ACTA ARITHMETICA
XX (1972)

The distribution of polynomials over finite fields, II

by

STEPHEN D. COHEN (Glasgow)

1. Introduction. Let $k = \mathrm{GF}(q)$ be the finite field of order $q = p^b$. For fixed polynomials $f(x), g(x)$ in $k[x]$, the author proved in [1] an estimate, in terms of the Galois group of $f(x) - tg(x)$, t an indeterminate, over $k(t)$, for the number of polynomials of the form $f(x) - ag(x)$ $(a \in k)$ which factorise into irreducible polynomials in $k[x]$ of prescribed degree. In a similar way, if $(f_1, g_1), \ldots, (f_s, g_s)$ are s fixed polynomial pairs in $k[x]$, an estimate, in terms of the Galois group of $(f_1 - tg_1) \ldots (f_s - tg_s)$, for the number of a in k for which $f_i - ag_i$ has prescribed factorisation simultaneously for each $i = 1, \ldots, s$ can be stated (Section 2). This paper contains some of the consequences of this result.

In particular, if $s = 2$, say, it is shown that the elements a in k for which $f_1 - ag_1$ has certain prescribed factorisation need not be uniformly distributed among the elements a in k for which $f_2 - ag_2$ also has prescribed factorisation even when f_1/g_1 and f_2/g_2 are not functionally related in any way.

2. Notation and general results. If E is a Galois extension of a field F, then $G(E, F)$ will denote the Galois group of E over F.

Let $Q(x)\,(= Q(x, t))$ be a separable polynomial over $k(t)$ (t an indeterminate) of degree n with splitting field K and Galois group $G = G\big(K, k(t)\big)$. Let k' $(= \mathrm{GF}(q^d)$ for some $d)$ be the algebraic closure of k in K. For any subset H of G, H^* will denote the subset of elements in H whose fixed field in K contains no element of k' not already in k. The first lemma follows from Lemma 1 of [1].

LEMMA 1. *If H is a subgroup of G, then*

$$|H^*| = \big(\varphi(d)/d\big)|H|,$$

where φ is Euler's function.

Now regard G as a group of permutations of the roots of $Q(x) = 0$, i.e. as a subgroup of S_n, the symmetric group on n letters. For any cycle pattern λ of S_n, put $G_\lambda = \{\sigma \in G$ having cycle pattern $\lambda\}$. Also, for any unramified first degree prime $t - a$ in $k(t)$, let $A(a)$ be the Artin symbol

for $t-a$, a unique conjugacy class in G. Then the proof of Theorem 1 in Section 4 of [1] yields Lemma 2 below. In fact, there we assumed that $Q(x) = f(x) - tg(x)$ with f, g in $k[x]$, but no use of this fact was made in proving the assertion of the theorem, except that the number of first degree ramified primes in K was $\leqslant (n!)^2$.

LEMMA 2. *If K contains at most l $(= l(n))$ first degree ramified primes, then the number of a in k such that $A(a)$ has cycle pattern λ is*

$$\frac{|G_\lambda^*|}{|G^*|}q + O(q^{1/2}),$$

where the implied constant depends only on n and l.

Notes. (i) l is bounded by a constant depending only on n and the degree of Q in t.

(ii) Recall that Lemma 2 is established by a method which, in part, follows a section of the proof of the Čebotarev Density Theorem in the algebraic number field case. As stated, it is sufficient for our purposes, but M. Fried has informed the author (written communication) that by following the complete proof of the Čebotarev theorem, we can improve the assertion of Lemma 2 to yield an estimate for the number of a in k with the same $A(a)$.

From now on we shall let $r(x) = f(x)/g(x)$ (more generally, $r_i(x) = f_i(x)/g_i(x)$ for any subscript i) be a rational function in $k(x)$ with f, g relatively prime, non-zero polynomials, not both constant, such that $r(x) \neq u(x^p)$ for any other rational function u in $k(x)$. (Thus all extensions considered are separable.) The degree of $r(x)(= \deg r)$ is $\max(\deg f, \deg g)$.

