ERRATA

Corrections to

THE GALOIS GROUP OF A POLYNOMIAL WITH TWO INDETERMINATE COEFFICIENTS

S. D. COHEN

Volume 90 (1980), 63–76

We make modifications to the results of [3], principally Theorem 2 and Corollary 3, to take account of an error in Lemma 5 which arises when wild ramification is involved. (This came to light following a query by M. Fried to whom I am grateful.) In fact, although some of the assertions of [3] conflict with known results, we show that our conclusions remain true (and can even be strengthened) under modified hypotheses. We also take advantage of the now complete classification of finite doubly transitive groups to simplify the details. In our discussion (which proceeds with the same notation) we can assume that p is a prime.

Now the proof of Lemma 5 is valid provided the cycle pattern μ is *tame*, i.e., provided $\mu_i = 0$ whenever $p \mid i$. When μ is wild the claim that necessarily $G(h, F\{t\})$ is cyclic is unjustifiable, see [2], §8, although further study may reveal what alternative deductions could be made. Simply observe here that then the p-Sylow group of $G(h, F\{t\})$ supplies non-trivial elements σ of G whose cycle lengths are powers of p and for which $\lambda(\sigma) \leqq \sum_{p \mid i} i\mu_i$. In particular, the validity of Lemma 5 and Corollary 6 is restored if the following sentence is added to their hypotheses. *Suppose that either* μ *is tame or* $\mu = (1^{(n-p)}, p^{(1)})$.

Clearly Lemma 7 and so Theorem 1 remain valid as stated. Indeed, by the above, $G = S_n$ whenever there exists $(\beta_1, \beta_2, \beta_3)$ in F^3 with $\mu(B) = (1^{(n-2)}, 2^{(1)})$ (even if $g(X)$, X^a and X^b are linearly dependent over $F(X^p)$, e.g. whenever $p = 2$). Thus, for example, if $p = 2$, n is odd and $f(X) = X^n + tX^2 + u$ then $G = S_n$.

Next, observe that the purported existence of an automorphism σ_i in Lemma 8 is actually only established when $\mu(\sigma_i)$ is tame or a p-cycle. (Note however from the proof that, if $p \nmid c$ then certainly $\mu(\sigma_4)$ is tame unless $g(X) = g_1(X^p)X^{a^*}$, $p \nmid a$). Consequently, the conclusion "$G \nsubseteq A_n$" of Lemma 9 is conditional on one of the $\mu(\sigma_i)$ being tame (or, if $p = 2$, a transposition) as well as odd.

In the revised version of Theorem 2 which follows, the condition $p \nmid (a, n)$ is replaced by the condition $p \nmid (a(n - a), c)$ (which although generally stronger does allow the possibility that $p \mid (a, n)$ provided

$p \nmid c$). Following from the failure of Lemma 9 in some cases (e.g. whenever $p = 2$), we cannot always distinguish between $G = S_n$ and $G = A_n$ but the main conclusion that exceptions occur only when $a = n - 1$ or $c = 1$ remains valid.

THEOREM 2. *Suppose that f is given by* (1) *with $a = n, b = 0$ and $p \nmid (a(n - a), c)$. Suppose $G \neq S_n$. Then one of the following* (i)-(v) *holds.*

(i) $a, c \in \{1, n - 1\}$,

(ii) $a = n - 1$ *and* $p \mid (n, c)$,

(iii) $c = 1$ *and* $p \mid a(n - a, a - 1)$,

(iv) $g(X) = g_1(X^p)X^{a^*}$, $p \nmid a$,

(v) $G = A_n$ *and either* $p \mid (c, n)$ *with n even and a odd or* $p \mid a(n - a)$ *with c odd and also, if $p \nmid n$, n odd.*

