* k *is algebraically closed and* $\chi(X) = cX^r$ *with* $0 \neq c \in k$ *and nonzero integer* r, *we have the following.*

(3.1) *There exists* $M \triangleleft \operatorname{Gal}(f, k(X))$ *with* $M < \operatorname{Gal}(f_\chi, k(X))$ *such that* $\operatorname{Gal}(f, k(X))/M$ *is a cyclic group whose order is nondivisible by* char k *but divides* r.

(3.2) *If* $\operatorname{Gal}(f, k(X)) = S_n$, *then* $\operatorname{Gal}(f_\chi, k(X)) = S_n$ *or* A_n.

(3.3) *If* $\operatorname{Gal}(f, k(X)) = S_n$ *and* char $k = 2$, *then* $\operatorname{Gal}(f_\chi, k(X)) = S_n$.

(3.4) *If* $\operatorname{Gal}(f, k(X))$ *is nonabelian simple, then* $\operatorname{Gal}(f_\chi, k(X)) = \operatorname{Gal}(f, k(X))$.

(3.5) *If* $\operatorname{Gal}(f, k(X)) = A_n$ *and* $3 \neq n \neq 4$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$.

(3.6) *If* $\operatorname{Gal}(f, k(X)) = A_n$ *and* $n = 4$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$ *or* $(Z_2)^2$.

(3.7) *If* $\operatorname{Gal}(f, k(X)) = A_n$ *and* $n = 3$, *then* $\operatorname{Gal}(f_\chi, k(X)) = A_n$ *or* Z_1.

(3.8) *If* $\mathrm{Gal}(f, k(X)) = A_n$ *and* $\mathrm{char}\, k = 3$, *then* $\mathrm{Gal}(f_\chi, k(X)) = A_n$.

(3.9) *If* $\mathrm{Gal}(f, k(X)) = \mathrm{PSL}(2, q)$ *for a prime power* $q > 3$, *then* $\mathrm{Gal}(f_\chi, k(X)) = \mathrm{PSL}(2, q)$.

(3.10) *If* $\mathrm{Gal}(f, k(X)) = \mathrm{PSL}(2, q)$ *with* $1 < q = n - 1 = $ *a power of* $\mathrm{char}\, k$, *then* $\mathrm{Gal}(f_\chi, k(X)) = \mathrm{PSL}(2, q)$.

Namely, $\mathrm{Gal}(K^*, K)$, i.e., the Galois group of the splitting field of $Y^{|r|} - \left(\frac{x}{c}\right)^{r/|r|}$ over $k(X)$ is a cyclic group whose order is nondivisible by $\mathrm{char}\, k$ but divides r, and hence (3.1), (3.2), (3.3) follow from (2.1), (2.4), (2.5) respectively, and (3.i) follows from (2.$i + 4$) for $4 \leq i \leq 10$.

Here are still some more

Corollaries of the Substitutional Principle. *Letting the situation be as in the Substitutional Principle, and remembering that* $\mathrm{Gal}(f_\chi, k(X)) < \mathrm{Gal}(f, k(X)) < S_n$, *and assuming that*

$$\chi(X) = \chi_d(\chi_{d-1}(\cdots(\chi_1(X))\cdots)),$$

where d *is a positive integer and*

$$\chi_i(X) = \frac{\chi_i'(X)}{\chi_i''(X)} \in k(X) \setminus k$$

with coprime nonzero members $\chi_i'(X)$ *and* $\chi_i''(X)$ *of* $k[X]$ *for* $1 \leq i \leq d$, *and upon letting* K_i^* *to be a splitting field of* $\chi_i'(Y) - X\chi_i''(Y)$ *over* $k(X)$ *for* $1 \leq i \leq d$, *we have the following.*

(4.1) *If for each* i *with* $1 \leq i \leq d$ *we have that there is no nonidentity group which is a homomorphic image of* $\mathrm{Gal}(f, k(X))$ *as well as* $\mathrm{Gal}(K_i^*, k(X))$, *then* $\mathrm{Gal}(f_\chi, k(X)) = \mathrm{Gal}(f, k(X))$.

(4.2) *If* $\mathrm{Gal}(f, k(X))$ *is a simple group which is not a homomorphic image of* $\mathrm{Gal}(K_i^*, k(X))$ *for any* i *with* $1 \leq i \leq d$, *then* $\mathrm{Gal}(f_\chi, k(X)) = \mathrm{Gal}(f, k(X))$.

(4.3) *If* $\mathrm{Gal}(K_i^*, k(X))$ *is solvable for each* i *with* $1 \leq i \leq d$, *and* $\mathrm{Gal}(f, k(X))$ *is nonabelian simple, then* $\mathrm{Gal}(f_\chi, k(X)) = \mathrm{Gal}(f, k(X))$.

(4.4) *If* $\mathrm{Gal}(K_i^*, k(X))$ *is solvable for each* i *with* $1 \leq i \leq d$, *and* $\mathrm{Gal}(f, k(X)) = A_n$, *and* $3 \neq n \neq 4$, *then* $\mathrm{Gal}(f_\chi, k(X)) = A_n$.

Namely, (4.1), (4.2), (4.3), and (4.4) follow by repeatedly applying (2.6), (2.7), (2.8), and (2.9) respectively.

Although we shall not use it in this paper, here is a third basic principle of computational Galois theory; for a proof see §61 of volume I of van der Waerden's book [V], and for some applications see the 1958 follow-up [A4] of my 1957 paper.

Basic Homomorphism Principle. *If* $f(Y) \in R_v[Y]$ *where* R_v *is the valuation ring of a valuation* v *of* K *and if* $\bar{f}(Y)$ *has no multiple roots in any overfield of* $\overline{K}$, *where* $\overline{K}$ *is the residue field of* v *and* $\bar{f}(Y) \in \overline{K}(Y)$ *is obtained by applying the canonical epimorphism* $R_v \to \overline{K}$ *to the coefficients of* $f(Y)$, *then, as a permutation group, the Galois group* $\mathrm{Gal}(\bar{f}, \overline{K})$ *may be regarded as a subgroup of the Galois group* $\mathrm{Gal}(f, K)$.

To give some concrete examples of valuations, assume that $K = k(x)$ where x is a transcendental over a field k. Then for every nonconstant irreducible

$\phi(x) \in k[x]$ we get a valuation v_ϕ of $k(x)/k$ by taking

$$v_\phi \left(\frac{\pi(x)\phi(x)^l}{\epsilon(x)} \right) = l$$

for any integer l and any nonzero $\pi(x)$ and $\epsilon(x)$ in $k[x]$ which are non-divisible by $\phi(x)$; we may call this the $\phi(x) = 0$ valuation of $k(x)/k$; if $\phi(x) = x - c$ with $c \in k$ then we may also call it the $x = c$ valuation of $k(x)/k$; note that for any other nonconstant irreducible $\phi^*(x) \in k[x]$ we have $v_\phi = v_{\phi^*} \Leftrightarrow \phi$ and ϕ^* are constant multiples of each other. In addition to these valuations, there is exactly one more valuation v_∞ of $k(x)/k$ given by taking

$$v_\infty \left(\frac{\pi(x)}{\epsilon(x)} \right) = \deg \epsilon(x) - \deg \pi(x)$$

for all nonzero $\pi(x)$ and $\epsilon(x)$ in $k[x]$; we may call this the $x = \infty$ valuation of $k(x)/k$.

Let $\lambda > \mu \geq 0$ be integers, and consider the polynomial $\xi(Z)Y^\lambda + \eta(Z)Y^\mu$ in indeterminates Y and Z where $\xi(Z)$ and $\eta(Z)$ are nonzero coprime polynomials in Z with coefficients in k. Let y be an element in an overfield of $K = k(x)$ such that $\xi(x)y^\lambda + \eta(x)y^\mu = 0$. Now, upon letting $\hat{v}_1, \ldots, \hat{v}_h$ be the extensions of $v = v_\phi$ to $\hat{K} = K(y)$, for $1 \leq j \leq h$ we have

$$\bar{r}(\hat{v}_j : v) v(\xi(x)\eta(x)) = \left| \bar{r}(\hat{v}_j : v) v \left(\frac{-\eta(x)}{\xi(x)} \right) \right| = |\hat{v}_j(y^{\lambda-\mu})| = (\lambda - \mu)|\hat{v}_j(y)|$$

and hence

$$\bar{r}(\hat{v}_j : v) \equiv 0 \left(\frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, v(\xi(x)\eta(x)))} \right)$$

and therefore by (†) we get

(††) $$[\hat{K} : K] \equiv 0 \left(\frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, v(\xi(x)\eta(x)))} \right).$$

From this we deduce the following

First Irreducibility Lemma. *Let $\lambda > \mu \geq 0$ be integers, and consider the polynomial $\xi(Z)Y^\lambda + \eta(Z)Y^\mu$ in indeterminates Y and Z where $\xi(Z)$ and $\eta(Z)$ are nonzero coprime polynomials in Z with coefficients in a field k. Let y be an element in an overfield of $k(Z)$ such that $\xi(Z)y^\lambda + \eta(Z)y^\mu = 0$. Assume that there exists a finite number of nonconstant irreducible polynomials $\phi_1(Z), \ldots, \phi_m(Z)$ in Z with coefficients in k such that, upon letting ν_i be the largest integer for which $\phi_i(Z)^{\nu_i}$ divides $\xi(Z)\eta(Z)$ in $k[Z]$, we have $\text{GCD}(\lambda - \mu, \nu_1, \ldots, \nu_m) = 1$. Then $[k(y, Z) : k(Z)] = \lambda - \mu$, and the polynomial $\xi(Z)Y^\lambda + \eta(Z)Y^\mu$ is irreducible in $k(Y)[Z]$.*[50]

Namely, by (††) we see that

$$[k(y, Z) : k(Z)] \equiv 0 \left(\frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, \nu_i)} \right) \quad \text{for } 1 \leq i \leq m$$

---

[50]That is, $\xi(Z)Y^\lambda + \eta(Z)Y^\mu$ is either a nonzero element of $k(y)$ or a nonconstant irreducible polynomial in Z with coefficients in $k(y)$.

and clearly

$$\frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, \nu_1, \ldots, \nu_m)} = \text{LCM}\left(\frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, \nu_1)}, \ldots, \frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, \nu_m)}\right)$$

and hence

$$[k(y, Z) : k(Z)] \equiv 0\left(\frac{\lambda - \mu}{\text{GCD}(\lambda - \mu, \nu_1, \ldots, \nu_m)}\right).$$

Since $\text{GCD}(\lambda - \mu, \nu_1, \ldots, \nu_m) = 1$, we get

$$[k(y, Z) : k(Z)] \equiv 0(\lambda - \mu)$$

and since $y^{\lambda - \mu} = -\eta(Z)/\xi(Z)$, we conclude that

$$[k(y, Z) : k(Z)] = \lambda - \mu$$

and the polynomial $Y^{\lambda - \mu} + \eta(Z)/\xi(Z)$ is irreducible in $k(Z)[Y]$. Therefore by the Gauss Lemma,[51] the polynomial $\xi(Z)Y^{\lambda - \mu} + \eta(Z)$ is irreducible in $k[Y, Z]$, and hence again by the Gauss Lemma, the polynomial $\xi(Z)Y^{\lambda - \mu} + \eta(Z)$ is irreducible in $k(Y)[Z]$, and therefore the polynomial $\xi(Z)Y^\lambda + \eta(Z)Y^\mu$ is irreducible in $k(Y)[Z]$.

Let us now convert the above lemma into the following

Second Irreducibility Lemma. *Let $\lambda > \mu \geq 0$, and let $\xi_\lambda(Y, Z)$ and $\eta_\mu(Y, Z)$ be nonzero homogeneous polynomials of respective degrees λ and μ in (Y, Z) with coefficients in a field k. Assume that the polynomials $\xi_\lambda(Y, Z)$ and $\eta_\mu(Y, Z)$ are regular in Z,[52] and the polynomials $\xi_\lambda(1, Z)$ and $\eta_\mu(1, Z)$ have no nonconstant common factor in $k[Z]$. Also assume that there exists a finite number of nonconstant irreducible polynomials $\phi_1(Z), \ldots, \phi_m(Z)$ in Z with coefficients in k such that, upon letting ν_i to be the largest integer for which $\phi_i(Z)^{\nu_i}$ divides $\xi_\lambda(1, Z)\eta_\mu(1, Z)$ in $k[Z]$, we have $\text{GCD}(\lambda - \mu, \nu_1, \ldots, \nu_m) = 1$. Then the polynomial $\xi_\lambda(Y, Z) + \eta_\mu(Y, Z)$ is irreducible in $k(Y)[Z]$.*

To prove this, note that $Z \mapsto YZ$ gives a $k(Y)$-automorphism of $k(Y)[Z]$ which sends the polynomial $\xi_\lambda(Y, Z) + \eta_\mu(Y, Z)$ to the polynomial $\xi_\lambda(1, Z)Y^\lambda + \eta_\mu(1, Z)Y^\mu$. By the First Irreducibility Lemma, the second polynomial is irreducible in $k(Y)[Z]$ and hence so is the first.

As an illustration, let $n > t > 1$ be integers such that $\text{GCD}(n, t) = 1$. Now if u is any element in an algebraic closure $\bar{k}$ of k such that $u^n = 1 = u^t$, then, since $\text{GCD}(n, t) = 1$, we must have $u = 1$; therefore 1 is the only common root of $Z^n - 1$ and $Z^t - 1$ in $\bar{k}$. Again since $\text{GCD}(n, t) = 1$, either n or t is nondivisible by the characteristic of k, and hence either $Z^n - 1$ or $Z^t - 1$ is devoid of multiple roots in $\bar{k}$. Therefore the polynomials $(Z^n - 1)/(Z - 1)$ and $(Z^t - 1)/(Z - 1)$ have no common root in $\bar{k}$ and at least one of them has no multiple root in $\bar{k}$, and hence they have no nonconstant common factor in $k[Z]$ and at least one of them has no nonconstant multiple irreducible factor in $k[Z]$; since $n > t > 1$, we conclude that their product has at least one nonconstant

---

[51] The Gauss Lemma says that a nonzero polynomial in indeterminates Y and Z with coefficients in a field k is irreducible in $k[Y, Z]$ if and only if it is irreducible in $k(Z)[Y]$ and, as a polynomial in Y, its coefficients have no nonconstant common factor in $k[Z]$.

[52] That is, their degrees in Z coincide with their degrees in (Y, Z).

nonmultiple irreducible factor in $k[Z]$.[53] By applying the k-automorphism $Z \mapsto Z + 1$ of $k[Z]$ and by multiplying the second polynomial by $-a$, where a is any nonzero element of k, we see that the polynomials $(Z + 1)^n - 1)/Z$ and $-a[(Z + 1)^t - 1]/Z$ have no nonconstant common factor in $k[Z]$ and their product has at least one nonconstant nonmultiple irreducible factor in $k[Z]$. Consequently by taking $(Z + Y)^n - Y^n/Z$ and $-a[(Z + Y)^t - Y^t]/Z$ for $\xi_\lambda(Y, Z)$ and $\eta_\mu(Y, Z)$, and by letting $\phi_1(Z), \ldots, \phi_m(Z)$ to be the distinct monic nonconstant irreducible factors of $\xi_{\lambda(1,Z)}\eta_\mu(1, Z)$ in $k[Z]$, and by letting ν_i to be the largest integer for which $\phi_i(Z)^{\nu_i}$ divides $\xi_\lambda(1, Z)\eta_\mu(1, Z)$ in $k[Z]$, we see that $\xi_\lambda(Y, Z)$ and $\eta_\mu(Y, Z)$ in $k[Z]$ are nonzero homogeneous polynomials of respective degrees $\lambda = n - 1$ and $\mu = t - 1$ in (Y, Z) with coefficients in k such that the polynomials $\xi_\lambda(1, Z)$ and $\eta_\mu(1, Z)$ have no nonconstant common factor in $k[Z]$, and for some i we have $\nu_i = 1$, and hence trivially we have $\mathrm{GCD}(\lambda - \mu, \nu_1, \ldots, \nu_m) = 1$. Therefore by the Second Irreducibility Lemma we get the following

Third Irreducibility Lemma. *Let $n > t > 1$ be integers such that $\mathrm{GCD}(n, t) = 1$. Let Y and Z be indeterminates over a field k, and let $0 \neq a \in k$. Then the polynomial $((Z + Y)^n - Y^n/Z - a[(Z + Y)^t - Y^t]/Z$ is irreducible in $k(Y)[Z]$.*

20. THE TILDE POLYNOMIAL AND BORROWING CYCLES

Let us now apply the twisted derivative method to the polynomial

$$\widetilde{F}_{n,s} = \widetilde{F}_{n,s}(X, Y) = Y^n - aY^t + X^s$$

with $1 \leq t < n$ and $\mathrm{GCD}(n, t) = 1$, where s is a positive integer, a is a nonzero element in a field k of characteristic p,[54] and X and Y are indeterminates over k. We want to calculate the Galois group $\widetilde{G}_{n,s} = \mathrm{Gal}(\widetilde{F}_{n,s}, k(X))$.[55]

Let $\bar{k}$ be an algebraic closure of k, and let

$$(\mathrm{i}) \qquad d = \frac{n - t}{e} \quad \text{where } e = \begin{cases} 1 & \text{if } p = 0, \\ \max p^\mu \text{ with } n - t \equiv 0(p^\mu) & \text{if } p \neq 0. \end{cases}$$

Now

$$(\mathrm{ii}) \qquad Y^n - aY^t = Y^t \prod_{i=1}^d (Y - \beta_i)^e$$

with pairwise distinct nonzero elements $\beta_1, \ldots, \beta_d$ in $\bar{k}$ and $\mathrm{GCD}(e, t) = 1$, and hence by the First Irreducibility Lemma we see that $\widetilde{F}_{n,s}$ is irreducible in $\bar{k}(X)[Y]$, and therefore $\widetilde{F}_{n,s}$ *is irreducible in* $k(X)[Y]$.[56]

Let us put $x = X$ and let y be a root of $\widetilde{F}_{n,s}$ in an overfield of $k(x)$. Then

$$(\mathrm{iii}) \qquad x^s = ay^t - y^n$$

---

[53]That is, there exists a nonconstant irreducible member of $k[Z]$ which divides the said product but whose square does not divide the said product.