Now specialise the earlier discussion to the case in which $Q(x,t) = \prod_{i=1}^{s} (f_i(x) - tg_i(x))$ where the $r_i = f_i/g_i$, $i = 1, \ldots, s$, are rational functions with the above conventions. Then $n = \sum_{i=1}^{s} \deg r_i$. Further any $\sigma \in G$ has a cycle pattern which may be written as a product $\lambda_1 \ldots \lambda_s$, where λ_i permutes the roots of $f_i(x) - tg_i(x) = 0$, $i = 1, \ldots, s$.

For any polynomial $h(x)$ of degree m in $k[x]$, we shall say that $h(x)$ has cycle pattern $\lambda = 1^{a_1}, \ldots, m^{a_m}$ if, in the prime factorisation of $h(x)$ in $k(x)$, there are precisely a_d irreducible polynomials of degree d, $d = 1, \ldots, m$. As in [1], we shall identify corresponding cycle patterns of polynomials and automorphisms. The connection between the two is apparent from the following extension of Lemma 5 of [1]. The proof is exactly similar and is omitted.

LEMMA 3. *Suppose that $f_i(x) - ag_i(x)$ $(a \in k)$ is square-free, $i = 1, \ldots, s$. Then it has cycle pattern λ_i, for each $i = 1, \ldots, s$, if and only if $A(a) \subseteq G_\lambda^*$, where $\lambda = \lambda_1 \ldots \lambda_s$.*

As remarked in the proof of Theorem 5 in [1], Lemma 3 can be extended to assert that if $t-a$ is ramified in K and we let $A(a)$ denote any of the (not now unique) conjugacy classes of G possessing the defining property of the Artin symbol then $r_i(x)$ $(1 \leqslant i \leqslant s)$ takes the value $a \in k$ for some $x \in k$ if any $\sigma \in A(a)$ fixes some root of $f_i(x) - tg_i(x) = 0$.

From Lemmas 2 and 3 (with $l = (n!)^2$ in Lemma 2), we obtain immediately the following extension of Theorem 1 of [1].

THEOREM 1. *With the above notation and conventions, $\pi_\lambda(r_1, \ldots, r_s, q)$, where $\lambda = \lambda_1 \ldots \lambda_s$, the number of a in k for which $f_i(x) - ag_i(x)$ has cycle pattern λ_i, for each $i = 1, \ldots, s$, is given by*

$$\pi_\lambda(r_1, \ldots, r_s, q) = \frac{|G_\lambda^*|}{|G^*|}q + O(q^{1/2}),$$

where the implied constant depends only on n.

3. Uniform distribution. For given rational functions $r_1, \ldots, r_s$ and cycle pattern $\lambda = \lambda_1 \ldots \lambda_s$, we wish to compare $\pi_\lambda(r_1, \ldots, r_s, q)$ with the individual $\pi_{\lambda_i}(r_i, q)$, $i = 1, \ldots, s$, using the estimates of Theorem 1. For *uniform distribution for λ*, we require

$$\pi_\lambda(r_1, \ldots, r_s, q) = \Big\{\prod_{i=1}^{s} \pi_{\lambda_i}(r_i, q)\Big\} q^{1-s} + o(q),$$

for fixed n. However, this need not occur. To investigate this phenomenon we put $s = 2$ in Theorem 1 for simplicity. Further, we shall use the subscript i $(i = 1, 2)$ in G_i, k_i, etc. to denote the situation described in Theorem 1 with $Q = f_i - tg_i$, $i = 1, 2$.

