REND. SEM. MAT. UNIV. PADOVA, Vol. 117 (2007)

Proof of the Existence of Certain Triples of Polynomials.

(after a question of L. Vaserstein and E. Wheland)

UMBERTO ZANNIER (*)

ABSTRACT - Let a, b, c be complex coprime polynomials with $a + b + c = 0$ and denote by $M > 0$ their maximum degree and by $\nu(a), \nu(b), \nu(c)$ the numbers of their respective distinct roots. These integer data are relevant in the context of the Stothers-Mason "abc-theorem for function fields"; for instance such theorem implies that $\nu(a) + \nu(b) + \nu(c) > M$. Actually, L. Vaserstein and E. Wheland [VW] have explicitly raised the question to describe all the possibilities for the data. Here we show that essentially there is no restriction other than the above inequality. Our method relies on Riemann Existence Theorem, applied to construct certain covers of the projective line with suitable ramification conditions. Though this method works only over $\boldsymbol{C}$, we shall point out that the result remains true in positive characteristic $p > M$.

1. Introduction.

The present paper has been inspired by a question raised in [VW], which we now explain using a notation similar to that paper.

Let F be an algebraically closed field of characteristic 0 and let $a, b, c \in F[t]$ be (pairwise) coprime polynomials, not all constant and such that $a + b + c = 0$.

Let us put $M := \max(\deg a, \deg b, \deg c) > 0$ and let us denote by l (resp. by h, k) the number of distinct roots of a (resp. of b, c). As in [VW], let us also assume that $s := \deg a < M$ [1]. Note that, in view of $a + b + c = 0$, this implies $\deg b = \deg c = M$.

(*) Indirizzo dell'A.: Scuola Normale Superiore, Piazza dei Cavalieri, 7, 56126 Pisa - Italy.
E-mail: u.zannier@sns.it

[1] It turns out that this assumption is really a normalization, essentially irrelevant for our purposes. In fact, it just means that "∞ is a zero of a/c". Now, in any case we may perform a projective linear transformation $t \mapsto (\alpha t + \beta)/(\gamma t + \delta)$ to map a finite zero of a/c to ∞. This device allows one to reformulate in complete generality (i.e. without the restriction $s < M$) our existence result proved below.

In this setting, we have some obvious restrictions on these quantities, namely:

$$(1) \qquad 0 \leq l \leq s < M, \qquad 0 < h, k \leq M,$$

which just say that the number of roots cannot exceed the degree. Observe that another restriction is that

$$(2) \qquad l = 0 \Leftrightarrow s = 0.$$

These inequalities represent constraints in order that the 5-tuple (s, M, l, h, k) may come from actual polynomials a, b, c.

A further, subtler, restriction comes from the well-known Stothers-Mason "*abc*-theorem for polynomials" (see e.g. [L] or [VW] or [Z1]) which in this context reads:

$$(3) \qquad l + h + k \geq M + 1.$$

Now, in the paper [VW] (see p. 3) the authors explicitly raise the question of describing all the possibilities for these quantities s, M, l, h, k, in both cases of zero and positive characteristic. (They also add that "This seems to be a difficult problem, even when char$(F) = 0$.")

The object of this paper is to show that (1), (2), (3) represent the sole restrictions in characteristic 0, when F is algebraically closed. An argument involving good reduction shows that the same is true in characteristic $> M$. More precisely, we shall prove the following

THEOREM. *Let F be an algebraically closed field of characteristic* 0 *and let s, M, l, h, k be integers satisfying* (1), (2), (3) *above. Then there exist coprime polynomials $a, b, c \in F[t]$ with $a + b + c = 0$, having respectively degrees s, M, M and l, h, k distinct roots.*

The same existence conclusion is true if char$(F) > M$.

Our method goes back to our papers [Z1], [Z2]: the sought polynomials correspond to a cover $\boldsymbol{P}_1 \to \boldsymbol{P}_1$ of the projective line with certain conditions on the ramifications above $0, 1, \infty$. By Riemann Existence Theorem the desired cover exists if and only if suitable permutations on M letters may be found. This translates the problem into a purely combinatorial condition, which we shall explore.