[54]Here p may or may not be zero. Later on we shall specialize to the case of $p \neq 0$; with the further assumption that $n \equiv 0(p)$ and $s \equiv 0(t)$, the polynomial $\widetilde{F}_{n,s}$ reduces to the polynomial $\widetilde{F}_n$ considered in §11.

[55]In a moment we shall show that $\widetilde{F}_{n,s}$ has no multiple roots in any overfield of $k(X)$, and hence the Galois group $\mathrm{Gal}(\widetilde{F}_{n,s}, k(X))$ is defined.

[56]For $s = 1$ this also follows by noting that $\widetilde{F}_{n,1}$ is monic of degree 1 in X.

and hence y is transcendental over k. Let $E(y, Z)$ be the polynomial in an indeterminate Z such that $E(y, Y)$ is the twisted Y-derivative of $\widetilde{F}_{n,s}(x, Y)$ at y. Then

$$E(y, Z) = \frac{(Z + y)^n - y^n}{Z} - \frac{a[(Z + y)^t - y^t]}{Z}$$

and hence by the Third Irreducibility Lemma we see that $E(y, Z)$ *is irreducible in* $k(y)[Z]$.

For a moment suppose that $s = 1 < t$; then by (iii) we have $x \in k(y)$, and hence $E(y, Z)$ is irreducible in $k(x, y)[Z]$, and therefore by the Twisted Derivative Criterion we see that $\widetilde{F}_{n,1}(X, Y)$ has no multiple roots in any over-field of $k(X)$, and so $\mathrm{Gal}(\widetilde{F}_{n,1}, k(X))$ is defined; since $E(y, Z)$ is irreducible in $k(x, y)[Z]$, it also follows that $\mathrm{Gal}(\widetilde{F}_{n,1}, k(X))$ is 2-transitive. Thus, *if* $s = 1 < t$ *then* $\widetilde{F}_{n,1}$ *is devoid of multiple roots and* $\widetilde{G}_{n,1}$ *is 2-transitive.*

Reverting to general s but still assuming $t > 1$, since $\widetilde{F}_{n,s}(X, Y) = \widetilde{F}_{n,1}(X^s, Y)$ and $\widetilde{F}_{n,1}(X, Y)$ has no multiple roots in any overfield of $k(X)$, it follows that $\widetilde{F}_{n,s}(X, Y)$ has no multiple roots in any overfield of $k(X)$. Thus, *if* $t > 1$ *then* $\widetilde{F}_{n,s}$ *is devoid of multiple roots and hence* $\widetilde{G}_{n,s}$ *is defined.*

To give a direct proof of $\widetilde{F}_{n,s}$ being devoid of multiple roots, let us calculate its Y-discriminant.

So first recall that the Y-discriminant of a monic polynomial $f = f(Y)$ of degree $n > 0$ in Y with coefficients in a field K is denoted by $\mathrm{Disc}_Y(f)$ and is defined by putting

$$\mathrm{Disc}_Y(f) = \mathrm{Res}_Y(f, f_Y) = \text{the } Y\text{-resultant of } f \text{ and } f_Y,$$

where f_Y is the (ordinary) Y-derivative of f. Upon letting m be the degree of f_Y, we note that $\mathrm{Res}_Y(f, f_Y)$ is the determinant of a certain $n + m$ by $n + m$ matrix; also note that $m = n - 1 \Leftrightarrow n \not\equiv 0(\mathrm{char}\, K)$; finally note that if $f_Y = 0$, i.e., if $\mathrm{char}\, K = p \neq 0$ and $f \in K[Y^p]$, then we take $\mathrm{Disc}_Y(f) = 0$. For calculational purposes, upon letting $f = \prod_{i=1}(Y - \alpha_i)$ we observe that

$$\mathrm{Disc}_Y(f) = \prod_{i=1}^{n} f_Y(\alpha_i)$$

and upon assuming $f_Y \neq 0$ and upon letting $f_Y = \epsilon \prod_{i=1}^{m}(Y - \epsilon_i)$ we observe that

$$\mathrm{Disc}_Y(f) = (-1)^{nm} \epsilon^n \prod_{i=1}^{m} f(\epsilon_i).$$

Finally, upon letting

$$\mathrm{Disc}_Y^*(f) = \text{the modified } Y\text{-discriminant of } F = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

we note that[57]

$$\mathrm{Disc}_Y^*(f) = (-1)^{n(n-1)/2}\mathrm{Disc}_Y(f).$$

Let us record the following well-known

---

[57]On pages 82–87 of volume I of van der Waerden's book [V], it seems to be wrongly asserted that $\mathrm{Disc}_Y^*(f) = \mathrm{Disc}_Y(f)$. Some authors call $\mathrm{Disc}_Y^*(f)$ the discriminant of f.

Discriminant Criterion. *If* $\operatorname{char} K \neq 2$ *and* f *is devoid of multiple roots, then:* $\operatorname{Gal}(f, K) \subset A_n \Leftrightarrow \operatorname{Disc}_Y^*(f)$ *is a square in* K.

Now for the (ordinary) Y-derivative of $\widetilde{F}_{n,s}$ we have

$$(\widetilde{F}_{n,s})_Y = nY^{n-1} - taY^{t-1}$$

$$= \begin{cases} -taY^{t-1} \neq 0 & \text{if } n \equiv 0(p), \\ nY^{t-1} \prod_{i=1}^{n-t}(Y - b\omega_i) \neq 0 & \text{if } n \not\equiv 0(p), \end{cases}$$

with $b, \omega_1, \ldots, \omega_{n-t}$ in $\bar{k}$ such that $nb^{n-t} = ta$ and $\prod_{i=1}^{n-t}(Y - \omega_i) = Y^{n-t} - 1$ and hence

$$\operatorname{Disc}_Y(\widetilde{F}_{n,s}) = \begin{cases} (-1)^{n(t-1)}(-ta)^n(X^s)^{t-1} & \text{if } n \equiv 0(p), \\ (-1)^{n(n-1)}n^n(X^s)^{t-1} \prod_{i=1}^{n-t}[X^s - n^{-1}(n-t)ab^t\omega_i^t] & \text{if } n \not\equiv 0(p), \end{cases}$$

and therefore, because $\operatorname{GCD}(n - t, t) = 1$, we get

(iv) $\quad \operatorname{Disc}_Y(\widetilde{F}_{n,s}) = \begin{cases} (-1)^{nt}t^na^nX^{s(t-1)} & \text{if } n \equiv 0(p), \\ X^{s(t-1)}[n^nX^{s(n-t)} - (n-t)^{n-t}t^ta^n] & \text{if } n \not\equiv 0(p), \end{cases}$

and, observing that if $n \equiv 0(p)$ then in k we have $n^n = 0$ and $-(n-t)^{n-t}t^t = (-1)^{n-t+1}t^n = (-1)^{nt}t^n$,[58] we conclude that in both the cases we have

$$\operatorname{Disc}_Y(\widetilde{F}_{n,s}) = n^nX^{s(n-1)} - (n-t)^{n-t}t^ta^nX^{s(t-1)}.$$

Thus always $\operatorname{Disc}_Y(\widetilde{F}_{n,s}) \neq 0$ and hence $\widetilde{F}_{n,s}$ is devoid of multiple roots.

If $s = 1$ and $n - t \not\equiv 0(p)$ then by (i), (ii), (iii) we see that the valuation $x = 0$ of $\bar{k}(x)/\bar{k}$ splits in $\bar{k}(x, y) = \bar{k}(y)$ into the $n - t + 1 = d + 1$ valuations $y = 0, y = \beta_1, \ldots, y = \beta_d$ with reduced ramification exponents $t, 1, \ldots, 1$, and hence if also $t \not\equiv 0(p)$ then by the Cycle Lemma we can find a t-cycle in $\operatorname{Gal}(\widetilde{F}_{n,1}, \bar{k}(X))$, and therefore, since by the Basic Extension Principle we have $\operatorname{Gal}(\widetilde{F}_{n,1}, \bar{k}(X)) < \operatorname{Gal}(\widetilde{F}_{n,1}, k(X))$, we get a t-cycle in $\operatorname{Gal}(\widetilde{F}_{n,1}, k(X))$. Thus, *if* $n - t \not\equiv 0(p)$ *and* $t \not\equiv 0(p)$ *then* $\widetilde{G}_{n,1}$ *contains a* t-*cycle.*

Let us note the following Corollary of an 1871 Theorem of Jordan [J2]; a proof can also be found in 13.3 on page 34 of Wielandt [Wi], and in 4.4 on page 171 of Volume I of Huppert [HB].

Jordan's Corollary. A_n *and* S_n *are the only primitive permutation groups of degree* n *containing a* 3-*cycle.*

Let us also note the following two 1892 Theorems of Marggraff [Mar]; these are given as Theorems 13.5 and 13.8 on pages 35 and 38 of Wielandt [Wi] respectively.[59]

Marggraff's First Theorem. A_n *and* S_n *are the only primitive permutation groups of degree* n *having a* $(n - \nu)$-*point stabilizer, with* $1 < \nu < n/2$, *which acts transitively on the remaining* ν *symbols.*

Marggraff's Second Theorem. *A primitive permutation group of degree* n *containing a* ν-*cycle, with* $1 < \nu < n$, *is* $(n - \nu + 1)$-*transitive.*

---

[58] Note that if n and t are both odd then $n - t + 1$ and nt are both odd, whereas if one out of n and t is odd and the other even then $n - t + 1$ and nt are both even, and finally, since $\operatorname{GCD}(n, t) = 1$, the remaining possibility of n and t both being even cannot occur.

[59] Apparently, Marggraff's Second Theorem can also be found in [J2]; see Neumann [N].

For a moment suppose that $n - t \not\equiv 0(p)$ and $1 < t \not\equiv 0(p)$.[60] Now, in view of what we have proved above, $\widetilde{G}_{n,1}$ is a 2-transitive permutation group containing a t-cycle and hence if $t = 2$ then obviously[61] $\widetilde{G}_{n,1} = S_n$; if $t = 3$ then by Jordan's Corollary[62] we have $\widetilde{G}_{n,1} = A_n$ or S_n ; if $t < \frac{n}{2}$ then by Marggraff's First Theorem we have $\widetilde{G}_{n,1} = A_n$ or S_n ; if $t < n - 4$ then by Marggraff's Second Theorem and CTT we have $\widetilde{G}_{n,1} = A_n$ or S_n ; if $t = n - 4$ then automatically $12 \neq n \neq 24$ and hence by Marggraff's Second Theorem and CTT we have $\widetilde{G}_{n,1} = A_n$ or S_n ; and if $t = n - 3$ then again automatically $12 \neq n \neq 24$ and hence if also $11 \neq n \neq 23$, then by Marggraff's Second Theorem and CTT we have $\widetilde{G}_{n,1} = A_n$ or S_n . In all these cases, if t is even then we must have $\widetilde{G}_{n,1} = S_n$ because A_n cannot have a cycle of even length, and if t is odd and $p \neq 2$ then, in view of the Discriminant Criterion, by (iv) we can unambiguously decide between A_n and S_n ; in particular, if k is algebraically closed and $n \equiv 0(p)$ and $p \neq 2$ and t is odd then we get A_n because in that case $\mathrm{Disc}_Y^*(\widetilde{F}_{n,1})$ is a square in $k(x)$. Again, in all these cases, assuming k to be algebraically closed, in view of Corollaries (3.2) to (3.8) of the Substitutional Principle, we see that (1) t is even $\Rightarrow \widetilde{G}_{n,1} = S_n \Rightarrow \widetilde{G}_{n,s} = A_n$ or S_n ; (2) t is odd and $n = 4 \Rightarrow \widetilde{G}_{n,1} = A_n$ or S_n with $n = 4 \Rightarrow \widetilde{G}_{n,s} = (Z_2)^2$ or A_n or S_n ; (3) t is odd and $n > 4$ and $p = 2 \Rightarrow \widetilde{G}_{n,1} = A_n$ or S_n with $n > 4 \Rightarrow \widetilde{G}_{n,s} = A_n$ or S_n ; (4) t is odd and $n = 4$ and $p \neq 2$ and $\mathrm{Disc}_Y^*(\widetilde{F}_{n,1})$ is a square in $k(x) \Rightarrow \widetilde{G}_{n,1} = A_n$ with $n = 4 \Rightarrow \widetilde{G}_{n,s} = (Z_2)^2$ or A_n ; (5) t is odd and $n > 4$ and $p \neq 2$ and $\mathrm{Disc}_Y^*(\widetilde{F}_{n,1})$ is a square in $k(x) \Rightarrow \widetilde{G}_{n,1} = A_n$ with $n > 4 \Rightarrow \widetilde{G}_{n,s} = A_n$; and finally (6) t is odd and $p \neq 2$ and $\mathrm{Disc}_Y^*(\widetilde{F}_{n,1})$ is not a square in $k(x) \Rightarrow \widetilde{G}_{n,1} = S_n \Rightarrow \widetilde{G}_{n,s} = A_n$ or S_n .

Now for a moment suppose that $n \equiv 0(p)$. Then $t \not\equiv 0(p)$ and hence by (iv) we see that $x = 0$ and $x = \infty$ are the only valuations of $k(x)/k$ which are possibly ramified in $k(x, y)$. Moreover, if $s \equiv 0(t)$ then, in view of (i), (ii), (iii), either by direct reasoning we see that the valuation $x = 0$ of $k(x)/k$ is unramified in $k(x, y)$, or alternatively, first, upon letting $x^* = x^s$ we see that the valuation $x^* = 0$ of $k(x^*)/k$ splits in $k(x^*, y) = k(y)$ into several valuations out of which $y = 0$ is the only valuation which is possibly ramified over $k(x^*)$ and for it the reduced ramification index is t and the residue degree is 1 , and now upon letting

$$ x' = \begin{cases} x & \text{if } p = 0, \\ x^{s'} \text{ where } s' = \max p^\lambda \text{ with } s \equiv 0(p^\lambda) & \text{if } p \neq 0, \end{cases} $$

we see that $x'^{s/s'} = x^*$ and s/s' is a positive integer which is divisible by t but not divisible by p and hence by MRT[63] we see that the valuation $x' = 0$ of $k(x')$ is unramified in $k(x', y)$, and finally from this we deduce that the valuation $x = 0$ of $k(x)/k$ is unramified in $k(x, y)$.[64]

---

[60]Note that if $n \equiv 0(p)$ then automatically $n - t \not\equiv 0(p)$ and $t \not\equiv 0(p)$ because by assumption $\mathrm{GCD}(n, t) = 1$.

[61]A 2-cycle is simply a transposition, and a 2-transitive permutation group containing a transposition must contain all transpositions and hence must be the symmetric group.

[62]A 2-transitive permutation group is automatically primitive.

[63]MRT=Abhyankar's Lemma = pages 181–186 of [A5].

[64]This last deduction follows from the easy to prove fact which says that if a valuation v of a

Thus, if $n \equiv 0(p)$ and $s \equiv 0(t)$, then $x = \infty$ is the only valuation of $k(x)/k$ which is possibly ramified in $k(x, y)$, and hence[65] $x = \infty$ is the only valuation of $k(x)/k$ which is possibly ramified in a least Galois extension of $k(x)$ containing $k(x, y)$. It only remains to note that, by Result 4 on page 841 of the 1957 paper [A3], as a consequence of the genus formula, every member of the algebraic fundamental group of the affine line over an algebraically closed field k of characteristic $p \neq 0$ is a quasi p-group; therefore in our case, if $\widetilde{G}_{n,s} = A_n$ or S_n and $p \neq 2$ then we must have $\widetilde{G}_{n,s} = A_n$, because clearly S_n is not a quasi p-group for any $n \geq p > 2$; likewise, if $\widetilde{G}_{n,s} = (Z_2)^2$ or A_n or S_n with $n = 4$ and $p = 2$, then we must have $\widetilde{G}_{n,s} = (Z_2)^2$ or S_n because A_4 is not a quasi 2-group.

Let us put all this together in the following

Summary about the tilde polynomial. Let k be an algebraically closed field k of characteristic $p \neq 0$, and consider the polynomial $\widetilde{F}_n = Y^n - aY^t + X^s$ in indeterminates X and Y over k, where a is a nonzero element of k, and n, s, t are positive integers with $\mathrm{GCD}(n, t) = 1$ and $t < n \equiv 0(p)$ and $s \equiv 0(t)$. Then $\widetilde{F}_n$ gives an unramified covering of the affine line over k, and for the Galois group $\widetilde{G}_n = \mathrm{Gal}(\widetilde{F}_n, k(X))$ we have the following.

(II.1) If $1 < t < 4$ and $p \neq 2$, then $\widetilde{G}_n = A_n$.

(II.2) If $1 < t < n - 3$ and $p \neq 2$, then $\widetilde{G}_n = A_n$.

(II.3) If $1 < t = n - 3$ and $p \neq 2$ and $11 \neq p \neq 23$, then $\widetilde{G}_n = A_n$.

(II.4) If $1 < t < 4 < n$ and $p = 2$, then $\widetilde{G}_n = A_n$ or S_n.

(II.5) If $1 < t < n - 3$ and $p = 2$, then $\widetilde{G}_n = A_n$ or S_n.

Here CT was not used in the proofs of (II.1) and (II.4). Moreover,[66] the following special cases of (II.2) and (II.5) were proved without using CT.

(II.2*) If $1 < t < n/2$ and $p \neq 2$, then $\widetilde{G}_n = A_n$.

(II.5*) If $1 < t < n/2$ and $p = 2$, then $\widetilde{G}_n = A_n$ or S_n.

Note. In the next section we shall consider the unramified covering of the affine line given by the polynomial $\overline{F}_n = Y^n - XY^t + 1$ with $n = p + t$ and $t \not\equiv 0(p)$ which was introduced in §11; there the calculation of the Galois group of $\overline{F}_n$ will be based on the fact that it contains a p-cycle because the valuation $X = \infty$ splits into the valuations $Y = 0$ and $Y = \infty$ with reduced ramification exponents t and p respectively.[67] In the present section we considered the unramified covering of the affine line given by the polynomial $\widetilde{F}_n = Y^n - aY^t + X^s$ with $n \equiv 0(p)$ and $\mathrm{GCD}(n, t) = 1$ and $s \equiv 0(t)$ which was also introduced in §11; contrary to the Galois group of the polynomial $\overline{F}_n$, it is not easy to find any cycle in the Galois group of the polynomial $\widetilde{F}_n$ because now the valuation

---

field K is unramified in a finite separable algebraic field extension L of K then the unique extension of v to a finite purely inseparable field extension K' of K is unramified in the compositum of L and K'.

