About an Old Romanian TST Problem

by Titu Andreescu and Marian Tetiva

1. Introduction. The problem [1] which we discuss in this note has been proposed in a 1983 Team Selection Test (TST) for the International Mathematical Olympiad from that year by the Romanian algebraist Toma Albu. This is its statement:

Problem. Let p be an odd prime number, let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p over the field of rational numbers, and let $x_1, \ldots, x_p$ be the complex roots of f. Prove that for any non-constant polynomial g with rational coefficients, and of degree less than p, the numbers $g(x_1), \ldots, g(x_p)$ are pairwise distinct.

And here comes the (non-elementary) solution intended by the proposer.

First solution of the problem. Being irreducible, f is (possibly associate to) the minimal polynomial of any of its roots; thus, the degree of any x_i over $\mathbb{Q}$ is precisely p, the degree of f. Let us consider the polynomial

$$u = (X - g(x_1)) \cdots (X - g(x_p))$$

whose coefficients are values of symmetric polynomials for $x_1, \ldots, x_p$ (as $-(g(x_1) + \cdots + g(x_p))$, or $\sum_{1 \le i < j \le p} g(x_i)g(x_j)$, etc). Because the fundamental symmetric polynomials in p indeterminates have rational values for $x_1, \ldots, x_p$ (this values being the coefficients of f, modulo the signs), by the fundamental theorem of symmetric polynomials (asserting that any symmetric polynomial with coefficients in a field can be expressed as a polynomial – with coefficients in the same field – of the fundamental symmetric polynomials), we infer that the coefficients of u are also rational numbers. Also, clearly, any $g(x_i)$ $(1 \le i \le p)$ is a root of u. By looking at the tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}(g(x_i)) \subseteq \mathbb{Q}(x_i)$$

and by writing the multiplicativity formula for the degrees of the extensions

$$p = [\mathbb{Q}(x_i) : \mathbb{Q}] = [\mathbb{Q}(x_i) : \mathbb{Q}(g(x_i))][\mathbb{Q}(g(x_i)) : \mathbb{Q}],$$

we find that the degree of the minimal polynomial of $g(x_i)$ over $\mathbb{Q}$ (which is the same as $[\mathbb{Q}(g(x_i)) : \mathbb{Q}]$) is a divisor of p. (We will also get this conclusion by using only the properties of minimal polynomials in the next solutions that we want to present, even in a slightly more general context.)

Thus, this degree is either equal to 1, or equal to p. However, the degree of $g(x_i)$ over $\mathbb{Q}$ cannot be 1, since this would imply that $g(x_i)$ is a rational number, which is not possible, because x_i would be the root of the polynomial $g(X) - g(x_i)$, which would then have rational coefficients and degree less than the degree of the minimal polynomial f of x_i. Thus the minimal polynomial of, say, $g(x_1)$ has degree p, and, also, this minimal polynomial must be a divisor of $u = (X - g(x_1)) \cdots (X - g(x_p))$ which also has degree p, rational coefficients, and $g(x_1)$ as a root. It follows that u *is* the minimal polynomial of $g(x_1)$ (and of any of the $g(x_i)$, $1 \le i \le p$) over $\mathbb{Q}$, therefore it is an irreducible polynomial, and then its roots $g(x_1), \ldots, g(x_p)$ are distinct, as desired.

We see that the proposer used in his solution (a few rudiments of) field theory. The introduction into this topic has been made in the lectures he held for the Romanian (extended) team for that year's IMO, before the problem was proposed for the test. Unfortunately, it was a fact that the students did not solve the problem by this method (or by any other), and this is one reason for which we wrote this note: namely, to present

two more solutions that avoid the use of field extensions – solutions which are, let us say so, "more elementary". In fact just a little knowledge of the basic properties of the minimal polynomial of an algebraic number over $\mathbb{Q}$ is required to understand them. So we will first review these properties.