Then certainly G is a subgroup of the direct product $G_1 \times G_2$. Further, if r_1, r_2 are uniformly distributed for each $\lambda = \lambda_1\lambda_2$, then it is clear from Theorem 1 that, for large q, we must have

$$G^* = G_1^* \times G_2^*, \tag{3.1}$$

and, conversely, the truth of (3.1) implies that r_1, r_2 are uniformly distributed for all λ. However, (3.1) is equivalent to the two statements

$$G = G_1 \times G_2 \tag{3.2}$$

and

$$k' = k_1'(k_2') \text{ and } k_1' \cap k_2' = k, \quad \text{i.e. } k' \cong k_1' \otimes_k k_2', \tag{3.3}$$

using tensor product notation. In fact, by Galois theory,

$$G/G_1 \cong G(K, K_1) \cong G(K_2, K_1 \cap K_2),$$

so that (3.2) is equivalent to the fact that $G_2 \cong G(K_2, K_1 \cap K_2)$ which, in turn, is the same as

$$K_1 \cap K_2 = k(t), \quad \text{i.e. } K \cong K_1 \otimes_{k(t)} K_2, \tag{3.4}$$

since $K = K_1(K_2)$. To summarise, statement (3.1) is equivalent to statements (3.3) and (3.4).

Of course, (3.4) never holds when r_1, r_2 are a *composite pair*, meaning that there exist rational functions r, r_3, r_4 with $\deg r > 1$ such that $r_1 = r(r_3)$ and $r_2 = r(r_4)$. Moreover, (3.4) may quite easily remain false even when r_1, r_2 are not a composite pair. For example, if q is odd, take $r_1(x)$ to be the quartic polynomial $x^4 + ax^2 + bx$ $(b \neq 0)$ and $r_2(x)$ to be the function $(x^3 + 8ax^2 + 16a^2x - 64b^2)/64x$, so that $f_2(x) - tg_2(x)$ is the cubic resolvent of $r_1(x) - t$. Hence, in fact, $K_1 \cap K_2 = K_1$. Furthermore, it is possible for (3.4) to be true and yet (3.3) and hence (3.1) to be false (see example below).

EXAMPLE. As a concrete example, we consider a polynomial r_1 which is such that the a in k for which $f_1 - ag_1$ have a given cycle pattern are not uniformly distributed among the quadratic residues in k. We shall ignore error terms throughout. Thus assume q is odd and put $r_1(x) = x^4 + 4x^3 + 27$ and $r_2(x) = x^2$, so that r_1, r_2 are not a composite pair. Let $a(q)$ (respectively, $b(q)$) be the number of quadratic residues a in k for which $r_1(x) - a$ is irreducible (respectively, a is a value of the function $r_1(x)$, $x \in k$). Then, since $G_1^* = S_4$ and $G_2^* = S_2$, the truth of (3.1) would imply that $a(q) = (1/8)q$, $b(q) = (5/16)q$. But notice that $K_2 = k(y)$, where $y^2 = t$ and discriminant $(r_1(x) - t) = -256t(t-27)^2 = (16i(t-27)y)^2$, where $i^2 = -1$, so that $16i(t-27)y \in K_1$.

Case (i). $q \equiv 1 \pmod 4$. Here $i \in k$ so that $K_1 \cap K_2 = K_2$. In fact $G = G^*$ is that subset of $G_1 \times G_2$ given by

$$G^* = \{\sigma_1\sigma_2 \in S_4 \times S_2 \colon \sigma_1, \sigma_2 \text{ are both even or both odd}\}.$$

It follows that $a(q) = 0$ and $b(q) = (3/8)q$.

Case (ii). $q \equiv -1 \pmod 4$. Here $i \notin k$, K_1 or K_2 but $i \in K$. Hence (3.4) (and so (3.2)) holds but (3.3) (and so (3.1)) is false, since $k' = k(i) \neq k_1'(k_2') = k$. In this case,

$$G^* = \{\sigma_1\sigma_2 \in S_4 \times S_2 \colon \text{one of } \sigma_1, \sigma_2 \text{ is odd and one even}\},$$

so that $a(q) = \frac{1}{4}q = b(q)$.

Finally, note that if $r_1(x) = -(x^4 + 4x^3 + 27)$, then a similar situation to that described for $q \equiv 1 \pmod 4$ in the above example prevails for all q with q odd.