[65]Say by Proposition 1 of [A1].

[66]In view of the above discussion, without using CT we see that if $1 < t < 4 = n$ and $p = 2$, then $\widetilde{G}_n = (Z_2)^2$ or S_n, and using CT we see that if $1 < t = n - 3$ and $\widetilde{G}_n \neq A_n$, then either $n = p = 11$ and $\widetilde{G}_n = M_{11}$, or $n = p = 23$ and $\widetilde{G}_n = M_{23}$.

[67]Actually, by reciprocating the roots of $\overline{F}_n$ we shall get the polynomial $Y^n - XY^p + 1$ for which the valuation $X = \infty$ splits into the valuations $Y = 0$ and $Y = \infty$ with reduced ramification exponents p and t respectively.

$X = \infty$ has the valuation $Y = \infty$ as the only extension and for it the reduced ramification exponent is n which is a multiple of p; so what we did was to "borrow" a t-cycle by going down to the subfield $k(X^s)$ of $k(X)$, i.e., by embedding the Galois group over $k(X)$ as a subgroup of the Galois group over $k(X^s)$ where the latter does contain a t-cycle. This method of borrowing cycles can already be found in Hilbert's 1892 paper [H] where he "borrows" a transposition to embed A_n in S_n, thereby constructing A_n coverings of the rational number field $\mathbb{Q}$.

21. The bar polynomial

Let us now turn to the polynomial

$$\overline{F}_{n,q} = Y^n - XY^t + 1$$

with $n = q + t$ and positive integer $t \not\equiv 0(p)$ mentioned in §11. This is a polynomial in indeterminates X and Y with coefficients in a field k of characteristic $p \neq 0$, and q is a positive power of p.

The (ordinary) Y-derivative of $\overline{F}_{n,q}$ is given by

$$(\overline{F}_{n,q})_Y = n(Y^{n-1} - XY^{t-1})$$

and so we get

$$\overline{F}_{n,q} = \frac{Y}{n}(\overline{F}_{n,q})_Y + 1$$

and hence for the Y-discriminant of $\overline{F}_{n,q}$ we have

$$\mathrm{Disc}_Y(\overline{F}_{n,q}) = n^n = \text{ a nonzero element of } k.$$

Therefore this gives an unramified covering of the affine line over k. At any rate, $\overline{F}_{n,q}$, as a polynomial in Y, is devoid of multiple roots, and so we can talk about its Galois group over $k(X)$. We are interested in calculating this Galois group $\overline{G}_{n,q} = \mathrm{Gal}(\overline{F}_{n,q}, k(X))$.

Now $\overline{F}_{n,q}$, as a polynomial in X, is linear and in it the coefficient of X has no common factor with the terms devoid of X. Therefore $\overline{F}_{n,q}$ is irreducible in $k[Y][X]$ and hence in $k(X)[Y]$. Consequently, $\overline{G}_{n,q}$, *as a permutation group of degree n, is transitive.*

Regarding $\overline{F}_{n,q}$ as a polynomial in Y and reciprocating its roots we get the polynomial

$$\Theta = \Theta(Y) = Y^{q+t} - xY^q + 1,$$

where we have put $x = X$. Let y be a root of this polynomial in some overfield of $k(x)$. Then solving $\Theta(y) = 0$ for x we get the equation $x = y^t + y^{-q}$. The $q = p$ case of this equation was really the starting point of this paper and it was originally obtained by taking $h = c_1 = 1$ in Proposition 1 of the 1957 paper [A3]. The case of general q can also be obtained by taking $h = q/p$ and $c_{q/p} = 1$ and $c_i = 0$ for $1 \le i < q/p$ in that Proposition. By the said Proposition, or directly by looking at the above equation, we see that (1) the simple transcendental extension $k(y)$ of k is a separable algebraic field extension of the simple transcendental extension $k(x)$ of k with field degree $[k(y) : k(x)] = q + t$; (2) $v_\infty : x = \infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$; (3) v_∞ splits in $k(y)$ into the valuations $w_0 : y = 0$ and $w_\infty : y = \infty$; and (4) for the residue degrees and reduced ramification exponents

we have $\bar{d}(w_0 : v_\infty) = 1$ and $\bar{r}(w_0 : v_\infty) = q$, and $\bar{d}(w_\infty : v_\infty) = 1$ and $\bar{r}(w_\infty : v_\infty) = t$. Now $\overline{G}_{n,q} = \mathrm{Gal}(\overline{F}_{n,q}, k(X)) = \mathrm{Gal}(\Theta, k(x))$, and hence in view of (3) and (4), by the Cycle Lemma we see that if k is algebraically closed and $q = p$ then $\overline{G}_{n,p}$ contains a p-cycle; by the Basic Extension Principle, as a permutation group, $\mathrm{Gal}(\overline{F}_{n,q}, \bar{k}(X))$ is a subgroup of $\mathrm{Gal}(\overline{F}_{n,q}, k(X))$ where $\bar{k}$ is an algebraic closure of k; therefore, without assuming k to be algebraically closed, we have that *if $q = p$ then $\overline{G}_{n,p}$ contains a p-cycle*.

Let prime denote the twisted Y-derivative at y. Then

$$\begin{aligned}
\Theta'(Y) &= [Y^q(Y^t - x)]' + (1)' \quad \text{(by linearity)} \\
&= [Y^q(Y^t - x)]' \quad \text{(because constant}' = 0) \\
&= (Y + y)^q(Y^t - x)' + Y^{q-1}(y^t - x) \quad \text{(by power product rule)} \\
&= (Y + y)^q(Y^t)' + Y^{q-1}(y^t - x) \quad \text{(because constant}' = 0) \\
&= (Y + y)^q(Y^t)' - y^{-q}Y^{q-1} \quad \text{(because } x = y^t + y^{-q})
\end{aligned}$$

and hence by the definition of $(Y^t)'$ we get

$$\Theta'(Y) = [(Y + y)^q]\frac{(Y + y)^t - y^t}{Y} - y^{-q}Y^{q-1}$$

and therefore

$$\Theta'(0) = ty^{q+t-1} \neq 0.$$

Let $\Delta(Y)$ be the polynomial obtained by reciprocating the roots of $\Theta'(Y)$. Then $\Delta(Y)$ is a monic polynomial of degree $q + t - 1$ in Y with coefficients in $k(y)$ and we have

$$\begin{aligned}
\Delta(Y) &= \left(\frac{Y^{q+t-1}}{ty^{q+t-1}}\right)\Theta'\left(\frac{1}{Y}\right) \\
&= \left[\left(\frac{Y^q}{y^q}\right)\left(\frac{1}{Y} + y\right)^q\right]\frac{\left(\frac{Y^t}{y^t}\right)\left[\left(\frac{1}{Y} + y\right)^t - y^t\right]}{\left(\frac{tY}{y}\right)\left(\frac{1}{Y}\right)} - \left(\frac{Y^{q+t-1}}{ty^{q+t-1}}\right)\left(\frac{y^{-q}}{Y^{q-1}}\right) \\
&= [(Y + y^{-1})^q]\frac{y[(Y + y^{-1})^t - Y^t]}{t} - \frac{Y^t}{ty^{2q+t-1}}.
\end{aligned}$$

Let $\Lambda(Z)$ be the polynomial obtained by multiplying the roots of $\Delta(Z)$ by ty. Then $\Lambda(Z)$ is a monic polynomial of degree $q + t - 1$ in an indeterminate Z with coefficients in $k(y)$ and we have

$$\begin{aligned}
\Lambda(Z) &= (ty)^{q+t-1}\Delta\left(\frac{Z}{ty}\right) \\
&= \left[(ty)^q\left(\frac{Z}{ty} + \frac{1}{y}\right)^q\right]\frac{(ty)^{t-1}y\left[\left(\frac{Z}{ty} + \frac{1}{y}\right)^t - \left(\frac{Z}{ty}\right)^t\right]}{t} - \frac{(ty)^{q+t-1}\left(\frac{Z}{ty}\right)^t}{ty^{2q+t-1}} \\
&= [(Z + t)^q]\frac{(Z + t)^t - Z^t}{t^2} - \frac{t^{q-2}Z^t}{y^{q+t}}
\end{aligned}$$

and hence

$$\Lambda(Z) = (Z + t)^q\gamma(Z) - t^{q-2}y^{-q-t}Z^t,$$

where $\gamma(Z)$ is the monic polynomial of degree $t-1$ in Z with coefficients in the prime field $k_p \subset k$ given by

$$\gamma(Z) = t^{-2}[(Z+t)^t - Z^t] = \sum_{i=0}^{t-1} \gamma_i Z^{t-1-i},$$

where $\gamma_i = t^{i-1}\binom{t}{i+1} \in k_p$ with $\gamma_0 = 1$. Now $\gamma(0) = t^{t-2}$ and $\gamma(-t) = (-1)^{t+1}t^{t-2}$ and hence $\gamma(0) \neq 0 \neq \gamma(-t)$.

Let z be a root of $\Lambda(Z)$ in some overfield of $k(y)$. Then solving $\Lambda(z) = 0$ for y we get

$$(*) \qquad\qquad y^{q+t} = \frac{t^{q-2}z^t}{(z+t)^q \gamma(z)}$$

and so in particular we see that z is transcendental over k. Consider the valuation $\kappa : z = 0$ of $k(z)/k$ and let ζ be an extension of it to $k(y, z)$. Since $t \neq 0 \neq \gamma(0)$, by the above equation we see that

$$(q+t)\zeta(y) = \zeta(y^{q+t}) = \zeta\left(\frac{t^{q-2}z^t}{(z+t)^q \gamma(z)}\right) = \bar{r}(\zeta : \kappa)\kappa\left(\frac{t^{q-2}z^t}{(z+t)^q \gamma(z)}\right) = \bar{r}(\zeta : \kappa)t.$$

Since $q + t$ and t are coprime, we must have $\bar{r}(\zeta : \kappa) \geq q + t$. Therefore $[k(y, z) : k(z)] \geq q + t$ and hence by the above equation for y^{q+t} we get $[k(y, z) : k(z)] = q + t$.

Since $[k(y, z) : k(z)] = q + t$, by the above equation for y^{q+t} we see that the polynomial $(z+t)^q \gamma(z)Y^{q+t} - t^{q-2}z^t$ is irreducible in $k(z)[Y]$. Since the nonzero polynomials $(Z+t)^q \gamma(Z)$ and $t^{q-2}Z^t$ in Z with coefficients in k have no nonconstant common factor in $k[Z]$, we conclude that the polynomial

$$(Z+t)^q \gamma(Z)Y^{q+t} - t^{q-2}Z^t$$

is irreducible in $k[Y, Z]$. Consequently the polynomial $(Z+t)^q \gamma(Z)y^{q+t} - t^{q-2}Z^t$ is irreducible in $k(y)[Z]$, and hence *the polynomial $\Lambda(Z)$ is irreducible in $k(y)[Z]$*.[68] Therefore *the polynomials $\Lambda(Y)$ and $\Delta(Y)$ are irreducible in $k(y)[Y]$, and hence* $\mathrm{Gal}(\Lambda, k(y)) = \mathrm{Gal}(\Delta, k(y)) = $ *a transitive permutation group of degree $n - 1$*. Since this group is the one-point stabilizer of $\overline{G}_{n,q} = \mathrm{Gal}(\overline{F}_{n,q}, k(x))$, we conclude that: $\overline{G}_{n,q}$ *is 2-transitive*.

As we have noted above, if $q = p$ then $\overline{G}_{n,p}$ contains a p-cycle, and hence by a 1873 Theorem of Jordan we see that if also $t > 2$, then $\overline{G}_{n,p} = A_n$ or S_n. In Result 4 on page 841 of the 1957 paper [A3] we have noted that, as a consequence of the genus formula, every member of the algebraic fundamental group of the affine line over an algebraically closed ground field of characteristic $p \neq 0$ is a quasi p-group. Also obviously, for $n > 1$ and $p \neq 2$, the symmetric group S_n is not a quasi p-group. Therefore *if k is algebraically closed and $q = p \neq 2$ and $n = p + t$ with $t \not\equiv 0(p)$ and $t > 2$, then $\overline{G}_{n,p} = $ the alternating group A_n*.

Here is the 1873 Theorem of Jordan [J3] we spoke of; proofs can also be found in 13.9 on page 39 of Wielandt [Wi] and in 3.7 on page 331 of volume III of Huppert-Blackburn [HB].

---

[68]This also follows from the First Irreducibility Lemma. In fact, the above argument is a special case of the argument used in the proof of the said lemma.

Jordan's Theorem. *If a primitive permutation group G of degree $n = p + t$ contains a p-cycle, where p is prime and $t > 2$, then $G = A_n$ or S_n.*[69]

In the case $p = 2$, a p-cycle is simply a transposition, and obviously S_n is the only 2-transitive permutation group of degree n which contains a transposition.[70] Therefore *if $q = p = 2$ and $n = p + t$ with $t \not\equiv 0(p)$ and $t > 0$, then $\overline{G}_{n,p} =$ the symmetric group S_n.*

To throw away a second root of $\overline{F}_{n,q}$, or more precisely to throw away a root of $\Lambda(Z)$, this time around let prime denote the twisted Z-derivative at z. Then

$$\Lambda'(Z) = [(Z+t)^q \gamma(Z)]' - t^{q-2} y^{-q-t} [Z^t]' \quad \text{(by linearity)}$$
$$= (Z+z+t)^q \gamma'(Z) + Z^{q-1} \gamma(z) - t^{q-2} y^{-q-t}[Z^t]' \quad \text{(by power product rule)}$$
$$= (Z+z+t)^q \gamma'(Z) + Z^{q-1} \gamma(z) - \gamma(z)(z+t)^q z^{-t}[Z^t]' \quad \text{(by (*))}$$
$$= (Z+z+t)^q \bar{\gamma}(Z) + \gamma(z) Z^{q-1} - \gamma(z)(z+t)^q z^{-t} \bar{p}_{t-1}(Z),$$

where $\bar{p}_j(Z)$ is the monic polynomial of degree $j \geq 0$ in Z with coefficients in the prime field $k_p \subset k$ given by

$$\bar{p}_j(Z) = \frac{(Z+z)^{j+1} - z^{j+1}}{Z}$$

and

$$\bar{\gamma}(Z) = \sum_{j=0}^{t-2} \gamma_{t-2-j} \bar{p}_j(Z).$$

Let $\Phi(W)$ be the monic polynomial of degree $q + t - 2$ in an indeterminate W with coefficients in $k(z)$ obtained by multiplying the roots of $\Lambda'(W)$ by z. Then

$$\Phi(W) = z^{q+t-2} \Lambda'\left(\frac{W}{z}\right)$$
$$= \left[z^q \left(\frac{W}{z} + z + t\right)^q\right]\left[z^{t-2} \bar{\gamma}\left(\frac{W}{z}\right)\right] + \gamma(z) z^{t-1}\left[z^{q-1}\left(\frac{W}{z}\right)^{q-1}\right]$$
$$- \gamma(z)(z+t)^q z^{q-t-1}\left[z^{t-1} \bar{p}_{t-1}\left(\frac{W}{z}\right)\right]$$

and hence

$$\Phi(W) = (W + z^2 + tz)^q \hat{\gamma}(W) + \gamma(z) z^{t-1} W^{q-1} - \gamma(z)(z+t)^q z^{q-t-1} \hat{p}_{t-1}(W)$$

where $\hat{p}_j(W)$ is the monic polynomial of degree $j \geq 0$ in W with coefficients in $k[z]$ given by

$$\hat{p}_j(W) = \frac{(W+z^2)^{j+1} - z^{2j+2}}{W}$$

and

$$\hat{\gamma}(W) = \sum_{j=0}^{t-2} z^{t-2-j} \gamma_{t-2-j} \hat{p}_j(W).$$

---

[69] A 2-transitive permutation group is automatically primitive.

[70] A 2-transitive permutation group which contains a transposition, must automatically contain all transpositions, and hence must be the symmetric group.

Note that if $t = 1$ then $\hat{\gamma}(W) = 0$,[71] whereas if $t > 1$ then $\hat{\gamma}(W)$ is a monic polynomial of degree $t - 2$ in W with coefficients in $k[z]$, and hence, in particular, if $t = 2$ then $\hat{\gamma}(W) = 1$.