2. The minimal polynomial of an algebraic number. Let α be a complex number. The minimal polynomial of α over $\mathbb{Q}$ is the monic (that is, with the coefficient of the highest power of the indeterminate equal to 1) polynomial $h \in \mathbb{Q}[X]$ such that $h(\alpha) = 0$ and such that h has minimum degree among the non-zero polynomials annihilated by α (when such polynomials do exist; in this case α is called *algebraic over the field of rational numbers*, or, simply, *algebraic*). If h is the minimal polynomial of α, then any ah, with $a \in \mathbb{Q}^*$ has the same properties as h, except (when $a \neq 1$) from that of being monic (ah is said to be *associate* in divisibility to h, in the sense that any of h and ah divides the other). For instance, any rational number α is algebraic over $\mathbb{Q}$, with minimal polynomial $X - \alpha \in \mathbb{Q}[X]$. Also, the number $\alpha = 1 + \sqrt{2}$ is algebraic, having minimal polynomial $X^2 - 2X - 1$ (why?), and $\alpha = \sqrt[3]{2}$ has minimal polynomial $X^3 - 2$. It is well-known now (from Lindemann and Hermite, respectively) that the numbers π and e are transcendental over $\mathbb{Q}$, that is, non-algebraic (they are roots of no non-zero polynomial with rational coefficients), and that, basically, there are "much more" transcendental than algebraic numbers. However, it is not our purpose here to enter deeper in this topic.

The following properties of the minimal polynomial are easy to prove by using the Euclidean division of polynomials, and the derivative of a polynomial (and, of course, the definitions).

(i) The minimal polynomial of an algebraic number is irreducible over $\mathbb{Q}$. (A polynomial from $\mathbb{Q}[X]$ is irreducible – over $\mathbb{Q}$, or in $\mathbb{Q}[X]$ – if it cannot be expressed as a product of two polynomials from $\mathbb{Q}[X]$, both having degrees at least equal to 1.)

(ii) The roots of the minimal polynomial of an algebraic number α are not rational numbers, except for the case when α is rational, and its minimal polynomial is $X - \alpha$.

(iii) If h is the minimal polynomial of α and $q(\alpha) = 0$ for some $q \in \mathbb{Q}[X]$, then h is a divisor of q. Moreover, if α is a root of q having multiplicity k, then h^k divides q.

(iv) If $h(\alpha) = 0$, with $h \in \mathbb{Q}[X]$, and h is irreducible, then h is associate to the minimal polynomial of α (in particular, if h is monic and $h(\alpha) = 0$, then h is precisely the minimal polynomial of α).

(v) The roots of the minimal polynomial of α are all simple, hence mutually distinct. In general, an irreducible (in $\mathbb{Q}[X]$) polynomial cannot have multiple roots.

We encourage the reader to prove these assertions, or to find their proofs in any introductive course of higher algebra, for example [2,3] (which are also recommended for understanding the above first solution of the problem). At the moment when the problem has been proposed, an elementary solution was known only in the case $p = 3$ (of course, in the case $p = 2$, too, but if $p = 2$, then g can only be a first degree non-constant polynomial, and the problem simply follows from the fact that the roots of f are distinct, as we already mentioned). The solution for $p = 3$ (which, again, we invite the reader to find on hers/his own, before reading it) goes like this.

Pseudo-elementary solution in the case $p = 3$. As f has degree 3, g has degree at most 2. If it has degree 1, there is nothing to prove, as the roots x_1, x_2, x_3 are distinct (hence so will also be $ax_1 + b, ax_2 + b, ax_3 + b$, if $a \neq 0$). When $g = aX^2 + bX + c$ (with $a \neq 0$), we have $g(x_1) = g(x_2)$ if either $x_1 = x_2$, or $x_1 + x_2 = -\dfrac{b}{a}$. Since the first possibility is excluded, if we suppose $g(x_1) = g(x_2)$, we get

$$x_1 + x_2 = -\frac{b}{a} \in \mathbb{Q},$$

then

$$x_3 = (x_1 + x_2 + x_3) - (x_1 + x_2) \in \mathbb{Q}.$$

Thus, if we assumed $g(x_1) = g(x_2)$, then x_3 would be a rational number, and f would not be irreducible (having the factor $X - x_3$), a contradiction.