4. The value set of a function. Let $k^+ = k \cup \{\infty\}$. For any function $r = f/g \in k(x)$, it is convenient to extend r to be a function from $k^+ \to k^+$ by putting

$$r(\theta) = \infty, \quad \text{if} \quad g(\theta) = 0, \ \theta \in k$$

and

$$r(\infty) = \begin{cases} \infty, & \text{if} \quad \deg f > \deg g, \\ a/b, & \text{if} \quad \deg f = \deg g = m \text{ and} \\ & \quad f = ax^m + \ldots, \ g = bx^m + \ldots, \\ 0, & \text{if} \quad \deg f < \deg g. \end{cases}$$

For any subset A of k^+, $\mathscr{I}(r, A)$, the *value set* of r in A is the set of non-infinite values of $r(\beta)$ for β in A, i.e. $\mathscr{I}(r, A) = \{\alpha \in k\colon \exists \beta \in k^+ \text{ with } r(\beta) = \alpha\}$.

In this section, we extend the results of Section 5 of [1] by investigating to what extent a function is determined by $\mathscr{I}(r, k^+)$. (In [1], we considered the consequences of $\mathscr{I}(r, k^+) = k = \mathscr{I}(x, k)$.) Now, of course, if $r(x)$ is a *permutation function in* k^+, for which $\mathscr{I}(r, k^+) = k$ (e.g. if $r(x) = (ax+b)/(cx+d)$, $ad - bc \neq 0$), then for any functions r_1, r_2, $\mathscr{I}(r_1(r_2), k^+) \subseteq \mathscr{I}(r_1(r), k^+)$. Conversely, we may ask: does

$$\mathscr{I}(r_1, k^+) \subseteq \mathscr{I}(r_2, k^+) \tag{4.1}$$

imply that, for some functions r, r_3, r_4 with r a permutation function,

$$r_1 = r_3(r_4) \quad \text{and} \quad r_2 = r_3(r) \ ? \tag{4.2}$$

It turns out, that instead of (4.1), it is more convenient to discuss the slightly weaker condition

$$\mathscr{I}^-(r_1, k) \subseteq \mathscr{I}(r_2, k^+), \tag{4.3}$$

where for any $A \subseteq k^+$, $\alpha \in \mathscr{I}^-(r, A)$ if and only if there exists $\beta \in A$ with $r(\beta) = \alpha$ and β not a repeated root of $r(x) = \alpha$, i.e. $r'(\beta) \neq 0$. Certainly (4.1) implies (4.3). The reverse implication may or may not be true, although in the case of r a polynomial and $q = p$, Fried [2] has conjectured that, for large p,

$$\mathscr{I}^-(r_1, k) \subseteq \mathscr{I}(r_2, k) \quad \text{and} \tag{4.4}$$
$$\mathscr{I}^-(r_2, k) \subseteq \mathscr{I}(r_1, k) \Rightarrow \mathscr{I}(r_1, k) = \mathscr{I}(r_2, k).$$

We first find a sufficient condition for (4.3) to hold similar to that of Fried ([2], p. 100) in his discussion of integral polynomials, although the method of proof is different. Let the situation of Section 3 (with $s = 2$) prevail and let the roots of $f_1 - tg_1$ and $f_2 - tg_2$ in K be $y_1, \ldots, y_{n_1}$ and $z_1, \ldots, z_{n_2}$, respectively, where $n_i = \deg r_i$, $i = 1, 2$ so that $n = n_1 + n_2$.

THEOREM 2. *In the described notation, condition* (4.3) *holds if*

$$\bigcup_{i=1}^{n_1} G^*(K, k(y_i)) \subseteq \bigcup_{i=1}^{n_2} G^*(K, k(z_i)), \tag{4.5}$$

while for each $n = 1, 2, 3, \ldots$, *there exists a constant* $c = c(n)$ *such that if* $q > c$ *then* (4.3) *implies* (4.5).

Proof. The fact that (4.5) implies (4.3) follows immediately from Lemma 3 and the subsequent remark.