For a moment suppose that $t = 1$; then $\gamma(Z)$ is a monic polynomial of degree $t - 1 = 0$ in Z and hence $\gamma(Z) = 1$ and therefore $\gamma(z) = 1$; also as noted above $\hat{\gamma}(W) = 0$; finally $\hat{\rho}_{t-1}(W)$ is a monic polynomial of degree $t - 1 = 0$ in W and hence $\hat{\rho}_{t-1}(W) = 1$. Thus,

$$(1^*) \qquad t = 1 \Rightarrow \begin{cases} \Lambda(Z) = (Z + 1)^q - y^{-q-1}Z \quad \text{and} \\ \Phi(W) = W^{q-1} - (z+1)^q z^{q-2}. \end{cases}$$

Next, for a moment suppose that $t = 2$; then

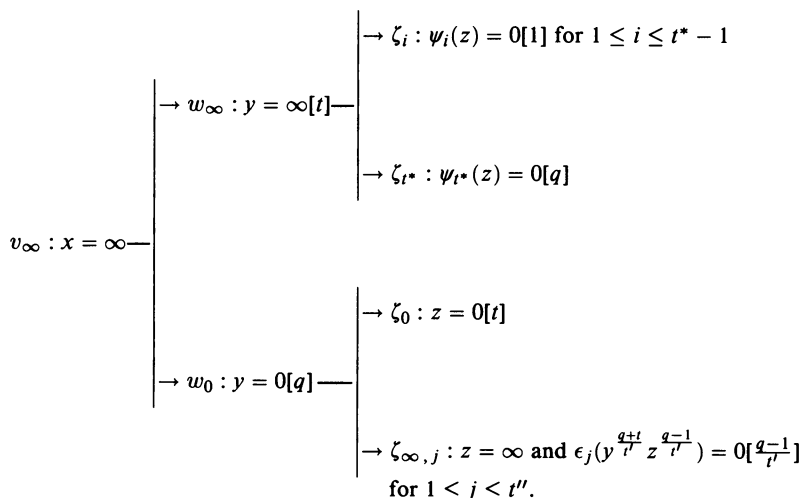$$\gamma(Z) = 2^{-2}[(Z + 2)^2 - Z^2] = Z + 1$$

and hence $\gamma(z) = z + 1$; also as noted above $\hat{\gamma}(W) = 1$ and clearly $(W + z^2 + tz)^q = W^q + (z + 2)^q z^q$; finally $\hat{\rho}_{t-1}(W)$ is the monic polynomial of degree 1 in W given by $\hat{\rho}_{t-1}(W) = W + 2z^2$ and hence

$$\begin{aligned} \Phi(0) &= (z + 2)^q z^q - (z + 1)(z + 2)^q z^{q-3}(2z^2) \\ &= (z + 2)^q z^{q-1}(z - 2z - 2) = -(z + 2)^{q+1} z^{q-1}. \end{aligned}$$

Thus,

$$(2^*) \qquad t = 2 \Rightarrow \begin{cases} \Lambda(Z) = (Z + 2)^q(Z + 1) - 2^{q-2}y^{-q-2}Z^2 \quad \text{and} \\ \Phi(W) = W^q + (z + 1)zW^{q-1} - (z + 1)(z + 2)^q z^{q-3}W \\ \qquad - (z + 2)^{q+1} z^{q-1}. \end{cases}$$

In the case of general t, by looking at the equation $(*)$, we get the following "ramification diagram" for the field extensions $k(x) \subset k(y) \subset k(y, z)$, where the square bracketed numbers are the reduced ramification exponents.

$$
\begin{array}{l}
v_\infty : x = \infty
\end{array}
\quad
\begin{array}{l}
\to w_\infty : y = \infty[t] \longmapsto
\begin{cases}
\to \zeta_i : \psi_i(z) = 0[1] \text{ for } 1 \le i \le t^* - 1 \\[1em]
\to \zeta_{t^*} : \psi_{t^*}(z) = 0[q]
\end{cases} \\[3em]
\to w_0 : y = 0[q] \longmapsto
\begin{cases}
\to \zeta_0 : z = 0[t] \\[1em]
\to \zeta_{\infty,j} : z = \infty \text{ and } \epsilon_j(y^{\frac{q+t}{t^t}} z^{\frac{q-1}{t^t}}) = 0[\frac{q-1}{t^t}] \\
\qquad \text{for } 1 \le j \le t''.
\end{cases}
\end{array}
$$

To explain the top half of the extreme right hand side in the above diagram, first note that, since $t \not\equiv 0(p)$, the Z-discriminant of $(Z + t^{-1})^t - t^{-t} \in k[Z]$

---

[71]Because in that case the summation in the above expression for $\hat{\gamma}(W)$ is empty.

is a nonzero constant; now 0 is a root of this monic polynomial and by reciprocating the roots of $((Z + t^{-1})^t - t^{-t}/Z$ we get $\gamma(Z)$; therefore $\gamma(Z)$ is free from multiple factors; since $\gamma(-t) \neq 0$, we conclude that $\gamma(Z) = \psi_1(Z)\psi_2(Z)\cdots\psi_{t^*-1}(Z)$, where, upon letting $\psi_{t^*}(Z) = Z + t$, we have that $\psi_1(Z), \psi_2(Z), \ldots, \psi_{t^*}(Z)$ are pairwise distinct nonconstant monic irreducible polynomials in Z with coefficients in k; let κ_i be the valuation of $k(z)/k$ given by $\psi_i(z)$; since $\mathrm{GCD}(q + t, q) = 1$, by $(*)$ we see that κ_i has a unique extension ζ_i to $k(y, z)$, and $\zeta_1, \zeta_2, \ldots, \zeta_{t^*}$ are exactly all the extensions of w_∞ to $k(y, z)$, and we have $\bar{r}(\zeta_i : \kappa_i) = q + t$ for $1 \leq i \leq t^*$, $\bar{r}(\zeta_i : w_\infty) = 1$ for $1 \leq i \leq t^* - 1$, and $\bar{r}(\zeta_{t^*} : w_\infty) = q$.

Turning to the bottom half, since $\mathrm{GCD}(q + t, t) = 1$, by $(*)$ we see that the valuation $\kappa_0 : z = 0$ of $k(z)/k$ has a unique extension ζ_0 to $k(y, z)$; since $t \not\equiv 0(p)$, upon letting $t' = \mathrm{GCD}(q + t, q - 1)$ we have $Z^{t'} - t^{q-2} = \epsilon_1(Z)\epsilon_2(Z)\ldots\epsilon_{t''}(Z)$, where $\epsilon_1(Z), \epsilon_2(Z), \ldots, \epsilon_{t''}(Z)$ are pairwise distinct nonconstant monic irreducible polynomials in Z with coefficients in k; now by $(*)$ we see that the valuation $\kappa_\infty : z = \infty$ of $k(z)/k$ has t'' extensions $\zeta_{\infty,1}, \zeta_{\infty,2}, \ldots, \zeta_{\infty,t''}$ to $k(y, z)$ which are characterized by saying that $\zeta_{\infty,j}(\epsilon_j(y^{(q+t)/t'}z^{(q-1)/t'})) > 0$ for $1 \leq j \leq t''$, and moreover $\zeta_0, \zeta_{\infty,1}, \zeta_{\infty,2}, \ldots, \zeta_{\infty,t''}$ are exactly all the extensions of w_0 to $k(y, z)$, and we have $\bar{r}(\zeta_0 : \kappa_0) = q + t$, $\bar{r}(\zeta_0 : w_0) = t$, $\bar{r}(\zeta_{\infty,j} : \kappa_\infty) = (q + t)/t'$ for $1 \leq j \leq t''$, and $\bar{r}(\zeta_{\infty,j} : w_0) = (q - 1)/t'$ for $1 \leq j \leq t''$.

Finally note that, since v_∞ is the only valuation of $k(x)$ which is ramified in $k(y)$, no valuation of $k(y)$, other than w_0 and w_∞, can be ramified in $k(y, z)$, and no valuation of $k(y, z)$, other than $\zeta_1, \zeta_2, \ldots, \zeta_{t^*}, \zeta_0, \zeta_{\infty,1}, \zeta_{\infty,2}, \ldots, \zeta_{\infty,t''}$, can be ramified in the splitting field of $\Phi(W)$ over $k(y, z)$.

Now, as noted above, if $t = 1$ then $\gamma(Z) = 1$, whereas if $t = 2$ then $\gamma(Z) = Z + 1$, and hence, in connection with the top half of the above diagram, we have that

$(1')$ $\qquad t = 1 \Rightarrow y^{q+1} = \dfrac{z}{(z+1)^q}$, and $t^* = 1$ and $\psi_1(z) = z + 1$

whereas

$(2')$

$$t = 2 \Rightarrow y^{q+2} = \frac{2^{q-2}z^2}{(z+2)^q(z+1)}, \quad t^* = 2, \quad \psi_1(z) = z + 1, \quad \text{and} \quad \psi_2(z) = z + 2.$$

Concerning the bottom half of the above diagram we note that

$$t = 2 \Rightarrow \frac{\mathrm{LCM}(\bar{r}(\zeta_0 : w_0), \bar{r}(\zeta_{\infty,1} : w_0), \ldots, \bar{r}(\zeta_{\infty,t''} : w_0))}{\bar{r}(\zeta_0 : w_0)}$$

$(2'')$

$$= \begin{cases} \frac{q-1}{6} & \text{if } q \equiv 1(3), \\ \frac{q-1}{2} & \text{if } q \not\equiv 1(3). \end{cases}$$

Recall that a permutation group is said to be *semiregular* if its stabilizer, at any point in the permuted set, is the identity; in our terminology this is equivalent to 1-antitransitive. By analogy, let us say that a univariate monic polynomial, with coefficients in some field, is *semiregular* over that field if by adjoining any one of its roots we get the splitting field. Note that then, assuming the roots to be distinct, the polynomial is semiregular if and only if its Galois group is semiregular.

For a moment suppose that $t = 1$ and k contains all the $(q-1)$th roots of 1. Then by (1^*) we see that $\Phi(W)$ is semiregular over $k(y, z)$ and hence its Galois group is 1-antitransitive; since this group is the 2-point stabilizer of the 2-transitive permutation group $\overline{G}_{n,q}$, we conclude that $\overline{G}_{n,q}$ is a $(2,3)$ group. Now if $p = 2$ then $\zeta_1((z+1)^q z^{q-2}) = q(q+1)$ and $\mathrm{GCD}(q-1, q(q+1)) = 1$, and therefore by (1^*) we see that $\Phi(W)$ is irreducible in $k(y, z)[W]$ and its Galois group is a cyclic group of order $q-1$, and hence in particular the said Galois group is a $(1,1)$ group; consequently, $\overline{G}_{n,q}$ is a $(3,3)$ group. On the other hand, if $p \neq 2$ then by $(1')$ we have $(z+1)^q z^{q-2} = z^{q-1} y^{-(q+1)}$ and hence by (1^*) we get

$$\Phi(W) = (W^{(q-1)/2} - z^{(q-1)/2} y^{-(q+1)/2})(W^{(q-1)/2} + z^{(q-1)/2} y^{-(q+1)/2})$$

and also

$$\zeta_1(z^{(q-1)/2} y^{-(q+1)/2}) = \frac{1}{2} \zeta_1((z+1)^q z^{q-2}) = \frac{q(q+1)}{2}$$

and

$$\mathrm{GCD}\left(\frac{q-1}{2}, \frac{q(q+1)}{2}\right) = 1,$$

and hence the above two factors of $\Phi(W)$ are irreducible in $k(y, z)[W]$ and the Galois group of $\Phi(W)$ over $k(y, z)$ is a cyclic group of order $\frac{q-1}{2}$. Thus, *if $t = 1$ and k contains all the $(q-1)$th roots of 1, then $\overline{G}_{n,q}$ is a $(2,3)$ group, and moreover if also $p = 2$ then $\overline{G}_{n,q}$ is a $(3,3)$ group and its order is $(q+1)q(q-1)$, whereas if $p \neq 2$ then $\overline{G}_{n,q}$ is not a $(3,3)$ group and its order is $\frac{(q+1)q(q-1)}{2}$.*

Therefore by an obvious corollary of the Zassenhaus-Feit-Suzuki Theorem we see that *if $t = 1$ and k contains all the $(q-1)$th roots of 1, then $\overline{G}_{n,q} = \mathrm{PSL}(2, q)$ with the possible exception that for $q = 7$ we may have $\overline{G}_{n,q} = \mathrm{A\Gamma L}(1, 8)$*.

The said corollary may be formulated in the following manner. For deducing this corollary from the Zassenhaus-Feit-Suzuki Theorem, the only thing we need to check is that if the (degree, order) pair $(2^l, 2^l(2^l - 1)l)$ of a Feit Group $\mathrm{A\Gamma L}(1, 2^l)$, where l is a prime, equals $(q + 1, \frac{(q+1)q(q-1)}{2})$ then $l = (2^l - 2)/2 = 2^{l-1} - 1$ and by direct calculation we see that this is not possible for $l = 2$, but is possible for $l = 3$, and is never possible for $l \geq 4$ because then $2^{l-1} - 1 = 1 + 2 + 2^2 + \cdots + 2^{l-2} \geq 1 + 2(l - 2) = l + (l - 3) > l$.

Corollary of the Zassenhaus-Feit-Suzuki-Theorem. *If $p = 2$, i.e., if q is a positive power of 2, then $\mathrm{PSL}(2, q)$ is the only $(3, 3)$ group of degree $q + 1$. If $p \neq 2$, i.e., if q is a positive power of an odd prime p, then $\mathrm{PSL}(2, q)$ is the only $(2, 3)$ group of degree $q + 1$ and order $\frac{(q+1)q(q-1)}{2}$ with the exception that, in the case $q = 7$, the group $\mathrm{A\Gamma L}(1, 8)$ also satisfies this description.*

Now, on the one hand, by Result 4 on page 841 of [A3] we know that, in case k is algebraically closed, $\overline{G}_{n,q}$ is a quasi p-group, and, on the other hand, for the group $\mathrm{A\Gamma L}(1, 8) = \mathrm{GF}(8) \rtimes \Gamma\mathrm{L}(1, 8)$ we have $\Gamma\mathrm{L}(1, 8) = \mathrm{GL}(1, 8) \rtimes \mathrm{Aut}(\mathrm{GF}(8))$ and hence $\mathrm{Aut}(\mathrm{GF}(8)) = Z_3$ is a homomorphic image of $\mathrm{A\Gamma L}(1, 8)$ and therefore $\mathrm{A\Gamma L}(1, 8)$ is not a quasi 7-group.[72] Con-

---

[72]A quasi p-group can be characterized as a finite group having no homomorphic image whose order is prime to p and greater than 1.

sequently, in case k is algebraically closed, the said exception cannot occur and hence *if k is algebraically closed and $t = 1$, then $\overline{G}_{n,q} = \mathrm{PSL}(2, q) = \mathrm{PSL}(2, n - 1)$.*

Before proceeding further, let us record the following

Fourth Irreducibility Lemma. *Remember that p is a prime number, and t is a positive integer.[73] For $0 \leq i \leq t$, let $f_i(Y)$ and $g_i(Y)$ be monic polynomials of degree $p + t - i$ in Y with coefficients in a field K_i, such that $g_i(Y)$ is obtained from $f_i(Y)$ by making one or more of the three operations of multiplying the roots by a nonzero quantity in K_i, reciprocating the roots,[74] and decreasing the roots by a quantity in K_i. Assume that, for $1 \leq i \leq t$, the polynomial $f_i(Y)$ is obtained by throwing away a root α_i of $g_{i-1}(Y)$, and for the field K_i we have $K_i = K_{i-1}(\alpha_i)$. Also assume that $f_0(Y)$ has no multiple roots.[75] Finally assume that there exist valuations $\hat{u}^{(i)}$ and $u^{(i)}$ of K_i for $0 \leq i \leq t$ such that $\hat{u}^{(0)} = u^{(0)}$; for $1 \leq i \leq t$, the valuation $\hat{u}^{(i)}$ is an extension of $\hat{u}^{(i-1)}$ to K_i; for $1 \leq i \leq t$, the valuation $u^{(i)}$ is an extension of $u^{(i-1)}$ to K_i; for every i with $1 \leq i \leq t$ we have $\bar{r}(\hat{u}^{(i)} : \hat{u}^{(i-1)}) \not\equiv 0(p)$; and for some j with $1 \leq j \leq t$ we have $\bar{r}(u^{(j)} : u^{(j-1)}) \equiv 0(p)$.*

Let u' be an extension of $u^{(t)}$ to a splitting field K' of $g_t(Y)$ over K_t, and let $r^* = \prod_{i=1}^{t} \bar{r}(u^{(i)} : u^{(i-1)})$ and $r' = \bar{r}(u' : u^{(t)})$. Let $u_1^{(t)} = u^{(t)}, u_2^{(t)}, \ldots, u_\delta^{(t)}$ be all the extensions of $u^{(t-1)}$ to K_t, and let

$$r'' = \frac{\mathrm{LCM}(\bar{r}(u_1^{(t)} : u^{(t-1)}), \ldots, r(u_\delta^{(t)} : u^{(t-1)}))}{\bar{r}(u^{(t)} : u^{(t-1)})}.$$

Finally let $\bar{u}^{(0)}, \ldots, \bar{u}^{(t)}, \bar{u}'$ be any valuations of $K_0, \ldots, K_t, K'$ respectively, with $\bar{u}^{(0)} = u^{(0)}$, such that $\bar{u}^{(i)}$ is an extension of $\bar{u}^{(i-1)}$ for $1 \leq i \leq t$, and $\bar{u}'$ is an extension of $\bar{u}^{(t)}$ for $1 \leq i \leq t$, and let $\bar{r}^* = \prod_{i=1}^{t} \bar{r}(\bar{u}^{(i)} : \bar{u}^{(i-1)})$ and $\bar{r}' = \bar{r}(\bar{u}' : \bar{u}^{(t)})$.

Then the polynomial $g_t(Y)$ is irreducible in $K_t[Y]$, and we have $|\mathrm{Gal}(g_t, K_t)| \equiv 0(r')$ and $r' \equiv 0(r'')$ and $\bar{r}^* \bar{r}' = r^* r'$. Moreover, if $g_{t-1}(Y)$ is irreducible in $K_{t-1}[Y]$, and the residue field of $u^{(0)}$ is an algebraically closed field of the same characteristic as K_0, and $\bar{r}(u_j : u^{(t-1)}) \not\equiv 0(\mathrm{char}\, K_0)$ for $1 \leq j \leq \delta$, then $r' = r''$.

To see this, take an extension $\hat{u}'$ of $\hat{u}^{(t)}$ to K'. By assumption

$$\bar{r}(u^{(j)} : u^{(j-1)}) \equiv 0(p) \quad \text{for some } j \text{ with } 1 \leq j \leq t$$

and clearly $\bar{r}(u' : u^{(0)}) = r^* r'$, and hence we must have $\bar{r}(u' : u^{(0)}) \equiv 0(p)$. Now both the valuations $\hat{u}'$ and u' are extensions of $\hat{u}^{(0)} = u^{(0)}$ to K' which is a Galois extension of K_0,[76] and hence $\bar{r}(\hat{u}' : \hat{u}^{(0)}) = \bar{r}(u' : u^{(0)})$, and therefore $\bar{r}(\hat{u}' : \hat{u}^{(0)}) \equiv 0(p)$. By assumption $\bar{r}(\hat{u}^{(i)} : \hat{u}^{(i-1)}) \not\equiv 0(p)$ for $1 \leq i \leq t$ and clearly $\bar{r}(\hat{u}' : \hat{u}^{(0)}) = \bar{r}(\hat{u}^{(1)} : \hat{u}^{(0)}) \ldots \bar{r}(\hat{u}^{(t)} : \hat{u}^{(t-1)})\bar{r}(\hat{u}' : \hat{u}^{(t)})$, and hence we must have $\bar{r}(\hat{u}' : \hat{u}^{(t)}) \equiv 0(p)$. By assumption K' is a splitting field of $g_t(Y)$ over K_t and hence $|\mathrm{Gal}(g_t, K_t)|$ must be divisible by $\bar{r}(\hat{u}' : \hat{u}^{(t)})$, and therefore $|\mathrm{Gal}(g_t, K_t)| \equiv 0(p)$; since $g_t(Y)$ is a monic polynomial of degree p in Y

---

[73]In this lemma, t is allowed to be divisible by p.