We see that this is not completely elementary, it requires the knowledge of the notion of irreducible polynomial, as the solutions we present further do – but, as we already said, these solutions, at least, do not need field theoretic results. Moreover, the notion of irreducible polynomial appears in the very statement of the problem, so it cannot be avoided anyway.

3. A more general result and its first proof. We will prove the following statement, clearly a generalization of the starting problem. It was proposed by I. Savu in *Gazeta Matematică* in 1987 [4] but, probably, the proposer of the initial problem, was familiar to this general form, too, although the first solution doesn't seem to be appropriate for it.

Proposition. If $f \in \mathbb{Q}[X]$ is an irreducible polynomial in $\mathbb{Q}[X]$, of degree n, if $x_1, \ldots, x_n$ are its complex roots, and if $g \in \mathbb{Q}[X]$ is of degree less than n and non-constant, then the numbers $g(x_1), \ldots, g(x_n)$ can be split into $k > 1$ groups of the same size l such that in each group the numbers are all equal, and the common values of the numbers from the k groups are mutually distinct. Of course, we have $kl = n$. More specific, we have, after a possible re-indexation, $g(x_1) = \cdots = g(x_l) = a_1$, $g(x_{l+1}) = \cdots = g(x_{2l}) = a_2$, and so on, until $g(x_{(k-1)l+1}) = \cdots = g(x_n) = a_k$, with $a_1, \ldots, a_k$ distinct.

First proof of the proposition – and second solution of the problem. We consider again the polynomial

$$u = (X - g(x_1)) \cdots (X - g(x_n))$$

whose coefficients are, as we have seen in the first solution, rational numbers (this does not depend on the degree of f being a prime, or greater than the degree of g). Consequently, the polynomial

$$v(X) = u(g(X)) = (g(X) - g(x_1)) \cdots (g(X) - g(x_n))$$

has rational coefficients, too. Clearly, each x_i is a root of v, so, as $x_1, \ldots, x_n$ are the roots of the irreducible polynomial f (their minimal polynomial), v must be divisible by f. Also, since g is non-constant, v is a non-constant polynomial, too (in particular, non-zero). Thus we have $v = f^r w$ with $r \geq 1$ and $w(x_i) \neq 0$ for any $1 \leq i \leq n$, by the unique factorization theorem in the ring $\mathbb{Q}[X]$ of the polynomials with coefficients in the field $\mathbb{Q}$. This means that the factor $(X - x_i)^r$ divides v, and $(x - x_i)^{r+1}$ does not divide v (the multiplicity of the root x_i for the polynomial v is precisely r) for any $1 \leq i \leq n$.

Now assume that (after some possible re-indexation) we have $g(x_1) = \cdots = g(x_l) = a$, with a distinct from any of the other values $g(x_{l+1}), \ldots, g(x_n)$. We then have

$$v(X) = (g(X) - g(x_1))^l (g(X) - g(x_{l+1})) \cdots (g(X) - g(x_n))$$

and no factor $g(X) - g(x_j)$ with $l + 1 \leq j \leq n$ has the root x_1. It follows that the multiplicity of the root x_1 for the polynomial v is ls, where s is the multiplicity of x_1 for $g(X) - g(x_1)$. Since the same multiplicity is r, we get $ls = r$. Nevertheless, note that the multiplicity of the root x_i for the polynomial $g(X) - g(x_i)$ does not depend on the index i, because any two such polynomials $g(X) - g(x_i)$ and $g(X) - g(x_j)$ have the same derivatives (and the multiplicity of a root of a polynomial equals the least order of a derivative of that polynomial which does not vanish for that root; therefore, the multiplicity of x_i as a root of $g(X) - g(x_i)$ equals the multiplicity of f as a factor of g' plus one). Consequently, if we further consider another group of equal values among $g(x_1), \ldots, g(x_n)$,