Suppose now that (4.3) holds. Then $\mathscr{I}^-(r_1, k) \cap \mathscr{I}(r_2, k^+) = \mathscr{I}^-(r_1, k)$ and so since $|\mathscr{I}(r_i, k^+) - \mathscr{I}^-(r_i, k)| \leqslant n$, by Theorem 1, for some $d = d(n)$, we have

$$\left| \frac{\left| \bigcup_{i=1}^{n_1} \bigcup_{j=1}^{n_2} G^*(K, k(y_i, z_j)) \right|}{|G^*|} - \frac{\left| \bigcup_{i=1}^{n_1} G^*(K_1, k(y_i)) \right|}{|G_1^*|} \right| \leqslant dq^{-1/2}. \tag{4.6}$$

We shall show later that

$$\frac{\left| \bigcup_{i=1}^{n_1} G^*(K_1, k(y_i)) \right|}{|G_1^*|} = \frac{\left| \bigcup_{i=1}^{n_1} G^*(K, k(y_i)) \right|}{|G^*|}. \tag{4.7}$$

Since $G^* \subseteq S_n$, so that $|G^*| \leqslant n!$, it follows from (4.6) and (4.7) that, if $q > c(n) = d^2(n!)^2$, then the left side of (4.6) is actually 0 and so

$$\bigcup_{i=1}^{n_1} \bigcup_{j=1}^{n_2} G^*(K, k(y_i, z_j)) = \bigcup_{i=1}^{n_1} G^*(K_1, k(x_i)), \tag{4.8}$$

since one is a subset of the other, yet both contain the same number of elements. Since (4.8) is equivalent to (4.5), it remains to prove (4.7). To do this, it is clearly sufficient to show that every automorphism in G_1^* can be extended in the same number of ways to an automorphism of G^*.

Let $\sigma \in G_1^*$ and denote some fixed extension of σ to G also by σ. Then the set of all extensions of σ to G is the coset $\sigma G(K, K_1)$. Put $K_1' = K_1(k')$, a normal extension of K_1. Then, by Galois theory, we have

$$G(K, K_1)/G(K, K_1') \cong G(K_1', K_1) \cong G(k', k_1'),$$

the last group being cyclic of order e, say. Hence there exists $\varrho^e \in G$, in $G(K, K_1')$ such that $\sigma G(K, K_1) = \bigcup_{i=0}^{e-1} \varrho^i \sigma G(K, K_1')$ and $\varrho(\alpha) = \alpha^{q^{d_1}}$ for all $\alpha \in k' = \mathrm{GF}(q^{ed_1})$ where $k_1' = \mathrm{GF}(q^{d_1})$. Also since $\sigma \in G_1^*$, $\sigma(\alpha) = \alpha^{q^j}$ for all $\alpha \in k'$, where $(j, d_1) = 1$. It follows that

$$\sigma G(K, K_1) \cap G^* = \bigcup_{\substack{i=0 \\ (j+d_1 i, ed_1)=1}}^{e-1} \varrho^i \sigma G(K, K_1'). \tag{4.9}$$

Now since $(j, d_1) = 1$, then $(j + d_1 i, ed_1) = 1 \Leftrightarrow (j + d_1 i, e_1) = 1$ where e_1 is that part of e relatively prime to d_1. Hence, since $(d_1, e_1) = 1$, the equation $(j + d_1 i, e_1) = 1$ has precisely $\varphi(e_1)$ distinct solutions for $i \pmod{e_1}$

and so precisely $\varphi(e_1)e/e_1$ distinct solutions $(\mathrm{mod}\, e)$. Consequently, the right side of (4.9) contains the same number (namely, $\varphi(e_1)e/e_1$) of cosets of $G(K, K')$ for all $\sigma \in G_1^*$ and (4.7) follows. The proof is complete.

Note. By a simple modification of the argument deducing (4.7) from (4.5), it can be proved that for any number $l = l(n) \geqslant 0$ and any δ with $0 \leqslant \delta < 1$, then there exists a constant $b = b(n, l, \delta)$ such that if $q > b$ and

$$|\mathscr{I}^-(r_1, k) - \mathscr{I}(r_2, k^+)| \leqslant lq^{\delta},$$

then (4.5) holds and therefore (4.3) is valid. This goes part of the way to proving Conjecture 2 of [2]. The truth of (4.4) requires to be established to complete the proof.