[74]In case of reciprocating the roots, we of course assume that zero is not a root.

[75]In any field extension of K_0.

[76]Because it is a splitting field of $f_0(Y)$ over K_0.

with coefficients in K_t, we conclude that $g_t(Y)$ is irreducible in $K_t[Y]$. Since K' is a splitting field of $g_t(Y)$ over K_t, we also get $|\operatorname{Gal}(g_t, K_t)| \equiv 0(r')$. Now K' is a Galois extension of K_{t-1}, and hence $r' \equiv 0(r'')$. Since K' is a Galois extension of K_0, and $\bar{u}'$ and u' are extensions of $\bar{u}^{(0)} = u^{(0)}$ to K', we also get $\bar{r}^*\bar{r}' = \bar{r}(\bar{u}' : \bar{u}^{(0)}) = \bar{r}(u' : u^{(0)}) = r^*r'$. If $g_{t-1}(Y)$ is irreducible in $K_{t-1}[Y]$ then K' is a least Galois extension of K_{t-1} containing K_t, and hence the last assertion follows from Proposition 7 on page 845 of [A3].

Note that this lemma gives an alternative proof of the irreducibility of $\Lambda(Y)$ in case of $q = p$ and $t = 1$. In fact we have the following

Corollary of the Fourth Irreducibility Lemma. *If k is algebraically closed and $F(Y)$ is a monic irreducible polynomial of degree $p + 1$ in Y with coefficients in $k(X)$ such that no valuation of $k(X)/k$, other than the valuation given by $X = \infty$, is ramified in the root field of $F(Y)$ over $k(X)$, then the Galois group $\operatorname{Gal}(F, k(X))$ is 2-transitive.*

To deduce this from the lemma, it suffices to note that, in view of Proposition 6 on page 835 of [A3], in the root field of $F(Y)$ over $k(X)$, the valuation $X = \infty$ must split into two valuations with reduced ramification exponents p and 1 respectively.[77]

More interestingly, in view of the ramification diagram and implication $(2'')$, by the above lemma we see that *if $q = p$ and $n = p + t$ with $t = 2 \not\equiv 0(p)$, then $\Phi(W)$ is irreducible in $k(y, z)[W]$ and so $\overline{G}_{n,p}$ is 3-transitive, and the order of its 3-point stabilizer $\operatorname{Gal}(\Phi, k(y, z))$ is divisible by τ, where $\tau = \frac{p-1}{6}$ or $\tau = \frac{p-1}{2}$ according as $p \equiv 1(3)$ or $p \not\equiv 1(3)$, and hence the order of $\overline{G}_{n,p}$ is divisible by $(p + 2)(p + 1)p\tau$, and moreover the reduced ramification exponent of any extension of ζ_0 (resp. $\zeta_1, \zeta_2, \zeta_{\infty,1}, \dots, \zeta_{\infty,t''}$) to a splitting field of $\Phi(W)$ over $k(y, z)$ is divisible by τ (resp. $p\tau, \tau, 1, \dots, 1$), and, in case k is algebraically closed, the reduced ramification exponent of any extension of ζ_0 (resp. $\zeta_1, \zeta_2, \zeta_{\infty,1}, \dots, \zeta_{\infty,t''}$) to a splitting field of $\Phi(W)$ over $k(y, z)$ equals τ (resp. $p\tau, \tau, 1, \dots, 1$).*[78]

Therefore by the following Corollary of CTT we see that *if $q = p$ and $n = p + t$ with $t = 2 \not\equiv 0(p)$, and if $\overline{G}_{n,p}$ is neither equal to A_n nor equal to S_n,*[79] *then either $p = 7$ and $\overline{G}_{n,p} = \operatorname{PSL}(2, 8)$, or $p = 7$ and $\overline{G}_{n,p} = \operatorname{P\Gamma L}(2, 8)$, or $p = 31$ and $\overline{G}_{n,p} = \operatorname{P\Gamma L}(2, 32)$.*

Corollary of CTT. *Let G be a 3-transitive permutation group of degree $n = p + 2$ with an odd prime p, such that G is neither equal to A_n nor equal to S_n. Then $p = 2^\mu - 1$ for some prime μ,*[80] *and either $G = \operatorname{PSL}(2, 2^\mu)$ or $G = \operatorname{P\Gamma L}(2, 2^\mu)$. Moreover, if the order of G is divisible by $(p + 2)(p + 1)p\tau$, where $\tau = \frac{p-1}{6}$ or $\frac{p-1}{2}$ according as $p \equiv 1(3)$ or $p \not\equiv 1(3)$, then either $p = 7$ and $G = \operatorname{PSL}(2, 8)$, or $p = 7$ and $G = \operatorname{P\Gamma L}(2, 8)$, or $p = 31$ and $G = \operatorname{P\Gamma L}(2, 32)$.*

To deduce the above Corollary from CTT, by inspection we see that no group

---

[77]Alternatively, in view of Proposition 6 on page 835 of [A3], this Corollary can be deduced from the fact that if G is a transitive permutation group of degree $p + 1$ of order divisible by p then G must contain a p-cycle and hence it must be 2-transitive.

[78]In the present case, by $(2')$ we have $t^* = 2$.

[79]That is if, as a permutation group, it is not isomorphic to either of these.

[80]Recall that a prime p is called a Mersenne prime if it is of the form $2^\mu - 1$ for some positive integer μ, and then automatically μ is itself a prime number.

listed in items (3) to (8) of CTT has degree of the form $p + 2$ with an odd prime p. Moreover the degree of every group listed in items (1) and (2) of CTT is of the form $\pi^\mu + 1$, with prime π and positive integer μ, and if we have $\pi^\mu + 1 = p + 2$ then, in case of odd π, we would get the contradiction $p = \pi^\mu - 1 \equiv 0(2)$. Therefore by CTT we conclude that $p = 2^\mu - 1$ for some prime μ, and G is a group between $\mathrm{PSL}(2, 2^\mu)$ and $\mathrm{P\Gamma L}(2, 2^\mu)$. Since μ is prime and $\mathrm{PSL}(2, 2^\mu)$ is a normal subgroup of $\mathrm{P\Gamma L}(2, 2^\mu)$ of index μ, there are no groups strictly between $\mathrm{PSL}(2, 2^\mu)$ and $\mathrm{P\Gamma L}(2, 2^\mu)$. Therefore $G = \mathrm{PSL}(2, 2^\mu)$ or $G = \mathrm{P\Gamma L}(2, 2^\mu)$. Now if the order of G is divisible by $(p+2)(p+1)p\tau$, then $(p+2)(p+1)p\mu = |\mathrm{P\Gamma L}(2, 2^\mu)| \geq |G| \geq (p+2)(p+1)p\tau$ and hence $\mu \geq \tau \geq \frac{p-1}{6} = (2^\mu - 2)/6$ and therefore $2^{\mu-1} - 1 \leq 3\mu$; on the other hand, if $\mu > 5$ then $2^{\mu-1} - 1 = (1 + 2 + 2^2) + (2^3 + 2^4 + \cdots + 2^{\mu-2}) \geq 7 + 8(\mu - 4) = 3\mu + 5(\mu - 5) > 3\mu$. Therefore if the order of G is divisible by $(p+2)(p+1)p\tau$, then we must have $\mu = 2$ or 3 or 5, i.e., $p = 3$ or 7 or 31; now the case $p = 3$ is ruled out because then $\mathrm{PSL}(2, 2^\mu) = A_n$ and $\mathrm{P\Gamma L}(2, 2^\mu) = S_n$ with $\mu = 2$ and $n = 5$; also, in case of $p = 31$, we cannot have $G = \mathrm{PSL}(2, 32)$ because $|\mathrm{PSL}(2, 32)| = 33 \cdot 32 \cdot 31 < 33 \cdot 32 \cdot 31 \cdot 5 = (p+2)(p+1)p\tau$.

Once again by Result 4 on page 841 of [A3] we know that, in case k is algebraically closed, the group $\overline{G}_{n,q}$ is a quasi p-group, and obviously, in the case $p \neq 2$, the group S_n is not a quasi p-group because it has Z_2 as a homomorphic image, and likewise, in the case of a Mersenne prime $p = 2^\mu - 1$, with a prime μ, the group $\mathrm{P\Gamma L}(2, 2^\mu)$ is not a quasi p-group because it has Z_μ as a homomorphic image. Therefore by the above italicized conclusion we see that *if k is algebraically closed and $q = p$ and $n = p + t$ with $t = 2 \not\equiv 0(p)$, then in the case $p \neq 7$ we have $\overline{G}_{n,p} = A_n$, whereas in the case $p = 7$ we have $\overline{G}_{n,p} = A_n$ or $\mathrm{PSL}(2, n - 1)$.*

Now let ω be an element in an overfield of $k(y, z)$ such that

$$(**) \qquad\qquad \Phi(\omega) = 0,$$

and let $\Psi(U)$ be the monic polynomial of degree $q - 1$ in an indeterminate U with coefficients in $k(y, z, \omega)$ obtained by throwing away the root ω of $\Phi(U)$. Actually, $\Phi(U) \in k(z)[U]$ and hence $\Psi(U) \in k(z, \omega)[U]$.

To compute $\Psi(U)$, let prime stand for the twisted U-derivative at ω; then we have $\Psi(U) = \Phi'(U)$, and by the prime power rule we have $(U^q)' = U^{q-1}$, and by the power rule we have $(U^0)' = 0$ and $(U)' = 1$, and by direct calculation we have

$$
\begin{aligned}
(U^{q-1})' &= \frac{(U + \omega)^{q-1} - \omega^{q-1}}{U} \\
&= \frac{\omega^{q-1}\left[-1 + \left(1 + \frac{U}{\omega}\right)^q \left(1 + \frac{U}{\omega}\right)^{-1}\right]}{U} \\
&= \frac{\omega^{q-1}\left[-1 + \left(1 + \frac{U^q}{\omega^q}\right)\left(1 - \frac{U}{\omega} + \frac{U^2}{\omega^2} - \frac{U^3}{\omega^3} + \cdots\right)\right]}{U} \\
&= \frac{\omega^{q-1}\left[-1 + \left(1 - \frac{U}{\omega} + \frac{U^2}{\omega^2} - \cdots + \frac{U^{q-1}}{\omega^{q-1}}\right)\right]}{U} \\
&= U^{q-2} - \omega U^{q-3} + w^2 U^{q-4} - \cdots + \omega^{q-3} U - w^{q-2},
\end{aligned}
$$

and therefore, in view of (2^*), by linearity we see that

(2^{**})

$$t = 2 \Rightarrow \begin{cases} \Psi(U) = U^{q-1} + (z+1)z[U^{q-2} - \omega U^{q-3} + \omega^2 U^{q-4} - \cdots + \omega^{q-3}U] \\ \qquad - (z+1)z[\omega^{q-2} + (z+2)^q z^{q-4}]. \end{cases}$$

For a moment suppose that k is algebraically closed and $q = p = 7$ and $t = 2$. Since A_9 is 4-transitive and $\mathrm{PSL}(2, 8)$ is sharply 3-transitive, by the above italicized assertion it follows that $\overline{G}_{n,p} \neq A_n \Leftrightarrow \overline{G}_{n,p} = \mathrm{PSL}(2, n-1) \Leftrightarrow \Psi(U)$ is reducible in $k(y, z, \omega)[U] \Leftrightarrow \Psi(U)$ completely factors (into linear factors) in $k(y, z, \omega)[U]$. To convert the question of reducibility of $\Psi(U)$ over the field $k(y, z, \omega)$ to its reducibility over the simpler field $k(z, \omega)$, first note that $k(z, \omega) \subset k(y, z, \omega)$ and hence $\Psi(U)$ is reducible in $k(z, \omega)[U] \Rightarrow \Psi(U)$ is reducible in $k(y, z, \omega)[U]$; next, by $(2')$ we see that $k(y, z, \omega)$ is a cyclic extension of $k(z, \omega)$ of degree 1 or 3 or 9, and hence $\Psi(U)$ completely factors in $k(y, z, \omega)[U] \Rightarrow$ the degrees of the irreducible factors of $\Psi(U)$ in $k(z, \omega)[U]$ are $(3,3)$ or $(3,1,1,1)$ or $(1,1,1,1,1,1)$. *Therefore if k is algebraically closed and $q = p = 7$ and $n = p + t$ with $t = 2$ then $\overline{G}_{n,p} \neq A_n \Leftrightarrow \overline{G}_{n,p} = \mathrm{PSL}(2, n-1) \Leftrightarrow \Psi(U)$ is reducible in $k(y, z, \omega)[U] \Leftrightarrow \Psi(U)$ completely factors (into linear factors) in $k(y, z, \omega)[U] \Leftrightarrow \Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow$ the degrees of the irreducible factors of $\Psi(U)$ in $k(z, \omega)[U]$ are $(3, 3)$ or $(3, 1, 1, 1)$ or $(1, 1, 1, 1, 1, 1)$.*

To further simplify the question of reducibility of $\Psi(U)$, we proceed to eliminate the last two possibilities of $(3, 1, 1, 1)$ and $(1, 1, 1, 1, 1, 1)$ for the degrees of the irreducible factors of $\Psi(U)$ in $k(z, \omega)$. Afterwards, we shall also indicate how the question of reducibility of $\Psi(U)$ in $k(z, \omega)[U]$ can be converted to its reducibility in $k_p(z, \omega)[U]$.

Recall that $\gamma(Z)$ is a monic polynomial of degree $t-1$ in Z with coefficients in the prime field $k_p \subset k$. Let

$$y^* = \frac{(z+t)^q \gamma(z)}{z^t}$$

and

$$\Lambda^*(Z) = (Z+t)^q \gamma(Z) - y^* Z^t \in k_p(y^*)[Z].$$

Now the element y^* is transcendental over k, the polynomial $\Lambda^*(Z)$ is irreducible in $k(y^*)[Z]$, the element z is a root of $\Lambda^*(Z)$, the polynomial $\Lambda'(Z) \in k_p(z)[Z]$ is obtained by throwing away the root z of $\Lambda^*(Z)$, the polynomial $\Phi(W) \in k_p(z)[W]$ is obtained by multiplying the roots of $\Lambda'(W)$ by z, the element ω is a root of $\Phi(W)$, the polynomial $\Psi(U) \in k_p(z, \omega)[U]$ is obtained by throwing away the root ω of $\Phi(U)$, and finally *if $q = p$ and $t = 2$ then the polynomial $\Phi(W)$ is irreducible in $k(z)[W]$ and hence $\mathrm{Gal}(\Lambda^*, k(y^*))$ and $\mathrm{Gal}(\Lambda^*, k_p(y^*))$ are 2-transitive permutation groups of degree $p + 1$.*

For $t = 2$ we have $\gamma(Z) = Z + 1$ and so

(2^{***}) $\quad t = 2 \Rightarrow y^* = \dfrac{(z+2)^q(z+1)}{z^2}$ and $\Lambda^*(Z) = (Z+2)^q(Z+1) - y^* Z^2.$

If $q = p$ and $t = 2$ then either directly by the above expression for y^*, or indirectly by the formulae $(*)$ and $(2')$ and the ramification diagram of the field extension $k(y) \subset k(y, z)$, we see that $w_0^* : y^* = 0$ and $w_\infty^* : y^* = \infty$ are the only valuations of $k(y^*)/k$ which are ramified in $k(z)$, the valuation w_0^*

splits into the valuations $\kappa_1 : z + 1 = 0$ and $\kappa_2 : z + 2 = 0$ of $k(z)/k$ with reduced ramification exponents $\bar{r}(\kappa_1 : w_0^*) = 1$ and $\bar{r}(\kappa_2 : w_0^*) = p$, and the valuation w_∞^* splits into the valuations $\kappa_0 : z = 0$ and $\kappa_\infty : z = \infty$ of $k(z)/k$ with reduced ramification exponents $\bar{r}(\kappa_0 : w_\infty^*) = 2$ and $\bar{r}(\kappa_\infty : w_\infty^*) = p - 1$. Thus, in case of $q = p$ and $t = 2$ we have the special ramification diagram for the field extension $k(y^*) \subset k(z)$ where the square bracketed numbers are the reduced ramification exponents:

$$
\begin{array}{l}
w_0^* : y^* = 0 \longrightarrow \left| \begin{array}{l} \to \kappa_1 : z + 1 = 0[1] \\[2em] \to \kappa_2 : z + 2 = 0[p] \end{array} \right. \\[4em]
w_\infty^* : y^* = \infty \longrightarrow \left| \begin{array}{l} \to \kappa_0 : z = 0[2] \\[2em] \to \kappa_\infty : z = \infty[p - 1]. \end{array} \right.
\end{array}
$$

For a moment suppose that $q = p$ and $t = 2$. Since the degree of $\Phi(W)$ is p, by the above diagram we see that κ_1 has a unique extension λ_1 to $k(z, \omega)$, for λ_1 we have $\bar{r}(\lambda_1 : \kappa_1) = p$, and the reduced ramification exponent of any extension of λ_1 to a splitting field of $\Psi(U)$ over $k(z, \omega)$ equals the reduced ramification exponent of any extension of κ_2 to the said splitting field. By direct calculation with the expression of $\Phi(W)$ given in (2^*), it can be shown that κ_2 has 3 extensions to $k(z, \omega)$ with reduced ramification exponents $(1, \frac{p-1}{2}, \frac{p-1}{2})$. Therefore, say by the Fourth Irreducibility Lemma, the reduced ramification exponent of any extension of λ_1 to the said splitting field must be divisible by $\frac{p-1}{2}$. Consequently the degree of some irreducible factor of $\Psi(U)$ in $k(z, \omega)[U]$ must be $\geq \frac{p-1}{2}$. The said direct calculation will not be given here,[81] and hence, for deducing the last consequence, at least in the case when k is algebraically closed, let us indirectly argue in the following manner.

So for a moment suppose that k is algebraically closed and $q = p$ and $t = 2$. Now in view of MRT,[82] by implication $(2')$ and by the paragraphs "Finally note that..." and "More interestingly...", we see that $\kappa_1, \kappa_2, \kappa_0$ are the only valuations of $k(z)/k$ which are ramified in a splitting field of $\Phi(W)$ over $k(z)$, and the reduced ramification exponent of any extension of κ_1 (resp. κ_2, κ_0) to the said splitting field is $\frac{p(p-1)}{2}$ (resp. $\frac{p-1}{2}, \frac{p-1}{2}$). Since the degree of $\Phi(W)$ is p, it follows that κ_1 has a unique extension λ_1 to $k(z, \omega)$, for λ_1 we have $\bar{r}(\lambda_1 : \kappa_1) = p$, and the reduced ramification index of any extension of λ_1 to a splitting field of $\Psi(U)$ over $k(z, \omega)$ is $\frac{p-1}{2}$. Therefore the degree of some irreducible factor of $\Psi(U)$ in $k(z, \omega)[U]$ must be $\geq \frac{p-1}{2}$.