Proof. Assume $A_n \not\subseteq G$. By Theorem 1 we can suppose that either $p \mid a$ or $p \mid (n(n - a), c(c - a))$. Suppose $p \nmid c (\neq 1)$ and (iv) does not hold. Then, as in [3], σ_4 is a c-cycle and G is $(n - c + 1)$-ply transitive. Hence by Corollary 5.4 of [1] (now unconditional since Hypothesis (S) is accepted as proven), G cannot be 6-transitive and so $c \geqq n - 4$. Moreover, the only 4 and 5 transitive groups are the Mathieu groups $M_n (n = 11, 12, 23, 24)$ and these possess no cycles of length $n - 3$ or $n - 4$, [5]. Thus $c \geqq n - 2$ and so either $p \mid a (= n - 1)$ and $c = n - 2$ or $a = c$. In the former case since F can be assumed to be algebraically closed we can suppose $g(X) = X^n + X^{n-2}$ and then $\mu(g(X) + X^{n-1} - 1) = (1^{(n-2)}, 2^{(1)})$ (the repeated factor being $(X + 1)^2$) while if $a = c = n - 2$ (with $p \nmid n - 2$), then σ_3 is a transposition. In either case $G = S_n$. Hence if $p \nmid c$ then $a = c = n - 1$. Similarly, the assumption $p \nmid a(n - a)$ yields $a = n - 1$ or $a = c = 1$.

Note finally that here one of the $\mu(\sigma_i)$ of Lemma 8 is odd and tame unless the conditions in (v) apply.

To demonstrate that $G = S_n$ is a possible conclusion even when $p = 2$ we supplement Theorem 2 with

THEOREM 2′. *Suppose f is given by* (1) *with $p < n - 1$ and that either $c = p$ or $p \nmid n$ with $a = p$ or $n - p$. Then $A_n \subseteq G$. Indeed, if $p = 2$, then $G = S_n$.*

Proof. Consideration of one of σ_2, σ_3 or σ_4 produces the existence of a p-cycle in G and the result follows from Theorem 13.9 of [10] provided $p < n - 2$, while from the list on p. 8 of [1], $c = n - 2 = p$, a prime, for example, is impossible for 3-transitive groups.

The scope of these results could be enlarged by considering specific "non-awkward" g or by employing Theorem 13.10 of [10]

(including more recent improvements such as in [7]) or by using the classification of doubly transitive groups to improve the lower bound given in Theorem 15.1 of [10] for the minimal degree of such a group.

For Corollary 3 (regarding trinomials) we additionally assume that $p \nmid a(n-a)$ (but not necessarily that $p \mid n$ as in [8]) and supplement it with a special case of Theorem 2'.

COROLLARY 3. *Let* $f(X) = X^n + tX^a + u$, *where* $(a, n) = 1$.

(i) *Suppose that* $p \nmid a(n-a)$ *and also that* $p \nmid n$ *if* $a = 1$ *or* $n-1$. *Then* $A_n \subseteqq G$. *Indeed, for* p *odd,* $G = S_n$ *unless* $2p \mid n$.

(ii) *Suppose that* $p < n-1$ *and* $a = p$ *or* $n-p$. *Then* $A_n \subseteqq G$ *with* $G = S_n$ *if* $p = 2$.

We comment here that existing results already called for modification of the original Corollary 3. For example, the trinomial discriminant formula [6] implies that if $p \mid (n-a)$ and n is even then $G \subseteqq A_n$ and, in particular, Uchida [9] showed that, if $f(X) = X^{11} + tX^2 + u$, then $G = M_{11}$ when $p = 3$ (although, as mentioned earlier $G = S_{11}$ when $p = 2$).

Finally, although the original proof of Theorem 12 is lacking in some cases (for example, when $b = 0$ and $p \mid (n-a)(a-b)b$, we can show that it remains valid as stated. Indeed (as is desirable in view of the possibility that Theorem 2 yields only $A_n \subseteqq G$), we can justify the conclusion of Theorem 12 *assuming only that* $A_n \subseteqq G$ (rather than $G = S_n$). This flows from the improved version of Lemma 11 in [4] in which it is assumed only that $A_n \subseteqq G$ with $|G| > 3$ for the same conclusions to hold. Also, in [4] it is proved that if (15) holds with $|G| > 3$ (and $n \neq 4$, if $q = 2$), then necessarily $f(X)$ divides a polynomial of the form $Xg_1^q(X) - \alpha g_2^q(X)$, where here $\alpha \in F(t, u)$. Indeed, aside from a factor X^m, say, f itself is of this form (otherwise a zero of f is algebraic over $F(t)$) which is clearly impossible. The remaining cases of small n and p can be cleared up separately using Lemma 5 and its extensions. In particular, $G = A_3$ is impossible. We omit the details.