say $g(x_{l+1}) = \cdots = g(x_{l+m}) = b$ with b different from any of $g(x_{l+m+1}), \ldots, g(x_n)$ (and, of course, different from a), we will obtain in the same way that $ms = r$, by expressing in two ways the multiplicity of x_{l+1} as a root of v. Thus $m = l$, and clearly, we can go on similarly with another group of equal values among $g(x_1), \ldots, g(x_n)$, and find that the number of x_i that produce that group is the same as l and m, and so on, until we exhaust all $g(x_i)$. Thus $g(x_1), \ldots, g(x_n)$ split (as claimed) into equal-sized groups of equal numbers. The number k of the groups cannot be 1, because in this case we would have $g(x_1) = \cdots = g(x_n) = a$, and, since $na = g(x_1) + \cdots + g(x_n)$ is a rational number, a would be rational, too. But then x_1 (for example) would be root of the polynomial $g(X) - a$ with rational coefficients and with degree less than $n = \deg(f)$. This is, however, not possible, since f, being irreducible, is also the minimal polynomial of x_1 (and of any of its roots), thus no non-zero polynomial with rational coefficients and degree less than n admits x_1 as a root.

For the given contest problem, when $n = p$ is a prime, we must have $kl = p$ with $k > 1$, meaning that $k = p$ ($l = 1$), that is, all values $g(x_1), \ldots, g(x_p)$ are mutually distinct, as required.

4. **Second proof for the proposition.** The following helping result finally allows a pretty simple solution to our problem – in fact, for the general result of the proposition.

Lemma. If $x_1, \ldots, x_n$ are the roots of the irreducible (over $\mathbb{Q}$) polynomial $f \in \mathbb{Q}[X]$, and $g \in \mathbb{Q}[X]$ is any polynomial with rational coefficients, then the numbers $g(x_1), \ldots, g(x_n)$ have the same minimal polynomial.

Proof of the lemma. Note again that, being irreducible, f is (associate to) the minimal polynomial of any of its roots. Suppose $h \in \mathbb{Q}[X]$ is the minimal polynomial of $g(x_i)$, for some $1 \leq i \leq n$, hence we have

$$h(g(x_i)) = 0.$$

Equivalently, we can say that x_i is a root of the polynomial $h(g(X))$, which must therefore be divisible by the (possibly associate to the) minimal polynomial f of x_i. This shows that any root of f is also a root of $h(g(X))$, that is

$$h(g(x_j)) = 0$$

for any (other) index $1 \leq j \leq n$. In other words, $g(x_j)$ is also a root of the minimal polynomial of $g(x_i)$, implying that the minimal polynomial of $g(x_j)$ is a divisor of the minimal polynomial of $g(x_i)$. Since in this reasoning the indices i and j are, clearly, interchangeable, we infer that the reverse is also true (that is, the minimal polynomial of $g(x_i)$ is a divisor of the minimal polynomial of $g(x_j)$), consequently $g(x_i)$ and $g(x_j)$ have the same minimal polynomial, for any $i, j \in \{1, \ldots, n\}$. as we wanted to prove. Now let's see

The second proof of the proposition – and third solution of the problem. As in the previous proofs, we find that the polynomial

$$u = (X - g(x_1)) \cdots (X - g(x_n))$$

has rational coefficients. We consider the minimal polynomial h of any of the $g(x_i)$, which has to be a divisor of u, because $u(g(x_i)) = 0$ for every $1 \leq i \leq n$. But, because every root of u has the same minimal polynomial h, it follows that the only irreducible factor of u is h (if some other irreducible factor would appear, it would be the minimal polynomial of some roots of u), therefore the factorization of u is $u = h^l$ for some positive integer l. Thus the roots of u split into $k = \dfrac{n}{l}$ groups of l equal elements each, as required.