Finally for a moment suppose that k is algebraically closed and $q = p = 7$ and $t = 2$. Then by the above paragraph and the paragraph following (2^{**}) we see that $\Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow$ the degrees of the irreducible

---

[81] But it will be given in my forthcoming paper [A7].
[82] MRT = Abhyankar's Lemma = Pages 181–186 of [A5].

factors of $\Psi(U)$ in $k(z, \omega)[U]$ are $(3,3)$ or $(3,1,1,1)$. Thus, $\Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow \mathrm{Gal}(\Lambda^*, k(y^*))$ is 2-transitive but neither 3-transitive nor sharply 2-transitive. Therefore, since $\mathrm{AGL}(1, 8)$ is sharply 2-transitive, by the Special CDT we conclude that $\Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow \mathrm{Gal}(\Lambda^*, k(y^*)) = \mathrm{PSL}(2, 7)$ or $\mathrm{A\Gamma L}(1, 8)$; by the Zassenhaus-Feit-Suzuki Theorem, both of these are $(2,3)$ groups, and hence $\Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow$ the degrees of the irreducible factors of $\Psi(U)$ in $k(z, \omega)[U]$ are $(3,3)$ and they have a common splitting field over $k(z, \omega)$ with Galois group Z_3. It follows that $\Psi(U)$ is reducible in $k_p(z, \omega)[U] \Leftrightarrow$ the degrees of the irreducible factors of $\Psi(U)$ in $k_p(z, \omega)[U]$ are $(3, 3) \Leftrightarrow \mathrm{Gal}(\Lambda^*, k_p(y^*))$ is 2-transitive but neither 3-transitive nor sharply 2-transitive $\Leftrightarrow \mathrm{Gal}(\Lambda^*, k_p(y^*))$ is not 3-transitive; therefore by CTT, Special CDT, and the Zassenhaus-Feit-Suzuki Theorem, we see that $\Psi(U)$ is reducible in $k_p(z, \omega)[U] \Leftrightarrow \mathrm{Gal}(\Lambda^*, k_p(y^*)) = \mathrm{PSL}(2, 7)$ or $\mathrm{A\Gamma L}(1, 8) \Leftrightarrow \mathrm{Gal}(\Lambda^*, k_p(y^*)) \notin \{S_8, A_8, \mathrm{AGL}(3, 2), \mathrm{PGL}(2, 7)\}$.

Let us close this long section with a

Summary about the bar polynomial. Let k be an algebraically closed field of characteristic $p \neq 0$. Let q be a positive power of p and let $n = q + t$ where t is a positive integer with $t \not\equiv 0(p)$. Let $\overline{F}_{n, q} = Y^n - XY^t + 1 \in k[X, Y]$ and let $\overline{G}_{n, q} = \mathrm{Gal}(\overline{F}_{n, q}, k(X))$. Without using CT we have shown that if $t = 1$ then $\overline{G}_{n, q} = \mathrm{PSL}(2, q) = \mathrm{PSL}(2, n - 1)$, whereas if $q = p$ and $t > 2 \neq p$ then $\overline{G}_{n, q} = A_n$, and finally if $q = p$ and $t > 2 = p$ then $\overline{G}_{n, q} = S_n$.[83] Using CT we have shown that if $q = p \neq 7$ and $t = 2$ then $\overline{G}_{n, q} = A_n$. Using CT, and referring to $(2^*), (2'), (**), (2^{**}), (2^{***})$ for notation and remembering that z is transcendental over k, we have also shown that if $q = p = 7$ and $t = 2$ then $\overline{G}_{n, q} \neq A_n \Leftrightarrow \overline{G}_{n, q} = \mathrm{PSL}(2, n - 1) \Leftrightarrow \Psi(U)$ is reducible in $k(y, z, \omega)[U] \Leftrightarrow \Psi(U)$ completely factors (into linear factors) in $k(y, z, \omega)[U] \Leftrightarrow \Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow$ the degrees of the irreducible factors of $\Psi(U)$ in $k(z, \omega)[U]$ are $(3, 3)$ and they have a common splitting field over $k(z, \omega)$ with Galois group $Z_3 \Leftrightarrow \mathrm{Gal}(\Lambda^*, k(y^*)) = \mathrm{A\Gamma L}(1, 8) \Leftrightarrow \Psi(U)$ is reducible in $k_p(z, \omega)[U] \Leftrightarrow$ the degrees of the irreducible factors of $\Psi(U)$ in $k_p(z, \omega)[U]$ are $(3, 3) \Leftrightarrow \mathrm{Gal}(\Lambda^*, k_p(y^*)) = \mathrm{A\Gamma L}(1, 8)$.

Remark. To establish the above long chain of equivalences, we still need to prove that

$(')$ $\qquad \overline{G}_{9, 7} = \mathrm{PSL}(2, 8) \Rightarrow \mathrm{Gal}(\Lambda^*, k(y^*)) \neq \mathrm{PSL}(2, 7)$

and

$('')$ $\qquad \mathrm{Gal}(\Lambda^*, k(y^*))$
$\qquad\qquad = \mathrm{A\Gamma L}(1, 8) \Rightarrow \mathrm{Gal}(\Lambda^*, k_p(y^*)) \notin \{S_8, A_8, \mathrm{AGL}(3, 2),$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathrm{PGL}(2, 7), \mathrm{PSL}(2, 7)\}.$

Now $\mathrm{Gal}(\Lambda, k(y))$ and $\mathrm{AGL}(1, 8)$ are the 1-point stabilizers of $\overline{G}_{9, 7}$ and $\mathrm{PSL}(2, 8)$ respectively, and hence to prove $(')$ it suffices to show that

$(''')$ $\qquad \mathrm{Gal}(\Lambda, k(y)) = \mathrm{AGL}(1, 8) \Rightarrow \mathrm{Gal}(\Lambda^*, k(y^*)) \neq \mathrm{PSL}(2, 7)$

Let f be a nonconstant univariate monic polynomial with coefficients in a field K having no multiple roots in any field extension of K, and let K^* be a (finite)

---

[83] Since $\mathrm{PSL}(2, 2) = S_3$, it follows that if $q = p = 2$ then $\overline{G}_{n, q} = S_n$.

Galois extension of K. By (2') and (2***) we see that, in the case $q = p = 7$ and $t = 2$, the field $k(y)$ is a Galois extension of the field $k(y^*)$ and hence, by taking $f = \Lambda = \Lambda^*$ and $(K, K^*) = (k(y^*), k(y))$, implication (''') follows from the implication

$$(\natural) \qquad \text{Gal}(f, K^*) = \text{AGL}(1, 8) \Rightarrow \text{Gal}(f, K) \neq \text{PSL}(2, 7).$$

Also clearly for some finite algebraic field extension k^* of k_p we have that $\text{Gal}(\Lambda^*, k^*(y^*)) = \text{Gal}(\Lambda^*, k(y^*))$ and $k^*(y^*)$ is a Galois extension of $k_p(y^*)$ and hence, by taking $f = \Lambda^*$ and $(K, K^*) = (k_p(y^*), k^*(y^*))$, implication ('') follows from the implication

$(\natural\natural)$
$$\begin{aligned}\text{Gal}(f, K^*) &= \text{A}\Gamma\text{L}(1, 8) \\ &\Rightarrow \text{Gal}(f, K) \notin \{S_8, A_8, \text{AGL}(3, 2), \text{PGL}(2, 7), \text{PSL}(2, 7)\}.\end{aligned}$$

Now $\text{AGL}(1, 8)$ is a nonidentity solvable group and $\text{PSL}(2, 7)$ is a nonabelian simple group, and hence $\text{AGL}(1, 8)$ is not isomorphic to a normal subgroup of $\text{PSL}(2, 7)$, and therefore $(\natural)$ follows from the Refined Extension Principle. Likewise, $\text{A}\Gamma\text{L}(1, 8)$ is a nonidentity solvable group but all the nonidentity normal subgroups of $\{S_8, A_8, \text{AGL}(3, 2), \text{PGL}(2, 7), \text{PSL}(2, 7)\}$ are nonsolvable because they respectively contain the nonabelian simple group $\{A_8, A_8, \text{PSL}(3, 2), \text{PSL}(2, 7), \text{PSL}(2, 7)\}$ as a normal subgroup, and hence $\text{A}\Gamma\text{L}(1, 8)$ cannot be isomorphic to a normal subgroup of any one of the groups $\{S_8, A_8, \text{AGL}(3, 2), \text{PGL}(2, 7), \text{PSL}(2, 7)\}$, and therefore $(\natural\natural)$ also follows from the Refined Extension Principle.

Note. Assuming $q = p = 7$ and $t = 2$, in my forthcoming paper [A7], first by resolving the singularities of the curve $\Phi(\omega) = 0$ in the (z, ω)-plane I calculate its genus in terms of infinitely near singularities, and then, seeing that the genus is 2 and hence the curve is hyperelliptic, by means of adjoints I express it as a double covering of the line, and finally, using the resulting square-root parametrization of the curve I show that the polynomial $\Psi(U)$ factors in $k(z, \omega)[U]$ into two factors of degree 3, and so I conclude that $\overline{G}_{9,7} = \text{PSL}(2, 8)$. Initially I used the square-root parametrization to take the "norm" of $\Psi(U)$ which is a monic polynomial $\Psi^\natural(T, U)$ of degree 12 in U with coefficients which are polynomials in T over the prime field k_7. I used REDUCE and MACSYMA to calculate $\Psi^\natural(T, U)$; the largest coefficient degree in T turned out to be 216, and it took 10 pages to print out the exact expressions of the coefficients. From what I have said above, it follows that $\Psi(U)$ is reducible in $k(z, \omega)[U] \Leftrightarrow \Psi^\natural(T, U)$ is reducible in $k_7[T, U] \Leftrightarrow \Psi^\natural(T, U)$ factors in $k_7[T, U]$ into two polynomials of degree 3 in U. Although the last two tasks are finitistic in nature, the computer algebra packages REDUCE and MACSYMA refused to factor bivariate polynomials over a finite field! So I turned back to hand calculation in a hyperelliptic function field, using MACSYMA only for checking ordinary polynomial operations !!

22. THE ROOF POLYNOMIAL AND DECREASING INDUCTION

Let X and Y be indeterminates over an algebraically closed field k of characteristic $p \neq 0$, let $0 \neq a \in k$, let s and t be positive integers with $t \not\equiv 0(p)$, and consider the polynomial

$$\widehat{F}_n = Y^n - aX^sY^t + 1 \quad \text{with } n = p + t$$

mentioned in §11. This corresponds to the $q = p$ case of the more general polynomial

$$\widehat{F}_{n,q} = Y^n - aX^sY^t + 1$$

with $n = q + t$ and $q =$ a positive power of p which was also mentioned in §11. The polynomials $\widehat{F}_n$ and $\widehat{F}_{n,q}$ in turn may be obtained by substituting aX^s for X in the polynomials

$$\overline{F}_{n,q} = Y^n - XY^t + 1$$

with $n = q + t$ and $q =$ a positive power of p and

$$\overline{F}_n = Y^n - XY^t + 1 \quad \text{with } n = p + t.$$

As noted in the beginning of §21, the Y-discriminant of the polynomials $\overline{F}_n$ and $\overline{F}_{n,q}$ is the nonzero element n^n of k, and hence the Y-discriminant of the polynomials $\widehat{F}_n$ and $\widehat{F}_{n,q}$ is also the nonzero element n^n of k, and therefore each one of the four polynomials $\overline{F}_n, \overline{F}_{n,q}, \widehat{F}_n, \widehat{F}_{n,q}$ gives an unramified covering of the affine line over k.[84]

In the beginning of §21, we noted that the polynomials $\overline{F}_n$ and $\overline{F}_{n,q}$ are irreducible in $k(X)[Y]$, and considering the Galois groups $\overline{G}_n = \text{Gal}(\overline{F}_n, k(X))$ and $\overline{G}_{n,q} = \text{Gal}(\overline{F}_{n,q}, k(X))$, as summarized in the Summary and the Note at the end of that section, in the rest of that section we proved the following.[85]

(I.1*) If $t = 1$, then $\overline{G}_n = \text{PSL}(2, p) = \text{PSL}(2, n - 1)$.

(I.2*) If $t = 2$ and $p = 7$, then $\overline{G}_n = \text{PSL}(2, 8) = \text{PSL}(2, n - 1)$.

(I.3*) If $t = 2$ and $p \neq 7$, then $\overline{G}_n = A_n$.

(I.4*) If $t > 2$ and $p \neq 2$, then $\overline{G}_n = A_n$.

(I.5*) If $p = 2$, then $\overline{G}_n = S_n$.

(III.1*) If $t = 1$, then $\overline{G}_{n,q} = \text{PSL}(2, q) = \text{PSL}(2, n - 1)$.

As noted in the said Summary and Note, on the one hand, CT was not used in the proofs of (I.1*), (I.4*), (I.5*), and (III.1*), and on the other hand, the proof (I.2*) was complete only modulo the reducibility of the polynomial $\Psi(U)$ which will be established in [A7]. Actually, CT was used only in the sense that, assuming $t = 2$, we first showed $\overline{G}_n$ to be a 3-transitive permutation group of degree n and from this by CTT we deduced that $\overline{G}_n = A_n$ or S_n. Now the 3-transitivity tells us that $|\overline{G}_n| \geq n(n - 1)(n - 2)$ and hence if $p = 3$ then obviously $\overline{G}_n = A_n$ or S_n. Likewise, for $p = 5$ we need not invoke CT because again in that case, say in view of the following elementary theorem which occurs as item IV on page 148 of Carmichael's book [Ca],[86] the 3-transitivity directly tells us that $\overline{G}_n = A_n$ or S_n.

---

[84]That is, say in view of Proposition 1 of [A1], $X = \infty$ is the only valuation of $k(X)/k$ which is possibly ramified in the splitting field of $\overline{F}_n$ (resp. $\overline{F}_{n,q}, \widehat{F}_n, \widehat{F}_{n,q}$) over $K(X)$.

[85]As said earlier, my work on this paper started when, in September 1988, Serre told me that he could prove (I.1*). As he now tells me, his proof, which also applies to (III.1*), uses "descending Galois theory" which is different from my method which he calls the "ascending" method. With Serre's kind permission, his letter to me, dated 15 November 1990, describing his "descending" proof, is appended herewith.

[86]The statement of Charmichael's Theorem given on page 154 of Volume I of Huppert [HB] says that A_n and S_n are the only l-transitive groups of degree n for which $l > \frac{n}{3}$. This seems incorrect beacause for $(l, n) = (4, 11)$ we have $4 > \frac{11}{3}$ but the Mathieu group M_{11} is a 4-transitive group of degree 11, and for $(l, n) = (5, 12)$ we have $5 > \frac{12}{3}$ but the Mathieu group M_{12} is a 5-transitive group of degree 12.

Carmichael's Theorem. A_n *and* S_n *are the only* l-*transitive groups of degree* n *for which* $l > [\frac{n}{3} + 1]$ *where* $[\frac{n}{3} + 1]$ *is the greatest integer not exceeding* $\frac{n}{3} + 1$.

By Corollaries (3.5) to (3.10) of the Substitutional Principle, the Galois groups $\widehat{G}_{n,q} = \mathrm{Gal}(\widehat{F}_{n,q}, k(X))$ and $\widehat{G}_n = \mathrm{Gal}(\widehat{F}_n, k(X))$ have the same description as the above description of the Galois groups $\overline{G}_n = \mathrm{Gal}(\overline{F}_n, k(X))$ and $\overline{G}_{n,q} = \mathrm{Gal}(\overline{F}_{n,q}, k(X))$. Let us summarize this in the following

Summary about the roof polynomial. Let k be an algebraically closed field of characteristic $p \neq 0$, let $0 \neq a \in k$, and let s and t be positive integers with $t \not\equiv 0(p)$. Then the polynomials $\widehat{F}_n = Y^n - aX^sY^t + 1$ with $n = p + t$ and $\widehat{F}_{n,q} = Y^n - aX^sY^t + 1$ with $n = q + t$ and $q = $ a positive power of p, give unramified coverings of the affine line over k, and for their Galois groups $\widehat{G}_n = \mathrm{Gal}(\widehat{F}_n, k(X))$ and $\widehat{G}_{n,q} = \mathrm{Gal}(\widehat{F}_{n,q}, k(X))$ we have the following.

(I.1) If $t = 1$, then $\widehat{G}_n = \mathrm{PSL}(2, p) = \mathrm{PSL}(2, n - 1)$.

(I.2) If $t = 2$ and $p = 7$, then $\widehat{G}_n = \mathrm{PSL}(2, 8) = \mathrm{PSL}(2, n - 1)$.

(I.3) If $t = 2$ and $p \neq 7$, then $\widehat{G}_n = A_n$.

(I.4) If $t > 2$ and $p \neq 2$, then $\widehat{G}_n = A_n$.

(I.5) If $p = 2$, then $\widehat{G}_n = S_n$.

(III.1) If $t = 1$, then $\widehat{G}_{n,q} = \mathrm{PSL}(2, q) = \mathrm{PSL}(2, n - 1)$.

Here, CT is not used in the proofs of (I.1), (I.4), (I.5) and (III.1); likewise, it is not used in the proof of (I.3) for $p < 7$. Moreover, referring to the polynomial $\Psi(U)$ obtained by taking $q = p = 7$ in item (2**) of the §21, the proof of (I.2) is complete only modulo the reducibility of $\Psi(U)$ in $k(z, \omega)$ to be established in [A7].