We shall employ Theorem 2 in investigating whether (4.2) and (4.3) are equivalent. In this regard our description is complete only if it is known that $A(r_1, r_2) = g_1(y)f_2(x) - f_1(y)g_2(x)$ is irreducible in $k[x, y]$. This is certainly false if r_1, r_2 are a composite pair. However, if r_1, r_2 are not a composite pair then, in general, we would expect $A(r_1, r_2)$ to be irreducible in $k[x, y]$ (as in the rational polynomial case, see [5]). Of course, if (4.2) holds and $\deg r_3 > 1$, then $A(r_1, r_2)$ is reducible and (4.1) holds. First we state a lemma which generalises Lemma 6 of [1], which is recovered by putting $r_1(x) = x$. In its statement, y is any root of $r_1(x) = t$ and $z_1, \ldots, z_m$ $(m = n_2)$ are all the roots of $r_2(x) = t$, while, for $i = 1, \ldots, m$,

$$G'(K, k(y, z_i)) = \{\sigma \in G(K, k(y, z_i)) : \text{the largest subfield of } k' \text{ fixed by } \sigma \text{ is } k(y, z_i) \cap k'\}.$$

Lemma 4. *Statements* (i) *and* (ii) *below are equivalent.*

(i) (B(l)). $A(r_1, r_2)$ *has no absolutely irreducible factors in* $k(x, y, z)$, *where* $r_2(z) = r_1(y)$, *except precisely* l *factors, linear in* x. (Note that $A(r_1, r_2)$ always has at least one linear factor in $k(x, y, z)$, namely, $x - z$.)

(ii) *Each of the sets* $G'(K, k(y, z_i))$, $i = 1, \ldots, m$, *is equal to precisely* $l-1$ *others, while the distinct ones are pairwise disjoint.*

If, in addition, condition C(l) *holds, i.e.* $A(r_1, r_2)$ *is a product of* l *irreducible factors of the same degree in* $k[x, y]$, *then* (4.5) *holds if and, when* $l = 1$, *only if either* (i) *or* (ii) *holds (with the same* l*) and for all* i, $1 \leqslant i \leqslant m$

$$k(y, z_i) \cap k' = k. \tag{4.10}$$

Proof. The proof that (i) and (ii) are equivalent is similar to the proof of the corresponding part of Lemma 6 in [1] and is omitted.

For the remainder of the proof assume that C(l) holds. In this case, if $l = 1$, the $k(y, z_i)$, $i = 1, \ldots, m$, are all isomorphic so that (4.10) holds

for all $i = 1, \ldots, m$, if and only if it holds for one i ($\leqslant m$). Also note that (4.5) is equivalent to (4.8) and hence to

$$G^*(K, k(y)) = \bigcup_{i=1}^{m} G^*(K, k(y, z_i)), \tag{4.11}$$

which, in particular, implies that (4.10) holds for some i ($\leqslant m$). We may therefore assume from now on that, for all $i = 1, \ldots, m$, (4.10) holds and $G'(K, k(y, z_i)) = G^*(K, k(y, z_i))$.

By condition C(l), $\deg[k(y, z_i): k(y)] = m/l$, $i = 1, \ldots, m$, so that $|G(K, k(y, z_i))| = l|G(K, k(y))|/m$. Without loss of generality, let the distinct $G^*(K, k(y, z_i))$, $i = 1, \ldots, m$, be given by $i = 1, \ldots, h$. Then using the above remarks and Lemma 1, we have

$$\begin{aligned} \Big|\bigcup_{i=1}^{h} G^*(K, k(y, z_i))\Big| &\leqslant \sum_{i=1}^{h} |G^*(K, k(y, z_i))| \\ &= \sum_{i=1}^{h} (\varphi(d)/d)|G(K, k(y, z_i))| \\ &= (hl/m)(\varphi(d)/d)|G(K, k(y))| \\ &= (hl/m)|G^*(K, k(y))|. \end{aligned} \tag{4.12}$$

Now condition (ii) implies that $h = m/l$ and that equality holds throughout (4.12). This means that (4.11) is valid. Conversely, let $l = 1$ and (4.11) hold. Then, in fact, we must have $h = m$ and equality in (4.12). Hence (ii) is valid. The proof is complete.