REFERENCES

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

2. J. W. S. Cassels and A. Frohlich (Editors), *Algebraic Number Theory*, Academic Press, New York and London, 1967.

3. S. D. Cohen, *The Galois group of a polynomial with two indeterminate coefficients*, Pacific J. Math., **90** (1980), 63-76.

4. S. D. Cohen and W. W. Stothers, *The Galois group of* $f(x^r)$, submitted for publication.

5. G. Frobenius, *Uber die Charaktere der mehrfach transitiven Gruppen*, S. B. Akad. Berlin, **1904**, 558-571.
6. J. Heading, *The discriminant of an equation of* nth *degree*, Math. Gaz., **51** (1967), 324-326.
7. C. E. Praeger, *On elements of prime order in primitive permutation groups*, J. Algebra, **60** (1979), 126-157.
8. J. H. Smith, *General trinomials having symmetric Galois group*, Proc. Amer. Math. Soc., **63** (1977), 208-212.
9. K. Uchida, *Galois group of an equation* $X^n-aX+b=0$, Tohoku Math. J., **22** (1970), 670-678.
10. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London, 1964.

Correction to

THE TYPESET AND COTYPESET OF A RANK 2 ABELIAN GROUP

PHILLIP SCHULTZ

Volume 78 (1978)

Professors Vinsonhaler and Wickless have pointed out several errors in my paper, of which one at least is irreparable.

The proof of admissibility in Section 6 fails to show that for arbitrary coprime integers a and b, the group element $ax + by$ has the required height. In fact the argument in this section is incompatible with a Lemma of Dubois [1].

Vinsonhaler and Wickless have found a counterexample, similar to one in [1], which shows that my main theorem, Proposition 4, is false. Their results are to appear in [2].

REFERENCES

1. D. W. Dubois, *Applications of analytic number theory to the study of types sets of torsion free Abelian groups, I*, Pub. Math., **12** (1965), 59-63.
2. C. Vinsonhaler and W. J. Wickless, *The cotypeset of a torsion free Abelian group of rank two*, (to appear).

Correction to

NEW EXPLICIT FORMULAS FOR THE nTH DERIVATIVE OF COMPOSITE FUNCTIONS

PAVEL G. TODOROV

Volume 92 (1981), 217-236

(1) page 219, line 8 from below:

The printer has printed:

"Funktion und insbeson, inbesondere dere für die der Umkehrfunktion".

It must be:

"Funktion und insbesondere für die der Umkehrfunktion"

(2) page 234, line 5 above:

The denominator in the formula (61) has been printed: $(u'')^{2n-}$

It must be: $(u'')^{2n-3}$

(3) page 234, line 9 above:

It was printed:

$$a_{31}(n-1)\frac{u'''}{3!}$$

It must be:

$$a_{31}(n-1)\frac{u''''}{3!}$$

Correction to

ON THE ISOLATION OF ZEROES OF AN ANALYTIC FUNCTION

DOUGLAS S. BRIDGES

Volume 96 (1981), 13-22

On correcting the proofs of [1], I realized that the results of [1] preceding Proposition 1 do not enable us to take the first step in the proof of that Proposition. This gap in the proof can be filled easily by an application of the following additional lemma.

LEMMA. *Let f be differentiable and not identically zero on $\bar{B}(0, 1)$. Let ν be a positive integer, $0 < \rho < 1/2$, $r = \rho\sum_{k=0}^{\nu-1}(1-\rho)^k$, and $0 < \varepsilon < r$. Then there exists s such that $r - \varepsilon < s < r$ and* $\inf\{|f(z)|: |z| = s\} > 0$.