Now what does the "decreasing induction" in the title of this section refer to? Roughly speaking, it says that if we can find an unramified covering of the affine line with Galois group A_n then we can find one with Galois group A_{n-1}. If this were so without any qualification, then an A_n covering for large n would yield an A_n covering for all smaller n. But there is a qualification! More precisely, we have the following

Method of decreasing induction. Assuming that we are working over an algebraically closed field k of characteristic $p \neq 0$, let there be given an irreducible n-fold unramified covering of the affine line by the affine line,[87] such that the point at infinity splits exactly into two points, say the origin and the point at infinity, with ramification exponents p and $t = n - p \not\equiv 0(p)$, and let G be the Galois group of the given covering.[88] Now if $G = A_n$ with $n > 5$ then we can find an unramified covering of the affine line with Galois group A_{n-1}. More generally, without any condition on n or G, we can find an unramified covering of the affine line with Galois group $G^* \lhd G_1 = $ the 1-point stabilizer of G such that G_1/G^* is cyclic of order nondivisible by p.

To prove this informally, say the original line is the X-axis, and the covering line is the Y-axis, and let C be the least Galois covering of the X-axis "containing" (or, "dominating") the Y-axis. Then the Galois group of C over the Y-axis is the one-point stabilizer G_1 of G. Moreover, the origin of the

---

[87]That is, a covering of the projective line by the projective line, which is unramified over the affine line.

[88]That is, G is the Galois group of the associated least Galois covering.

Y-axis is tamely ramified in C, say with reduced ramification exponent t^*,[89] and the point at infinity of the Y-axis is the only other point which is possibly ramified in C. Now considering the Y^*-axis with $a^*Y^{*r} = Y$ with $0 \neq a^* \in k$ and $r \equiv 0(t^*)$, and passing to the "compositum" C^* of C and the Y^*-axis, by MRT[90] we see that C^* is an unramified covering of the affine line = the Y^*-axis, and upon letting G^* to be the Galois group of C^* over the Y^*-axis, by Corollary (3.1) of the Substitutional Principle we see that $G^* \triangleleft G_1 = $ the 1-point stabilizer of G, and G_1/G^* is cyclic of order nondivisible by p.

To apply this method to the polynomial $\overline{F}_n$, from the initial material[91] of §21 we recall that[92] by putting $X = x$ and reciprocating the roots of $\overline{F}_n$ we get the polynomial

$$\Theta(Y) = Y^{p+t} + xY^p + 1$$

and by letting y be a root of $\Theta(Y)$ in an overfield of $k(x)$ we have $k(x, y) = k(y)$, and by letting $\Theta'(Y)$ be the twisted Y-derivative of $\Theta(Y)$ at y, and letting $\Delta(Y)$ be the polynomial obtained by reciprocating the roots of $\Theta'(Y)$, and letting $\Lambda(Z)$ be the polynomial obtained by multiplying the roots of $\Delta(Z)$ by ty, we get

$$\Lambda(Z) = \gamma(Z)(Z + t)^p - t^{p-2}y^{-p-t}Z^t,$$

where

$$\gamma(Z) = t^{-2}[(Z + t)^t - Z^t].$$

Now $\Lambda(Z)$ is irreducible in $k(y)[Z]$ and has no multiple roots in any overfield of $k(y)$, and upon taking 1-point stabilizers, by (I.3*), (I.4*), and (I.5*) we get the following where CT is used only in the $p > 5$ case of (I.3**).

(I.3**) If $t = 2$ and $p \neq 7$, then $\mathrm{Gal}(\Lambda(Z), k(y)) = A_{n-1}$.

(I.4**) If $t > 2$ and $p \neq 2$, then $\mathrm{Gal}(\Lambda(Z), k(y)) = A_{n-1}$.

(I.5**) If $p = 2$, then $\mathrm{Gal}(\Lambda(Z), k(y)) = S_{n-1}$.

Remembering that s is any positive integer and a is any nonzero element of k, we let

$$\Lambda_{s,a}(Z) = \gamma(Z)(Z + t)^p - aY^{-s}Z^t$$

and we note that if $s \equiv 0(p + t)$ then $\Lambda_{s,a}(Z)$ can be obtained from $\Lambda(Z)$ by replacing y by $a'Y^{s/(p+t)}$, where $a' \in k$ is such that $t^{p-2}a'^{-p-t} = a$. In view of the LCM Theorem,[93] by the first ramification diagram[94] in §21, we see that LCM $(p - 1, t)$ is divisible by the reduced ramification exponent of every extension of the valuation $y = 0$ of $k(y)/k$ to a splitting field of $\Lambda(Z)$ over $k(y)$, and no valuation of $k(y)/k$, other than the valuations $y = 0$ and $y = \infty$, is ramified in the said splitting field. Therefore, if $s \equiv 0((p + t)\mathrm{LCM}(p - 1, t))$ then by MRT we see that no valuation of $k(Y)/k$, other than the valuation $Y = \infty$, is ramified in a splitting field of $\Lambda_{s,a}(Z)$ over $k(Y)$, and obviously $\Lambda_{s,a}(Z)$ has no multiple roots in any overfield of $k(Y)$, and in view of Corollaries (3.3), (3.5), and (3.8) of the Substitution Principle, by (I.3**), (I.4**), and (I.5**) we see that (3') if $t = 2$ and $p \neq 7$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$, whereas

---

[89]By the argument on pages 843–845 of [A3] we see that t^* divides LCM $(t, (p - 1)!)$ and hence the origin of the Y-axis is tamely ramified in C.

[90]MRT = pages 181–186 of [A5].

[91]Up to formula (*).

[92]Until further notice $q = p$ and $n = p + t$ with positive integer $t \not\equiv 0(p)$.

[93]That is, Proposition 7 on page 845 of [A3].

[94]Together with its explanation in the three paragraphs following it.

(4′) if $t > 2$ and $p \neq 2$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$, and finally (5′) if $p = 2$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = S_{n-1}$. Thus we have the following where CT is used only in the $p > 5$ case of (I. 3′).

(I. 0′) If $s \equiv 0((p + t)\,\mathrm{LCM}(p - 1, t))$ then no valuation of $k(Y)/k$, other than the valuation $Y = \infty$, is ramified in a splitting field of $\Lambda_{s,a}(Z)$ over $k(Y)$, and $\Lambda_{s,a}(Z)$ has no multiple roots in any overfield of $k(Y)$.

(I. 3′) If $t = 2$ and $p \neq 7$ and $s \equiv 0((p + t)\,\mathrm{LCM}(p - 1, t))$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$.

(I. 4′) If $t > 2$ and $p \neq 2$ and $s \equiv 0((p + t)\,\mathrm{LCM}(p - 1, t))$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$.

(I. 5′) If $p = 2$ and $s \equiv 0((p+t)\,\mathrm{LCM}(p-1, t))$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = S_{n-1}$.

Actually, the above four assertions remain valid if we replace the assumption that $s \equiv 0((p + t)\,\mathrm{LCM}(p - 1, t))$ by the weaker assumption that $s \equiv 0(\mathrm{LCM}(p - 1, t))$. To see this, first note that $\Lambda(Z)$ can be obtained from $\Lambda_{1,1}(Z)$ by replacing Y by $t^{2-p}y^{p+t}$; now since no valuation of $k(y)/k$, other than the valuations $y = 0$ and $y = \infty$, is ramified in a splitting field of $\Lambda(Z)$ over $k(y)$, it follows that no valuation of $k(Y)/k$, other than the valuations $Y = 0$ and $Y = \infty$, is ramified in a splitting field of $\Lambda_{1,1}(Z)$ over $k(Y)$; moreover since $\Lambda(Z)$ is irreducible in $k(y)[Z]$ and has no multiple roots in any overfield of $k(y)$, it follows that $\Lambda_{1,1}(Z)$ is irreducible in $k(Y)[Z]$ and has no multiple roots in any overfield of $k(Y)$; finally, in view of Corollary (3.1) the Substitutional Principle, by (I.3**) to (I.5**) we see that (3***) if $t = 2$ and $p \neq 7$, then $\mathrm{Gal}(\Lambda_{1,1}(Z), k(Y)) = A_{n-1}$ or S_{n-1}, and (4***) if $t > 2$ and $p \neq 2$, then again $\mathrm{Gal}(\Lambda_{1,1}(Z), k(Y)) = A_{n-1}$ or S_{n-1}, and (5***) if $p = 2$, then $\mathrm{Gal}(\Lambda_{1,1}(Z), k(Y)) = S_{n-1}$. Again, $\Lambda_{s,a}(Z)$ can be obtained from $\Lambda_{1,1}(Z)$ by substituting aY^s for Y and hence, in view of Corollaries (3.2) to (3.8) of the Substitutional Principle, we get the following where CT is used only in the $p > 5$ case of (I. 3″).

(I. 0″) No valuation of $k(Y)/k$, other than the valuations $Y = 0$ and $Y = \infty$, is ramified in a splitting field of $\Lambda_{s,a}(Z)$ over $k(Y)$, and $\Lambda_{s,a}(Z)$ is irreducible[95] in $k(Y)[Z]$ and has no multiple roots in any overfield of $k(Y)$.

(I. 3″) If $t = 2$ and $p \neq 7$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$ or S_{n-1}.

(I. 4″) If $t > 2$ and $p \neq 2$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$ or S_{n-1}.

(I. 5″) If $p = 2$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = S_{n-1}$.

Now $\gamma(0) \neq 0 \neq t$ and, upon letting Z' to be a root of $\Lambda_{1,1}(Z)$ in an overfield of $k(Y)$, we have

$$Y = \frac{Z'^t}{\gamma(Z')(Z' + t)^p}$$

and hence the valuation $Y = 0$ of $k(Y)/k$ splits in $k(Y, Z') = k(Z')$ into the valuations $Z' = 0$ and $Z' = \infty$ with reduced ramification exponents $t \not\equiv 0(p)$ and $p - 1 \not\equiv 0(p)$ respectively, and therefore by the LCM Theorem we see that $\mathrm{LCM}(p - 1, t)$ is divisible by the reduced ramification exponent of every extension of the valuation $Y = 0$ of $k(Y)/k$ to a splitting field of $\Lambda(Z)$ over $k(Y)$, and hence by MRT we see that if $s \equiv 0(\mathrm{LCM}(p-1, t))$ then no valuation of $k(Y)/k$, other than the valuation $Y = \infty$, is ramified in a splitting field of

---

[95]The irreducibility of $\Lambda_{s,a}$ follows from the First Irreducibility Lemma. Alternatively, it follows from the fact that a polynomial is irreducible if and only if its Galois group is transitive.

$\Lambda_{s,a}(Z)$ over $k(Y)$, and therefore by Result 4 on page 841 of [A3] we know that $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y))$ is a quasi p-group. Thus, in view of (I. 0″), (I. 3″), (I. 4″), and (I. 5″), we conclude with the following where CT is used only in the $p > 5$ case of (IV. 2′).

(IV. 0′) If $s \equiv 0(\mathrm{LCM}(p - 1, t))$, then no valuation of $k(Y)/k$, other than the valuation $Y = \infty$, is ramified in a splitting field of $\Lambda_{s,a}(Z)$ over $k(Y)$, and $\Lambda_{s,a}(Z)$ is irreducible in $k(Y)[Z]$ and has no multiple roots in any overfield of $k(Y)$.

(IV. 1′) If $t > 2$ and $p \neq 2$ and $s \equiv 0(\mathrm{LCM}(p - 1, t))$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$.

(IV. 2′) If $t = 2$ and $p \neq 7$ and $s \equiv 0(\mathrm{LCM}(p - 1, t))$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = A_{n-1}$.

(IV. 4′) If $p = 2$ and $s \equiv 0(\mathrm{LCM}(p - 1, t))$, then $\mathrm{Gal}(\Lambda_{s,a}(Z), k(Y)) = S_{n-1}$.

As we have said, CT is used only when $t = 2$; now in the case $t = 2$ we have $\gamma(Z) = Z + 1$ and hence $\Lambda_{s,a}(Z) = (Z + 1)(Z + 2)^p - aY^{-s}Z^t$; therefore by (I. 0″) we see that if $t = 2$ then $\Lambda_{s,a}(Z) = (Z + 1)(Z + 2)^p - aY^{-s}Z^t$ is unramified outside $Y = 0$ and $Y = \infty$. For getting hold of a variation of (I. 3‴) without CT, let us reprove the said unramifiedness in a more general context. So let

$$E(Z) = (Z + 1)(Z + b)^p - YZ^\tau$$

with $1 < \tau \leq p$ and $0 \neq b \in k$. Now for the (ordinary) Z-derivative we have

$$E_Z(Z) = (Z + b)^p - \tau YZ^{\tau-1}$$

and hence

$$E(Z) = (Z + 1)E_Z(Z) + E^*(Z),$$

where

$$E^*(Z) = (\tau - 1)YZ^{\tau-1}\left(Z + \frac{\tau}{\tau - 1}\right)$$

and therefore for the Z-discriminant we have

$$\begin{aligned}
\mathrm{Disc}_Z(E(Z)) &= \mathrm{Res}_Z(E(Z), E_Z(Z)) \\
&= \mathrm{Res}_Z(E^*(Z), E_Z(Z)) \\
&= (\tau - 1)^p Y^p E_Z(0)^{\tau-1} E_Z\left(\frac{-\tau}{\tau - 1}\right) \\
&= (\tau - 1)^p Y^p b^{p(\tau-1)} E_Z\left(\frac{-\tau}{\tau - 1}\right) \\
&= (\tau - 1)^p Y^p b^{p(\tau-1)}(-\tau Y)\left(\frac{-\tau}{\tau - 1}\right)^{\tau-1} \quad \text{if } b = \frac{\tau}{\tau - 1} \\
&= (-\tau)^\tau (\tau - 1)^{p-\tau+1} b^{p(\tau-1)} Y^{p+1} \quad \text{if } b = \frac{\tau}{\tau - 1}
\end{aligned}$$

and hence if $b = \frac{\tau}{\tau-1}$ then no valuation of $k(Y)/k$, other than the valuations $Y = 0$ and $Y = \infty$, is ramified in a splitting field of $E(Z)$ over $k(Y)$, and $E(Z)$ has no repeated roots in any overfield of $k(Y)$. Therefore, upon remembering that a is any nonzero element of k and s and t are any positive integers with $t \not\equiv 0(p)$, and upon letting

$$E_{s,a}(Z) = (Z + 1)(Z + b)^p - aY^{-s}Z^t$$

we get the following.[96]

(IV.0**) If $1 < t < p$ and $b = \frac{t}{t-1}$ then no valuation of $k(Y)/k$, other than the valuations $Y = 0$ and $Y = \infty$, is ramified in a splitting field of $E_{s,a}(Z)$ over $k(Y)$, and $E_{s,a}(Z)$ is irreducible[97] in $k(Y)[Z]$ and has no multiple roots in any overfield of $k(Y)$.

Before proceeding further, let us make note of the following

Alternate Corollary of the Fourth Irreducibility Lemma. *If $F(Z)$ is a monic irreducible polynomial of degree $p + 1$ in Z with coefficients in $k(Y)$ such that some valuation of $k(Y)/Y$, say the valuation $Y = \infty$, splits in a root field of $F(Z)$ over $k(Y)$ into two valuations with reduced ramification exponents p and 1, then the Galois group $\mathrm{Gal}(F(Z), k(Y))$ is 2-transitive.*

For a moment suppose that $1 < t < p$ and $b = \frac{t}{t-1}$. Now upon letting Z^* to be a root of $E_{1,1}(Z)$ in some overfield of $k(Y)$, we have

$$Y = \frac{Z^{*t}}{(Z^* + 1)(Z^* + b)^p}$$

and hence the valuation $Y = \infty$ of $k(Y)/k$ splits in $k(Y, Z^*) = k(Z^*)$ into two valuations with reduced ramification exponents p and 1 and therefore, by the above Alternate Corollary, $\mathrm{Gal}(E_{1,1}(Z), k(Y))$ is 2-transitive. By the above equation for Y we also see that the valuation $Y = 0$ of $k(Y)/k$ splits in $k(Z^*)$ into the valuations $Z^* = 0$ and $Z^* = \infty$ with reduced ramification exponents $t \not\equiv 0(p)$ and $p + 1 - t \not\equiv 0(p)$ respectively. Therefore on the one hand, by the LCM Theorem and MRT we see that if $s \equiv 0(t(p + 1 - t))$ then no valuation of $k(Y)/k$, other than the valuation $Y = \infty$, is ramified in a splitting field of $E_{s,a}(Z)$ over $k(Y)$, and hence by Result 4 on page 841 of [A3] we see that $\mathrm{Gal}(E_{s,a}(Z), k(Y))$ is a quasi p-group, and so if we already knew that $\mathrm{Gal}(E_{s,a}(Z), k(Y)) = A_{p+1}$ or S_{p+1} then we would conclude that $\mathrm{Gal}(E_{s,a}(Z), k(Y)) = A_{p+1}$. On the other hand, by the Cycle Lemma we see that if $\mathrm{GCD}(p + 1 - t, t) = 1$ then $\mathrm{Gal}(E_{1,1}(Z), k(Y))$ contains a t-cycle, and hence by Marggraff's First Theorem we see that if also $t < \frac{p+1}{2}$ then $\mathrm{Gal}(E_{1,1}(Z), k(Y)) = A_{p+1}$ or S_{p+1}. Note that if $p > 5$ and t is an odd prime factor of $\frac{(p-1)(p-3)}{4}$ then either t is an odd prime factor of $\frac{p-1}{2}$ or t is an odd prime factor of $\frac{p-3}{2}$, and in both the cases $1 < t < \frac{p+1}{2}$ and $\mathrm{GCD}(p+1, t) = 1$. Also note that, in the case $p > 5$, there do exist odd prime factors of $\frac{(p-1)(p-3)}{4}$, because otherwise we would have $p - 1 = 2^m$ with $m > 2$ and $p - 3 = 2^{m'}$ with $m' > 1$, and this would give $2^{m'-1} = \frac{p-3}{2} = \frac{p-1-2}{2} = 2^{m-1} - 1$ which would be a contradiction since $2^{m'-1}$ is even and $2^{m-1} - 1$ is odd. Thus, without using CT, we have proved the following.[98]

(IV.0*) If $p > 5$ then t can be chosen so that $1 < t < \frac{p+1}{2}$ and $\mathrm{GCD}(p + 1, t) = 1$, and for any such t, upon assuming $b = \frac{t}{t-1}$ and $s \equiv 0(t(p + 1 - t))$, we have that no valuation of $k(Y)/k$, other than the valuation

---

[96]For a while there will be no reference to n.

[97]The irreducibility of $E_{s,a,b}$ follows from the First Irreducibility Lemma.

[98]This was inspired by discussions with Walter Feit.