The result in positive characteristic will follow just by observing "good reduction" for the corresponding covers over $\overline{\boldsymbol{Q}}$.

Acknowledgments. I wish to thank Prof. L. Vaserstein for drawing my attention to the paper [VW].

2. Two lemmas on permutations.

We start by proving some results about permutations, which we shall then relate with the main problem.

In the sequel we shall denote by S_M the permutation group on $\{1, 2, \dots, M\}$. We shall denote permutations by greek letters, and let them act on the right of integers, so for $\alpha, \beta \in S_M$ the product $\alpha\beta$ will mean $\beta \circ \alpha$. We shall say that a permutation $\alpha \in S_M$ has type $(r_1, \dots, r_j)$ if α is the product of disjoint cycles of lengths $r_1, \dots, r_j$ (with $r_1 + \dots + r_j = M$). Finally, we shall put $\upsilon(\alpha) := j$.

We let $s, M, l, h, k \in \boldsymbol{N}$ be integers satisfying (1), (2), (3). We write (3) in the form

$$l + h + k = M + 1 + d, \qquad d \geq 0. \tag{4}$$

We also suppose, as we may, $h \geq k > 0$ and we introduce a little further notation. We let $n := M - l + 1 \geq 2$ and we define the integer m so that $2m \geq n$ and so that the set $\{m, n - m\}$ equals $\{M - s, s - l + 1\}$. Note that $0 < m < n$. (We have $m = \max(M - s, s - l + 1)$.)

If $l = 0$ we have $s = 0$ (by (2)) and $m = M$, $n = M + 1$.

Lemma 1. *Suppose $d = 0$. Then there exist permutations $\alpha, \beta \in S_M$ such that:*

(i) *α has type $(m, n - m, 1, \dots, 1)$, so $\upsilon(\alpha) = l + 1$.*
(ii) *$\upsilon(\beta) = h$, $\upsilon(\alpha\beta) = k$.*
(iii) *The group generated by α, β in S_M is transitive.*

Remark. Here and in the sequel we tacitly mean that if $m = M$ (i.e. if $s = l = 0$), α is an M-cycle and the $n - m$ as well as the 1's do not appear in its type. In other words, we forget any permutation which moves something $> M$.

Proof. We set $\alpha := (1, \dots, m)(m + 1, \dots, n)$, so indeed α has the stated type; namely, its disjoint cycles have lengths $m, n - m$ and 1; in turn, this implies that $\upsilon(\alpha) = 2 + (M - n) = 2 + M - (M - l + 1) = l + 1$.

Note that $h + k = M - l + 1 = n$ (by (4) and $d = 0$). Since $k \leq h$ we have $k \leq n/2 \leq m$.

Suppose first that $k \leq m - 1$ and that $m + 1 < n$. Now we set $\beta := (k, \dots, 1)(m, m + 1)(n, \dots, M)$. By the supposed inequalities, this formula gives the cycle decomposition of β and it follows that $\upsilon(\beta) = 1 + (m - 1 - k) + 1 + (n - m - 2) + 1 = n - k = h$.

Also, we have

$$\begin{aligned}\alpha\beta = (1,\dots,m)(k,\dots,1)(m+1,\dots,n)(m,m+1)(n,\dots,M) =\\ = (k,\dots,m)(m+1,\dots,n)(m,m+1)(n,\dots,M) =\\ = (k,\dots,m-1,m+1,\dots,n,m)(n,\dots,M)\end{aligned}$$

(omitting "$k,\dots,$" in case $k = m-1$). In turn, this equals $(k,\dots,m-1, m+1,\dots,n-1,n+1,\dots,M,n)$.

Hence in this case we find that $\upsilon(\alpha\beta) = (k-1)+1 = k$.