Proof. We argue by induction on ν, the case $\nu = 1$ having been dealt with in Lemma 2 of [1]. Suppose, then, that our Lemma obtains when $\nu = n - 1 > 0$, and consider the case $\nu = n$. Choose a positive integer m so that

$$t = r|e^{2\pi i/m} - 1| < \frac{1}{2}(1-r)$$

and define $\zeta_k = re^{2k\pi i/m}$ $(k = 0, \cdots, m-1)$. It is routine to verify that

the balls $\bar{B}(\zeta_k, t)$ lie in $\bar{B}(0, 1)$ and cover $\{z: |z| = r\}$; that $|\zeta_{k+1} - \zeta_k| = t$ for each k; and that there exists $d > 0$ such that $z \in \bigcup_{k=0}^{m-1} \bar{B}(\zeta_k, t)$ whenever $r - d \leqq |z| \leqq r + d$. Now

$$\begin{aligned}
&\rho \sum_{k=0}^{n-2} (1 - \rho)^k + 1 - 2r \\
&\quad = \rho \sum_{k=0}^{n-2} (1 - \rho)^k + 1 - 2\rho - 2\rho(1 - \rho) \sum_{k=0}^{n-2} (1 - \rho)^k \\
&\quad = (1 - 2(1 - \rho))\rho \sum_{k=0}^{n-2} (1 - \rho)^k + 1 - 2\rho \\
&\quad = (1 - 2\rho)\Big(1 - \rho \sum_{k=0}^{n-2} (1 - \rho)^k\Big) \\
&\quad > 0 ,
\end{aligned}$$

so that

$$\rho \sum_{k=0}^{n-2} (1 - \rho)^k + 1 - r > r ,$$

and therefore the balls $B(\zeta_k, 1 - r)$ each intersect $B(0, \rho \sum_{k=0}^{n-2} (1 - \rho)^k)$. The induction hypothesis now ensures that f is not identically zero on $\bar{B}(\zeta_k, 1 - r)$. Applying Lemma 2 of [1], we now compute r_k so that $t < r_k < (1/2)(1 - r)$ and $\inf\{|f(z)|: |z - \zeta_k| = r_k\} > 0$ $(0 \leqq k \leqq m - 1)$. It follows from Lemma 3 of [1] that either $\inf\{|f(z)|: z \in \bigcup_{k=0}^{m-1} \bar{B}(\zeta_k, r_k)\} > 0$, in which case $\inf\{|f(z)|: |z| = s\} > 0$ for any s with $r - \min(d, \varepsilon) < s < r$; or there exist finitely many points $z_1, \cdots, z_M$ of $\bigcup_{k=0}^{m-1} B(\zeta_k, r_k)$ and an operation $\delta: \boldsymbol{R}^+ \to \boldsymbol{R}^+$ such that $|f(z)| \geqq \delta(\alpha)$ whenever $\alpha > 0$, $z \in \bigcup_{k=0}^{m-1} \bar{B}(\zeta_k, r_k)$ and $|z - z_j| \geqq \alpha$ for each j. In the latter case, to complete the proof we need only choose s so that $r - \min(d, \varepsilon) < s < r$ and $s \neq |z_j|$ for each j.

REFERENCE

1. D. S. Bridges, *On the isolation of zeroes of an analytic function*, Pacific J. Math.

Correction to

REGULAR FPF RINGS

S. PAGE

Volume 79 (1978), 169-176

In [2] Proposition 3 states that for a left FPF left nonsingular ring any left ideal is essential in a direct summand of the ring. Unfortunately the proof is lacking as was pointed out by E. P.

Armendariz. The proof given only works for two sided ideals. The final results of the paper are in fact valid. The arguments of [2] do characterize the left self-injective left FPF regular rings. It is also easy to see (as is pointed out in [2]) that a strongly regular left FPF is left self-injective. In [3] it is shown that if R is nonsingular and left FPF, then $Q(R)$, the maximal left quotient ring is also left FPF. So we know the structure of the maximal quotient ring. We will show that, if R is a left FPF regular ring, Proposition 3 does hold.