We shall call (r_1, r_2) (in that order) an *l-exceptional pair* over k if conditions B(l), C(l) and (4.10) are satisfied. The following theorem now follows immediately from Theorem 2 and Lemma 4.

THEOREM 3. *Suppose that $A(r_1, r_2)$ is irreducible in $k[x, y]$. If $q > c(n)$ (as defined in Theorem 2), then (4.3) implies that (r_1, r_2) is a 1-exceptional pair over k.*

Conversely, if (r_1, r_2) is an l-exceptional pair over k, then (4.3) holds.

EXAMPLE 1. Here we give a non-trivial example of a 1-exceptional pair. Put $r_1(x) = x^2$, $r_2(x) = (x^3 - 3x - 2)/(3x + 2)$, so that r_1 and r_2 are not functionally related in any way. Then, if $r_1(y) = r_2(z)$, we have

$$\begin{aligned} A(r_1, r_2) &= \big(x^3 - 3(y^2+1)x - 2(y^2+1)\big), \text{ in } k(x, y), \\ &= (x - z)\big(x^2 + zx + \big(2z^2/(3z+2)\big)\big), \text{ in } k(x, y, z), \\ &= (x - z)\big(x + \tfrac{1}{2}z - \big(\sqrt{3}yz/2(z+1)\big)\big)\big(x + \tfrac{1}{2}z + \big(\sqrt{3}yz/2(z+1)\big)\big), \\ &\qquad \text{in } k(x, y, z, \sqrt{3}) = K. \end{aligned}$$

Now it is easy to show that $k(x, y) \cap k(\sqrt{3}) = k$ and hence if $\sqrt{3} \notin k$, i.e. if $q \not\equiv \pm 5 \pmod{12}$, then (r_1, r_2) is a 1-exceptional pair over k and (4.3) holds. In fact, $\mathscr{I}(r_2, k)$ contains all quadratic residues in k. Of course, this fact could have been established in other ways.

EXAMPLE 2. This example uses the criterion of Theorem 3 to construct a simple example of a pair r_1, r_2 with $A(r_1, r_2)$ reducible but with $\mathscr{I}(r_1, k) = \mathscr{I}(r_2, k)$.

Put $r_1 = x^6$, $r_2 = x^4$ and $q \equiv -1 (12)$ so that k contains no primitive 4th or 6th roots of unity. Then (x^6, x^4) and (x^4, x^6) are both 2-exceptional pairs since $k(y, z) \cap k' = k$, where $y^3 = \pm z^2$,

$$\begin{aligned} x^4 - y^6 &= (x^2 - y^3)(x^2 + y^3), \\ x^6 - y^6 &= (x - y)(x + y)(x^2 + yx + y^2)(x^2 + yx + y^2), \end{aligned} \tag{4.13}$$

and

$$x^4 - z^4 = (x - z)(x + z)(x^2 + z^2), \tag{4.14}$$

(the quadratic factors of (4.13) and (4.14) not being absolutely irreducible in $k(x, y, z)$). In fact,

$$\mathscr{I}(x^6, k) = \mathscr{I}(x^4, k) = \mathscr{I}(x^2, k).$$

We remark, finally, that it would be of interest to know of any pair (r_1, r_2) satisfying (4.3) that did not also satisfy (4.2) nor was l-exceptional for any l.

5. Remarks. For the first remark the author wishes to thank M. Fried. We recall that after Lemma 2 we specialised from a general polynomial $Q(x, t)$ to a particular one, namely $\prod_{i=1}^{s} (f_i - tg_i)$. In fact, with certain fairly obvious modifications, we could have pursued the discussion with arbitrary polynomials $F_i(x, t)$ instead of $f_i(x) - tg_i(x)$, $i = 1, \ldots, s$. Note, however, that if this is done then, in general, the polynomials $F_i(x, a)$ are not distinct for all a in k.