Also, the cycle decompositions that we have found show that no proper nonempty subset of $\{1,\dots,M\}$ is left invariant by the cycles of both α and β, so α,β generate a transitive subgroup.

The "extreme" cases $k = m$ and/or $m+1 = n$ are dealt with similarly. If both equalities hold, then $k = 1, n = 2$, since $k \le n/2$. Hence $M = l+1$. Now we may take α to be the identity and β to be an M-cycle.

If $k = m$ and $m+1 < n$ we define β with the same formulae, and the only difference with the above is that now this need not express the disjoint cycle decomposition. If $k = m$ we have $(k,\dots,1)(m,m+1) = (m,\dots,1,m+1)$; now $n > m+1$, and again we have $\upsilon(\beta) = 1 + (n-1-m-1)+1 = = n-m = n-k = h$.

If $n = m+1$ and $k < m$ we again define

$$\beta = (k,\dots,1)(m,m+1)(m+1,\dots,M) = (k,\dots,1)(m,m+2,\dots,M,m+1),$$

whence $\upsilon(\beta) = 1 + (m-k-1)+1 = m+1-k = n-k = h$, as required. (As remarked above, we forget permutations moving numbers $> M$.)

This completes the proof. QED

LEMMA 2. *For arbitrary d as in (4), there exist permutations α,β and transpositions $t_1,\dots,t_d$ in S_M such that:*

(i) *α has type $(m, n-m, 1,\dots,1)$, so $\upsilon(\alpha) = l+1$.*
(ii) *$\upsilon(\beta) = h$, $\upsilon(\alpha\beta t_1\cdots t_d) = k$.*
(iii) *$\alpha,\beta,t_1,\dots,t_d$ generate a transitive subgroup of S_M.*

PROOF. We argue by induction on $d \ge 0$. The case $d = 0$ is the content of Lemma 1, so we assume $d \ge 1$ and the result true up to $d-1$.

Suppose first that $h \ge k+1$. Then $h^* := h-1 \ge k$ and we may apply the inductive hypothesis with the same data, except that we replace h with h^* and d by $d-1$.

Let $\alpha^*,\beta^*,t_1^*,\dots,t_{d-1}^*$ be permutations as in the conclusion. In particular

β^* is a product of h^* disjoint cycles. Since $h^* < h \leq M$ one of the cycles is has length $q > 1$, and after renumbering we may assume it is $(1, \dots, q)$.

We have $(1, \dots, q)(1, 2) = (1)(2, \dots, q)$ so $\beta^*(1, 2)$ is a product of $h^* + 1 = h$ disjoint cycles, i.e., $\upsilon(\beta^*(1, 2)) = h$.

We then set $\alpha := \alpha^*$, $\beta := \beta^*(1, 2)$, $t_1 = (1, 2)$ and, for $i = 2, \dots, d$, $t_i := t^*_{i-1}$. Since $\alpha\beta t_1 \cdots t_d = \alpha^*\beta^* t^*_1 \cdots t^*_{d-1}$, plainly these new permutations satify the sought conclusion (note that they generate a group containing $\alpha^*, \beta^*, t^*_1, \dots, t^*_{d-1}$).

Suppose now that $h = k$. Since $2k = h + k = n + d \geq 3$ we have $k \geq 2$. We write $k = k^* + 1$ and apply the inductive hypothesis with the same data, but this time replacing k with k^* and d with $d - 1$.

Again, let α^*, β^*, $t^*_1, \dots, t^*_{d-1}$ be permutations as in the corresponding conclusion. So, $\alpha^*\beta^* t^*_1 \cdots t^*_{d-1}$ is a product of k^* disjoint cycles. Again, $k^* < M$, so one of the cycles will have length $q > 1$ and as before we denote it with $(1, \dots, q)$. Then $\alpha^*\beta^* t^*_1 \cdots t^*_{d-1}(1, 2)$ is the product of k disjoint cycles. It suffices then to define $\alpha := \alpha^*$, $\beta := \beta^*$, $t_i := t^*_i$ for $i = 1, \dots, d - 1$ and finally $t_d := (1, 2)$, to obtain the sought conclusion.