In what follows R is a ring with zero singular left ideal and maximal left quotient ring Q. We first show that $Q \otimes_R Q \cong Q$ by establishing the following lemma:

LEMMA A. *Let R be a left nonsingular left* FPF *ring and let $q \in Q$. Then $R + Rq$ embeds in a finitely generated free module.*

Proof. An idempotent e in Q is called abelian if for R-submodules I and J of Qe such that $I \cap J = 0$, $\mathrm{Hom}_R(I, J) = 0$. Now each idempotent of Q can be written as a finite sum of orthogonal abelian idempotents because Q is a self-injective regular ring of bounded index. The injective hull of Rq is Qe for some idempotent e. Let $e = \sum_{i=1}^{n} e_i$, where the e_i's are abelian and orthogonal. Clearly, $R + Rq$ embeds in $R(1 - e) \oplus \sum_{i=1}^{n}(Re_i + Rqe_i)$. Next look at $Re_i + Rqe_i \subset Qe_i$. We will show that $Re_i + Rqe_i$ embeds in a free module for each i. To this end, for convenience, we will assume e is abelian. Now we can reduce to the case where Re is faithful. To do this note that the left annihilator of $Re + Rqe$, ${}^{\perp}(Re + Rqe)$, is ${}^{\perp}((Re + Rqe)R)$, a two sided ideal. The two sided version of Proposition 3 of [2] implies that $R \cong R_1 \times R_2$ where $(Re + Rqe)R$ is essential in R_1. We can, therefore, assume without loss of generality that $R = R_1$. This makes Re faithful and so $Re + Rqe$ is a generator. This gives the existence of functions $f_1, \cdots, f_K$, to R so that $R = \sum_{i=1}^{K} \text{Image } f_i$. Let $W = \bigcap_{i=1}^{K} \ker f_i$. Let F be the sum of K copies of R, and $Q(F)$ the canonical hull of F. Let f be the map of $Re + Rqe$ to F given by f_i on the ith coordinate. We have $W = \ker f$. Since everything in sight is nonsingular, W is not essential in $Re + Rqe$. Let $W \oplus U$ be essential in $Re + Rqe$. Since $1 \in \sum_{i=1}^{K} \mathrm{Im}\, f_i$, there exists r_1, r_2 in R so that for $w \neq 0$ in W, $wf_i(r_1e + r_2qe) \neq 0$ for some i. Also since the image of U is essential in $\mathrm{im}\, f$, we see that $Wf(U) \neq 0$, in $Q(F)$. It follows, because all modules under consinderation are nonsigular, that for some non zero submodule $W_1 \subset W$, $\mathrm{Hom}_R(W, U) \neq 0$, which contradicts the fact that e was abelian, unless $W = 0$. The fact that $W = 0$ implies that f_i's give rise to an embedding. Finally, treat $R(1 - e)$ in the same way.

THEOREM. *Let R be a left nonsingular left* FPF *ring. Then Q is flat as a left R module and $Q \otimes Q \cong Q$.*

Proof. Lemma A gives the essential ingredients to apply the proof of Theorem 5.17 [1].

PROPOSITION. *Let R be a regular left* FPF *ring. Let $e = e^2 \in Q$. Then Re is a projective R module.*

Proof. By Theorem 2.8 of [4] it suffices to show $Q \otimes_R Re$ is a Q projective. Now we have $0 \to Re \to Q$ exact and Q is flat over R, so $0 \to Q \otimes Re \to Q \otimes Q$ is exact. The isomorphism $Q \otimes Q \cong Q$ gives $Q \otimes Re \cong Qe$, and hence is Q projective.

COROLLARY. *For any idempotent $e \in Q$, $Re \cap R$ is a summand of R.*

Proof. The sequence $0 \to Re \cap R \to R \to R(1 - e) \to 0$ splits.

We can now prove Proposition 3 of [2] for regular FPF rings. If L is a left ideal of R, then L is essential in a summand Qe of Q. Hence L is essential in Re, hence essential in $Re \cap R$, a summand of R.

REFERENCES

1. K. R., Goodearl, *Ring Theory*, Mono. and Text in pure and applied math. 33, Marcel Dekker, New York.
2. S. Page, *Regular FPF Rings*, Pacific J. Math., **79**, No. 1, (1978), 169-176.
3. ———, *Semi-prime and non-singular FPF rings, to appear.*
4. F. L. Sandomierski, *Nonsingular rings*, Proc. Amer. Math. Soc., **19** (1968), 225-230.