Next we remark that since the publication of [1], some material, due to Fried and related to that of [1] and the present paper has also appeared. In particular, [3] and [4]. Section 1 contain a discussion of the possible form of exceptional functions $r(x)$ (i.e. functions $r(x)$ for which $(r(x), x)$ is 1-exceptional).

Finally, we correct two errors in [1]. For the words "is irreducible" in the 20th and last lines of p. 258 and the 13th line down of p. 268 substitute "has no zero in k". (This brings these statements into line with assertion 29 of Theorem 2 of [4].) For the expression "$(n - \deg g)(n - 1)$" in the addendum on p. 270 read "$n(n-1)/(n - \deg g)$".

References

[1] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), pp. 255–271.

[2] M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arith. 15 (1969), pp. 91–115.

[3] — *On a conjecture of Schur*, Mich. Math. J. 17 (1970), pp. 41–55.

[4] — *Arithmetical properties of value sets of rational functions, II*, Acta Arith. (to appear).

[5] A. Schinzel, *Reducibility of polynomials of the form* $f(x)-g(y)$, Colloq. Math. 18 (1967), pp. 213–218.

UNIVERSITY OF GLASGOW
Glasgow, W. 2., U.K.

Received on 5. 9. 1970 (113)

ACTA ARITHMETICA
XX (1972)

Fixpunktmannigfaltigkeiten symplektischer Matrizen

von

B. Steinle (Erlangen)

EINLEITUNG

Nach H. Cartan besitzt der Quotientenraum $\mathfrak{H}^n = H^n/\mathrm{Sp}(n, \boldsymbol{Z})$, wo H^n den Siegel'schen Halbraum bezeichnet, die Struktur einer projektiven algebraischen Mannigfaltigkeit über dem komplexen Zahlkörper, wenn man $\mathfrak{H}^n$ noch in gewisser Weise „kompaktifiziert". Dabei sind die Fixpunkte von Modulsubstitutionen singuläre Punkte der Mannigfaltigkeit. Es ist daher wichtig, diese Fixpunkte zu kennen.

Modularkorrespondenzen sind gewisse mehrdeutige Abbildungen von $\mathfrak{H}^n$ auf sich, welche durch allgemeinere Matrizen M mit $M^t \cdot J \cdot M = rJ$ $(r \in \boldsymbol{Z}, r > 0)$ vermittelt werden. Auch für diese ist die Kenntnis ihrer Fixpunkte wichtig.

Nach ein paar Vorbereitungen in § 1 studieren wir in § 2 die Fixpunktmannigfaltigkeiten $\mathfrak{F}_M$ von Elementen $M \in \mathrm{Sp}(n, \boldsymbol{R})$ im Siegel'schen Halbraum H^n:

$$Z \in \mathfrak{F}_M \Leftrightarrow M(Z) = Z \tag{1}$$

$\left(M(Z) \overset{\text{def}}{=} (AZ+B)\cdot(CZ+D)^{-1}, \text{ wenn } M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\right)$.

Man kann M mit einer reellen Zahl multiplizieren und also in der etwas allgemeineren Form annehmen:

$$M^t \cdot J \cdot M = rJ; \quad r \in \boldsymbol{R},\ r > 0. \tag{2}$$

Unser Interesse richtet sich dabei auf zweierlei: Einerseits auf die Gestalt der auftretenden M, anderseits auf die Frage nach der Menge der Fixpunkte zu diesem M.

Fixpunkte besitzt ein M, das Lösung von (2) ist, genau dann, wenn seine Eigenwerte sämtlich vom absoluten Betrag $|\sqrt{r}|$ sind (Lemma 3 und 4). Die Lösungsmenge $\mathfrak{F}_M$ der Gleichung 1 zu einem festen M ist eine komplexe Mannigfaltigkeit, deren Dimension m einfach bestimmt werden kann (Satz 2). Nulldimensionale Fixpunktmannigfaltigkeiten