This completes the proof. QED

3. Proof of Theorem.

We let s, M, l, h, k be integers satisfying (1), (2), (3) above and we proceed to prove the existence of coprime polynomials $a, b, c \in \boldsymbol{C}[t]$ such that

$$(5) \qquad \deg a = s, \quad \deg b = \deg c = M, \quad \upsilon(a) = l, \quad \upsilon(b) = h, \quad \upsilon(c) = k,$$

where we have denoted by $\upsilon(q)$ the number of distinct roots of a polynomial q.

We define d by (4) and take permutations $\alpha, \beta, t_1, \dots, t_d$ as in Lemma 2. We also put $\gamma := \alpha\beta t_1 \cdots t_d$. We also choose distinct points $Q_1, \dots, Q_d \in \in \boldsymbol{P}_1 \setminus \{0, 1, \infty\}$.

By Riemann Existence Theorem (see e.g. [Vo] or [Z1,2]) there exist a compact Riemann Surface $\mathcal{S}$ and a non-constant holomorphic map $f : \mathcal{S} \to \boldsymbol{P}_1$, unbranched outside $\{0, 1, \infty, Q_1, \dots, Q_d\}$ and such that:

(i) The map f has degree M.

(ii) The ramification above 0 has cycle structure as α, above 1 as β, above ∞ as γ, above Q_i as t_i. (We mean that the ramification indices equal the cycle lengths.)

In fact, we may prescribe that the monodromy above the branch points is given respectively by $\alpha, \beta, \gamma^{-1}, t_1, \dots, t_d$, after we have chosen suitable loops going around the points $0, 1, \infty, Q_1, \ldots, Q_d$ (based at some other point $Q \in \boldsymbol{P}_1$) to define the monodromy by lifting these loops to $\mathcal{S}$. The condition that $\alpha\beta t_1 \cdots t_d \gamma^{-1}$ is the identity corresponds to the only relation of these loops in $\pi_1(\boldsymbol{P}_1 \setminus \{0, 1, \infty, Q_1, \ldots, Q_d\})$. (See [Vo] for a detailed modern exposition of all of this together with the proofs.)

We may compute the genus g of $\mathcal{S}$ with the Riemann-Hurwitz formula. The ramification contribution above 0 is $M - \upsilon(\alpha)$, above 1 is $M - \upsilon(\beta)$, above ∞ is $M - \upsilon(\gamma)$ and above Q_i is 1 (since t_i is a transposition).

Therefore the formula reads

$$\begin{aligned} 2g - 2 &= -2M + (M - l - 1) + (M - h) + (M - k) + d = \\ &= M - l - 1 - h - k + d = -2, \end{aligned}$$

where we have used (4) for the last equality; hence $g = 0$. Therefore we may assume that $\mathcal{S}$ is $\boldsymbol{P}_1$ and that f is a rational function in $\boldsymbol{C}(t)$.

Since the ramification indices above 0 are given by the cycle-lengths of the permutation α, it follows that f has a zero of order $M - s > 0$. After an automorphism of $\boldsymbol{P}_1$ we may then assume that this zero is ∞.

Write then $f = -a/c$ where a, c are coprime polynomials in $\boldsymbol{C}[t]$. Since ∞ is a zero of f of multiplicity $M - s$ and since $\deg f = M$, we have $\deg a = s$ and $\deg c = M$. The number of distinct roots of a is the number of finite zeros of f, so is $\upsilon(\alpha) - 1 = l$. Similarly, the number of zeros of c is the number of poles of f, which in turn is $\upsilon(\gamma) = k$.

Put $b = -a - c$, so $f - 1 = b/c$. Now we see that the number of zeros of b is the number of zeros of $f - 1$, i.e. is $\upsilon(\beta) = h$, as required.