For a more thorough (but not quite a necessary) analysis, we can start by noting that h is a product of a few of the factors $X - g(x_i)$, say

$$h = (X - g(x_{i_1})) \cdots (X - g(x_{i_k})).$$

Of course, $g(x_{i_1}), \ldots, g(x_{i_k})$ are pairwise distinct. Then (if $x_{i_1}, \ldots, x_{i_k}$ are not all of $x_1, \ldots, x_n$), consider some $j_1 \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$ and its minimal polynomial, h again. This time h, as a new factor of g must collect some of the factors $X - g(x_j)$ with $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$, for instance

$$h = (X - g(x_{j_1})) \cdots (X - g(x_{j_k})),$$

in such a way that

$$\{g(x_{i_1}), \ldots, g(x_{i_k})\} = \{g(x_{j_1}), \ldots, g(x_{j_k})\}$$

and $g(x_{j_1}), \ldots, g(x_{j_k})$ are mutually distinct. In other words, $g(x_{j_1}), \ldots, g(x_{j_k})$ coincide, in some order, with $g(x_{i_1}), \ldots, g(x_{i_k})$. This procedure can be continued on and on until we exhaust all factors $X - g(x_i)$ of u, and, clearly, it must eventually come to an end. We get that the numbers $g(x_i)$ split into a number l of equal sets (not multi-sets!) of size k, such that $kl = n$, which is a slightly different way to put the conclusion of the proposition. The second proof is done.

5. Final remarks. 1) The proposition remains true if g has not necessarily the degree less than the degree of f, with the only correction that we must not have necessarily $k > 1$ (that is, it is possible for all numbers $g(x_1), \ldots, g(x_n)$ to be equal, but only in some special cases). Indeed, by Euclidean division, we have $g = fc + r$, with rational polynomials c and r, with the degree of r less than the degree of f. Because $g(x_i) = f(x_i)c(x_i) + r(x_i) = r(x_i)$ and r is, as in the initial statement of the proposition, of degree less than the degree of f, we get the conclusion: if the remainder of g divided by f is a constant polynomial, then $g(x_1) = \cdots = g(x_n)$ (we have $k = 1$); otherwise, the values $g(x_1), \ldots, g(x_n)$ split into $k > 1$ equal-sized groups of equal numbers. Also note that $p = 2$ needs not be avoided – the result remains true in this case, too (but it follows immediately from the fact that the roots of f are distinct).

2) Remember from the first proof of the proposition that we have $ls = r$, where l is the number of equal values among $g(x_1), \ldots, g(x_n)$, s is the multiplicity of any x_i as a root of $g(X) - g(x_i)$, and r is the multiplicity of f as a factor of $u = (g(X) - g(x_1)) \cdots (g(X) - g(x_n))$. We also saw in that proof that $s = t + 1$, where t is the multiplicity of f as a factor of g'. On the other hand, from the second proof we know that $k = \dfrac{n}{l}$ is the degree of the minimal polynomial of any $g(x_i)$. Putting all these together we get the following interesting conclusion.

Corollary. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial, having the (complex) roots $x_1, \ldots, x_n$, and let $g \in \mathbb{Q}[X]$ be a nonconstant polynomial. Let k, t, and r be the degree of the minimal polynomial of any $g(x_i)$, the multiplicity of f in the factorization of the derivative of g, and the multiplicity of f as a factor of $u = (g(X) - g(x_1)) \cdots (g(X) - g(x_n))$ respectively. Then the equality

$$n(t + 1) = kr$$

holds.

References:

1. T. Albu: *Problem 3* from the 3rd Romanian TST for IMO, 1983
2. I. N. Herstein: *Topics in Algebra*, Xerox College Publishing, 1975
3. S. Lang: *Algebra*, Springer-Verlag, New York, 2002
4. I. Savu: *Problem O:502*, *Gazeta matematică B*, 1/1987

Titu Andreescu
Marian Tetiva