$Y = \infty$, is ramified in a splitting field $E_{s,a}(Z)$ over $k(Y)$, and $E_{s,a}(Z)$ is irreducible in $k(Y)[Z]$ and has no multiple roots in any overfield of $k(Y)$.

(IV.3*) If $p > 5$ then t can be chosen so that $1 < t < \frac{p+1}{2}$ and $\mathrm{GCD}(p + 1, t) = 1$, and for any such t, upon assuming $b = \frac{t}{t-1}$ and $s \equiv 0(t(p + 1 - t))$, we have $\mathrm{Gal}(E_{s,a}(Z), k(Y)) = A_{p+1}$.

The above two results with (Y, Z) changed to (X, Y), together with the results (IV.0′), (IV.1′), (IV.2′), and (IV.4′) with (n, Y, Z) changed to $(n + 1, X, Y)$,[99] may be summarized in the following

Summary about the primed roof polynomial. Let k be an algebraically closed field of characteristic $p \neq 0$, let a, b be nonzero elements in k, let n, s, t be positive integers with $n + 1 \not\equiv 0(p)$ and $n > t \not\equiv 0(p)$, and consider the monic polynomial of degree n in Y with coefficients in $k(X)$ given by

$$\widehat{F}_n' = h(Y)(Y + b)^p - aX^{-s}Y^t \quad \text{with } 0 \neq b \in k,$$

where $h(Y)$ is the monic polynomial of degree $n - p$ in Y with coefficients in k given by

$$h(Y) = \frac{(Y + n + 1)^{n+1-p} - Y^{n+1-p}}{(n + 1)^2}.$$

Then in the following cases $\widehat{F}_n'$ is irreducible in $k(Y)[Z]$, has no multiple roots in any overfield of $k(Y)$, and gives an unramified covering of L_k with the indicated Galois group $\widehat{G}_n' = \mathrm{Gal}(\widehat{F}_n', k(X))$.

(IV.1) If $n + 1 - p = t > 2 \neq p$ and $b = t$ and $s \equiv 0(p - 1)$ and $s \equiv 0(t)$, then $\widehat{G}_n' = A_n$.

(IV.2) If $n + 1 - p = t = 2$ and $p \neq 7$ and $b = t$ and $s \equiv 0(p - 1)$, then $\widehat{G}_n' = A_n$.

(IV.3) If $n = p + 1$ and $p > 5$, then t can be chosen so that $1 < t < \frac{p+1}{2}$ and $\mathrm{GCD}(p + 1, t) = 1$, and for any such t, upon assuming $b = \frac{t}{t-1}$ and $s \equiv 0(t(p + 1 - t))$, we have $\widehat{G}_n' = A_n$.

(IV.4) If $n + 1 - p = t$ and $p = 2$ and $b = t$ and $s \equiv 0(t)$, then $\widehat{G}_n' = S_n$.
Here CT is used only in the $p > 5$ case of (IV.2).

Referring to the summaries about the tilde polynomial and the roof polynomial and the primed roof polynomial, we have established the following four corollaries and we have arranged a proof of the First and the Second Corollaries independent of CT.

First Corollary. *For any $n \geq p > 2$, there exists an unramified covering of the affine line in characteristic p whose Galois group is A_n.*

Second Corollary. *For any $n \geq p = 2$, there exists an unramified covering of the affine line in characteristic p whose Galois group is S_n.*

Third Corollary. *Unramified coverings of the affine line in characteristic p with a few more Galois groups have been constructed.*

Fourth Corollary. *Let G be a quasi p-group. Assume that G has a subgroup H of index $p + 1$ such that H does not contain any nonidentity normal subgroup of G.[100] Also assume that p is not a Mersenne prime and p is different*

---

[99]Note that with these changes, if $n + 1 - p = t \not\equiv 0(p)$ then $\gamma(Y) = \frac{(Y+n+1)^{n+1-p} - Y^{n+1-p}}{(n+1)^2}$.

[100]Equivalently, G is isomorphic to a transitive permutation group of degree $p + 1$.

from 11 *and* 23. *Then there exists an unramified covering of the affine line in characteristic* p *having* G *as Galois group.*

It only remains to note that, in view of the said three Summaries, the above Forth Corollary follows from CTT, Special CDT, and the Corollary of the Fourth Irreducibility Lemma given in §21. Moreover, given any $n \geq p > 2$, as a definite alternative for getting an (A_n)-covering as asserted in the First Corollary without CT: if $p + 2 < n \not\equiv 0(p)$ then use (I.4) with $t = n - p$; if $n = p + 2$ and $p < 7$ then use (I.3) with $t = 2$; if $n = p + 2$ and $p \geq 7$ then use (IV.1) with $t = 3$ and $s = t(p - 1)$; if $n = p + 1$ and $p < 7$ then use (IV.2) with $t = 2$ and $s = p - 1$; if $n = p + 1$ and $p \geq 7$ then use (IV.3) with $t =$ the smallest odd prime factor of $\frac{(p-1)(p-3)}{2}$ and with $s = t(p + 1 - t)$, [note that in case of $n = 8$ and $p = 7$ this gives $t = 3$ and $s = 15$]; if $n \equiv 0(p)$ then use (II.1) with $t = 2$. Likewise, given any $n \geq p = 2$, as a definite alternative for getting an (S_n)-covering as asserted in the Second Corollary without CT: if $n \not\equiv 0(p)$ then use (I.5) with $t = n - p$; if $n \equiv 0(p)$ then use (IV.4) with $t = n + 1 - p$ and $s = t$.

The above cited three summaries are transcribed from my e-mail message to Serre dated 28 August 1989. This was only one out of the nearly a hundred e-mail and s-mail messages which flashed back and forth between him and me in the two year period September 1988 to September 1990. Indeed it has been a tremendous pleasure working with him. So once again my hearty MERCI MON AMI to Serre.

References

[A1]   S. S. Abhyankar, *On the ramification of algebraic functions*, Amer. J. Math. **77** (1955), 572–592.

[A2]   _____, *Local uniformization on algebraic surfaces over ground fields of characteristic* $p \neq 0$, Ann. of Math. **63** (1956), 491–526.

[A3]   _____, *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825–856.

[A4]   _____, *On the ramification of algebraic functions part* II: *Unaffected equations for characteristic two*, Trans. Amer. Math. Soc. **89** (1958), 310–324.

[A5]   _____, *Tame coverings and fundamental groups of algebraic varieties, Part* III: *Some other sets of conditions for the fundamental group to be abelian*, Amer. J. Math. **82** (1960), 179–190.

[A6]   _____, *Algebraic geometry for scientists and engineers*, Amer. Math. Soc., Providence, RI, 1990.

[A7]   _____, *Square-root parametrization of plane curves* (to appear).

[As]   M. Aschbacher, *Finite groups*, Cambridge University Press, Cambridge, 1986.

[B]   R. Brauer, *On the structure of groups of finite order*, Proc. Internat. Congress Math. **1** (1954), 209–217.

[Bu]   W. Burnside, *Theory of groups of finite order*, Cambridge University Press, Cambridge, 1911.

[BP]   W. S. Burnside and A. W. Panton, *Theory of equations*, Vols. I and II, Dublin, Hodges, Figgs and Co., London, 1904.

[C]   P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[Ca]   R. D. Carmichael, *Groups of finite order*, Dover, New York, 1956.

[Ch]   C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. **7** (1955), 14–66.

[CKS]   C. W. Curtis, W. M. Kantor, and G. M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups*, Trans. Amer. Math. Soc. **218** (1976), 1–59.

[D1]   L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig, 1958.

[D2]   _____, *On finite algebras*, Nachr. Akad. Wiss. Göttingen (1905), 358–393.

[F]   W. Feit, *On a class of doubly transitive permutation groups*, Illinois J. Math. **4** (1960), 170–186.

[Fr]   F. G. Frobenius, *Über auflösbare Gruppen* IV, Sitzungsberichte der Königlich Preußischen Akademie der Wissenchaften zu Berlin (1901), 1216–1230; reprinted as No. 63 on pages 189-203 of Band III of the "Gesammelte Abhandlungen" of Frobenius published by Springer-Verlag, New York, 1968.

[FT]   W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.

[G1]   D. Gorenstein, *Finite groups*, Chelsea Publishing Company, New York, 1980.

[G2]   _____, *Finite simple groups*, Plenum Press, New York, 1983.

[G3]   _____, *Classifying the finite simple groups*, Bull. Amer. Math. Soc. **14** (1986), 1–98.

[G4]   _____, *The classification of the finite simple groups, a personal journey: The early years*, A Century of Mathematics in America, Part I, Hist. of Math., vol. 1, Amer. Math. Soc., Providence, RI, 1988, pp. 447–476.

[H]   D. Hilbert, *Über die Irreduzibilität ganzzahligen Koefficienten*, Crelle J. **110** (1892), 104–129.

[HB]   B. Huppert and N. Blackburn, *Finite groups* I, II, III, Springer-Verlag, New York, 1982.

[J1]   C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Vill., Paris, 1870.

[J2]   _____, *Théorèmes sur les groupes primitifs*, J. Math. Pures Appl. **16**, 383–408.

[J3]   _____, *Sur la limite de transitivité des groupes non alternés*, Bull. Soc. Math. France **1**, 40–71.

[K1]   W. M. Kantor, *Rank 3 characterizations of classical geometries*, J. Algebra **36** (1975), 309–313.

[K2]   _____, *Homogeneous designs and geometric lattices*, J. Combin. Theory Ser. A **38** (1985), 66–74.

[KL]   W. M. Kantor and R. L. Liebler, *The rank 3 permutation representations of the finite classical groups*, Trans. Amer. Math. Soc. **271** (1982), 1–71.

[L]   M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. **54** (1987), 477–516.

[Mar]   B. Marggraff, *Über primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Dissertation, Giessen, 1892.

[Mas]   G. Mason, *The classification of quasi-thin simple groups*. (To appear).

[Mat]   E. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former, et sur les substitutions qui les laissent invariables*, J. Math Pures Appl., **18** (1861), 241–323.

[Mo]   E. H. Moore, *International Mathematics Congress, Chicago* 1893, New York, 1896, p. 210.

[N]   P. M. Neumann, *Some primitive permutation groups*, Proc. London Math. Soc. **50** (1985), 265–281.

[O]   M. E. O'Nan, *Normal structure of the one-point stabilizer of a doubly transitive permutation group* I *and* II, Trans. Amer. Math. Soc. **214** (1975), 1–74.

[R]   R. Ree, *Sur une famille de groupes de permutations doublement transitifs*, Canad. J. Math. **16** (1964), 797–820.

[S1]   J-P. Serre, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier **6** (1956), 1–42.

[S2]   _____, *Algebraic Groups and Class Fields*, Springer-Verlag, New York, 1988.

[St]   R. Steinberg, *Variations on a theme of Chevalley*, Pacific J. Math. **9** (1959), 875–891.

[Su1]   M. Suzuki, *On a class of doubly transitive groups*, Ann. Math. **75** (1962), 104–145.

[Su2]   _____, *Group Theory* I, II, Springer-Verlag, New York, 1986.

[V]   B. L. van der Waerden, *Modern Algebra* I, II, Frederick Ungar Publishing Co., New York, 1949.

[W]   J. H. M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), 349–352.

[Wi]   H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

[Z1]   H. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 17–44.

[Z2]   ——, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg **11**, 187–220.

APPENDIX BY J.-P. SERRE *

Harvard, November 15, 1990

Dear Abhyankar,

Here is my original proof that $PSL_2(\mathbf{F}_q)$ occurs for the equation $Y^{q+1} - XY + 1 = 0$.

I use "descending Galois theory," i.e., I construct *a priori* the Galois covering one wants. This is different from your "ascending" method; in particular, I don't need any characterization of $PGL_2(\mathbf{F}_q)$, or $PSL_2(\mathbf{F}_q)$, as a permutation group on $q + 1$ letters.

Notation. p is a prime; q is a power p^e of p.

$G = PGL_2(\mathbf{F}_q)$, i.e., the quotient of $GL_2(\mathbf{F}_q)$ by its center $\mathbf{F}_q^*$.

k is an algebraically closed field of characteristic p; all the curves I consider are over k.

Preliminary construction. I start from the obvious fact that G acts in a natural way (by "fractional linear transformations") on the projective line $\mathbf{P}_1$. In algebraic terms this means that G acts on $k(t)$ by $t \mapsto (at + b)/(ct + d)$. The quotient curve $\mathbf{P}_1' = \mathbf{P}_1/G$ is of course (Lüroth's theorem!) a projective line. Equivalently, the field of invariants of G in $k(t)$ is a purely transcendental field $k(x)$.

The first computational problem which arises is to write x explicitly. To do so, let us call (u, v) the homogeneous coordinates on $\mathbf{P}_1$, so that $t = v/u$. The invariant theory of $k[u, v]$ with respect to the action of G has been done long ago by Dickson. The basic covariants are the following homogeneous polynomials:

$$A(u, v) = uv^q - vu^q, \qquad B(u, v) = (uv^{q^2} - vu^{q^2})/A(u, v).$$

They are of degree $q + 1$ and $q^2 - q$ respectively. Hence the ratio

$$x = B(u, v)^{q+1}/A(u, v)^{q^2 - q}$$

is invariant by G. Its expression in terms of t is easy to find: if we write $A(u, v) = u^{q+1}a(t)$, $B(u, v) = u^{q^2 - q}b(t)$, we have

$$a(t) = t^q - t, \qquad b(t) = (t^{q^2} - t)/(t^q - t) = a(t)^{q-1} + 1$$

---

* The author expresses his appreciation to J. P. Serre for permission to include the following letter in this paper.

and

(*) $$x = b(t)^{q+1}/a(t)^{q^2-q} = (a(t)^{q-1} + 1)^{q+1}/a(t)^{q^2-q}.$$

This shows that x is a rational function of t of degree $q(q^2 - 1)$. Since it is invariant by G, which has order $q(q^2 - 1)$, Galois theory shows it *generates* the field of the G-invariant elements of $k(t)$. Hence we have found our parameter for $\mathbf{P}_1' = \mathbf{P}_1/G$.

Ramification. It is necessary to study the ramification in the Galois extension $k(t)/k(x)$ thus constructed. This amounts to looking for the fixed points of the action of G on the projective line $\mathbf{P}_1$. It is easy to see that these fixed points make up two orbits. Namely:

(a) The $\mathbf{F}_q$-rational points of $\mathbf{P}_1$. This orbit has $q + 1$ elements. The stabilizer of an element is a triangular subgroup ("Borel subgroup") of order $q(q - 1)$. Since that order is divisible by p, there is wild ramification.

The point of $\mathbf{P}_1'$ corresponding to this orbit is $x = \infty$.

(b) The "quadratic" points, i.e., the $\mathbf{F}_{q^2}$-rational points of $\mathbf{P}_1$ which are not rational over $\mathbf{F}_q$. There are $q^2 - q$ of them. The stabilizer of such a point is a cyclic group of order $q + 1$ ("nonsplit Cartan subgroup"). Since that order is prime to p, the ramification at such a point is tame.

The point of $\mathbf{P}_1'$ corresponding to this orbit is $x = 0$.

Hence we see that the covering of $\mathbf{P}_1'$ we get in this way is *ramified both at 0 and ∞, and nowhere else*. The next step is thus:

Getting rid of the ramification at 0 using Abhyankar's lemma. We consider the cyclic extension $k(X)$ of $k(x)$ defined by the equation $X^{q+1} = x$. By making a base change to that extension (i.e., by considering $k(t, X)/k(X)$) we get rid of the ramification at 0. Only the ramification at ∞ remains. Of course, one has to see what the new Galois group is. There are two cases:

(i) $p = 2$. The extensions $k(X)/k(x)$ and $k(t)/k(x)$ are disjoint. Hence the new Galois group is equal to the old one, namely $G = \mathrm{PGL}_2(\mathbf{F}_q)$, which happens to be equal to $\mathrm{PSL}_2(\mathbf{F}_q)$.

(ii) $p \neq 2$. The extensions $k(X)/k(x)$ and $k(t)/k(x)$ have a quadratic extension in common, namely $k(x^{1/2})$. Hence the new Galois group is $G' = \mathrm{PSL}_2(\mathbf{F}_q)$.

In both cases, one thus gets *a Galois extension of $k(X)$ with Galois group $\mathrm{PSL}_2(\mathbf{F}_q)$ which is ramified only at $X = \infty$.*

It remains to see that this extension is the same as the one you get by the equation $Y^{q+1} - XY + 1 = 0$.

An equation for the degrees $q+1$ extension. I go back to the $k(t)/k(x)$ extension with Galois group G. Let H be the triangular subgroup of G, of index $q + 1$. The fixed field $k(t)^H$ is an extension of degree $q + 1$ of $k(x)$ and we want to find a generator y for that field (which is also a purely transcendental field, of course). We may assume that H is the group of transformations $t \mapsto at + b$. This shows that the polynomial

$$y = a(t)^{q-1} = (t^q - t)^{q-1}$$

is invariant by H. Since its degree is $q(q - 1) = |H|$, the same argument as above shows that $k(y)$ is equal to $k(t)^H$.

I now write the equation of degree $q+1$ relating y to x. This is easy, since by construction, we have $x = (y+1)^{q+1}/y^q$, cf. $(*)$ above. We thus get the equation

$$(y+1)^{q+1} - xy^q = 0.$$

But I want to work on $k(X)$, with $x = X^{q+1}$. We have:

$$(y+1)^{q+1} - X^{q+1}y^q = 0.$$

Let me put $Y = (y+1)/yX$, i.e., $y = 1/(XY-1)$. The above equation becomes

$$Y^{q+1} - XY + 1 = 0,$$

and we are done.

This is the proof I found in 1988 when I started thinking about your problem. The first part is natural enough—and could indeed be applied to other groups, à la Nori. The second part (the search for the degree $q+1$ equation) is not; it looks like a happy coincidence, and I would not have found it if I had not known in advance your polynomial $Y^{q+1} - XY + 1$.

With best regards,
Yours

J-P. Serre

PS   The determination of the invariants of G in $k(t)$ is not new. I am almost certain to have seen it in print very long ago, as an elementary exercise in Galois theory. (Indeed: see Lang's *Algebra*, 2nd ed., p. 349, exercise 33, and also P. Rivoire, *Ann. Inst. Fourier* **6** (1955–1956), pp. 121–124.)

(Shreeram S. Abhyankar) MATHEMATICS DEPARTMENT, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907