This achieves our construction and proves the theorem for $F = \boldsymbol{C}$. However the general case of algebraically closed F of characteristic zero follows from the complex case by a standard argument. The coefficients and roots of the involved polynomials generate a certain finitely generated field over $\overline{\boldsymbol{Q}}$. This is the function field of a certain algebraic variety over $\overline{\boldsymbol{Q}}$ (possibly a point). By the Nullstellensatz we may take a point of this variety such that under specialization to this point the distinct roots of the polynomials remain distinct and the leading coefficients do not vanish. The resulting polynomials have algebraic coefficients and still the same integers s, M, l, h, k attached to them. Since F contains the algebraic numbers we are done.

To conclude the proof we deal with the case $\mathrm{char}(F) =: p > M$. To start with we take the above points $Q_1, \ldots, Q_d$ in a number field K, actually lying in some Discrete Valuation Ring $\mathcal{O}$ of K, with maximal ideal $\mathcal{P}$ above p. We may also assume that the reductions of the Q_i at $\mathcal{P}$ remain distinct and distinct from $0, 1, \infty$.

Now, by the above method we may realize the construction over $\overline{\boldsymbol{Q}}$, and by enlarging K and $\mathcal{O}$ we may assume that a, b, c have their roots and coefficients in K. As in the above proof, the polynomials a, b, c define a cover of $\boldsymbol{P}_1$ with certain ramification conditions at $0, 1, \infty, Q_1, \ldots, Q_d$, and unramified outside these points. By a result of S. Beckmann [B] (which traces back to Fulton and Grothendieck) the cover has good reduction modulo $\mathcal{P}$, provided p does not divide the order of the monodromy group. Since $p > M$ this is certainly the case.

It suffices then to take a model of the cover having good reduction; its reduction modulo $\mathcal{P}$ gives polynomials with the required properties over the residue field, which is a finite extension of $\boldsymbol{F}_p$.

This concludes the proof of the Theorem.

4. Final remarks.

We observe that the proof gives the more precise conclusion that the polynomial a may be taken with at most one multiple root.

A more precise requirement would be to find simple necessary and sufficient existence conditions for a, b, c, prescribing not just the degrees and numbers of roots but also the respective multiplicities. This has been carried out in special cases in [Z2], for covers unbranched outside $0, 1, \infty$. (See also [Z1] for other, simpler, examples in positive genus.)

The problem appears very difficult in positive (small) characteristic p. Certainly the conditions (1), (2), (3) are not themselves always sufficient for existence; for instance it may be shown that (3) cannot hold with equality if $M - s$ is a multiple of p. In [Z3] some sufficient conditions for good reduction appear which go beyond [B], but certainly not sufficiently general to cover the wider natural questions which arise here.

We have left aside all questions of rationality, when F is not assumed to be algebraically closed. The methods of this paper give a bound for the degree of a number field over which the construction can be realized (see also the paper [Z2]). However it seems unlikely that this leads to precise informations on the minimal field of definition.

REFERENCES

[B] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*. J. Algebra, **125**, no. 1 (1989), pp. 236–255.

[L] S. Lang, *Algebra*, Springer-Verlag.

[VW] L. VASERSTEIN - E. WHELAND, *Vanishing Polynomial Sums*, Comm. in Algebra, **31**, no. 2 (2003), pp. 751–772.

[Vo] H. VÖLKLEIN, *Groups as Galois groups*, Cambridge Studies in Adv. Math., **53**, Camb. Univ. Press, 1996.

[Z1] U. ZANNIER, *Some remarks on the S-unit equation in function fields*, Acta Arith. **LXIV** (1993), pp. 87–98.

[Z2] U. ZANNIER, *On Davenport's bound for the degree of* $f^3 - g^2$ *and Riemann Existence Theorem*, Acta Arith., **LXXI** (1995), pp. 107–137.

[Z3] U. ZANNIER, *Good reduction of certain covers* $\boldsymbol{P}^1 \to \boldsymbol{P}^1$, Israel J. of Math., **124** (2001), pp. 93–114.

Manoscritto pervenuto in redazione il 6 marzo 2006