Commuting Polynomials

I. YANTAROV

EDITOR'S NOTE. Mathematical problems that are proposed to high-school students are usually related to new results in mathematics in a rather oblique way. Or at best, they may only touch upon some very particular details, ruling out any chance for the reader to grasp the entire concept. A probable reason for this is that in mathematics everything is interrelated, and thus to understand even a fairly elementary question completely, one has to take into account considerations from nonelementary areas of mathematics.

The problem of commuting polynomials—the subject of this article—is a fortunate exception to this rule, because it allows one to do real mathematics by entirely elementary methods.

We knew about this problem from a letter we received two years ago from E. Turkevich, to whom we owe the first results in this area. A problem, completed with additional questions and divided into several steps, was then proposed for the research tour of the XIth Soviet Mathematical Olympiad and also appeared in the *Kvant Problem Book* under the number M455.

Formulation of the Problem.

Two polynomials P and Q in one variable are said to *commute*[1] if $P(Q(x))$ is equal to $Q(P(x))$. This implies that upon removal of parentheses and collecting terms we will obtain the same polynomials in each case. This is also equivalent to the requirement that for every real number d we have the numerical equality $P(Q(d)) = Q(P(d))$.

In Problem M455 of the *Kvant Problem Book* only polynomials with leading coefficient 1 were considered. We will refer to such polynomials as *unitary*. (As we will see later, any question about arbitrary commuting polynomials can always be reduced to one about polynomials with leading coefficient ±1.)

The problem consists of five connected subproblems:

(a) For any given number α find all polynomials of degree no greater than 3 that commute with the polynomial $P(x) = x^2 - \alpha$.

(b) Prove that there exists no more than one polynomial of a given degree that commutes with a given polynomial of degree 2.

The Russian original is published in *Kvant* 1979, no. 4, pp. 19–23.

TRANSLATION EDITOR'S NOTE: The reader will search the mathematical literature in vain for any mention of a mathematician named I. Yantarov. A clue to the true identity of the author of this paper can be found in the fact that “yantar’” in Russian means “amber” in English. The German word for “amber” is “Bernstein,” and indeed, the author of this article is I. Bernstein.

[1] From the Latin *commutativus*, “interchanging.”

(c) Find all polynomials of degrees 4 and 8 that commute with a given polynomial P of degree 2.

(d) Prove that if polynomials Q and R both commute with the polynomial P of degree 2, then they commute with each other.

(e) Prove the existence of an infinite sequence of polynomials $P_1, P_2, \ldots, P_k, \ldots$ among which every pair commute, the degree of each P_k is k, and $P_2 = x^2 - 2$.

Solution to Problems (a) through (d).

SOLUTION TO (a). Let $Q(x) = x^3 + ax^2 + bx + c$. The equality $P(Q(x)) = Q(P(x))$ can be rewritten as

$$\left(x^3 + ax^2 + bx + c\right)^2 - \alpha = \left(x^2 - \alpha\right)^3 + a\left(x^2 - \alpha\right)^2 + b\left(x^2 - \alpha\right) + c.$$

Before expanding these expressions, observe that on the right we have only even powers of x, while on the left there is an x^5 with coefficient $2a$. Hence $a = 0$. But then the coefficient of x^3 on the left is $2c$, and therefore c also vanishes. Thus $Q(x) = x^3 + bx^2$. Removing the parentheses and equating the coefficients of equal powers of x, we obtain

$$\begin{aligned} 2b &= -3\alpha, \\ b^2 &= 3\alpha^2 + b, \\ \alpha &= \alpha^3 + b\alpha. \end{aligned}$$

Let $\alpha = 2\gamma$. Then $b = -3\gamma$. The second equation implies that $9\gamma^2 = 12\gamma^2 - 3\gamma$, i.e., $\gamma^2 - \gamma = 0$. Hence either $\gamma = 0$ or $\gamma = 1$. It is easily verified that each of these values leads to a solution of the system.

We can summarize the result as follows. A polynomial of degree 3 that commutes with $P(x) = x^2 - \alpha$ exists only when either $\alpha = 0$ (and $P(x) = x^2$, $Q(x) = x^3$) or $\alpha = 2$ (and then $P(x) = x^2 - 2$, $Q(x) = x^3 - 3x$).

In a similar way one can prove that if the degree of Q is 2, then necessarily $Q = P$, and if the degree of Q is 1, then $Q(x) = x$.

You can see that this part of the problem is fairly simple. At the Olympiad, it was proposed to the students mainly as an introductory task. Nevertheless, a close look at the equations written above may give the clue to solving part (b), and thus a key to the whole problem.

SOLUTION TO (b). Let

$$\begin{aligned} Q(x) &= x^k + a_1x^{k-1} + a_2x^{k-2} + \cdots + a_{k-1}x + a_k, \\ P(x) &= x^2 + px + q. \end{aligned}$$

Consider the equality

$$\begin{aligned} (x^k + a_1x^{k-1} + \cdots + a_k)^2 + p(x^k + a_1x^{k-1} + \cdots + a_k) + q \\ -(x^2 + px + q)^k - a_1(x^2 + px + q)^{k-1} - \cdots - a_k = 0. \end{aligned}$$

Equating the coefficients of $x^{2k}, x^{2k-1}, \ldots, x^1, x^0$, we obtain a system of equations for $a_1, a_2, \ldots, a_k, p, q$. It is rather difficult even to write down this system, to say nothing of solving it. However, some useful observations can be made. Note that the coefficients $b_1, b_2, \dots, b_k$ of the powers $x^{2k-1}, x^{2k-2}, \dots, x^k$ in the expanded polynomial are

$$\begin{aligned} b_1 &= 2a_1 + R_1(p,q) = 0, \\ b_2 &= 2a_2 + R_2(p,q,a_1) = 0, \\ &\dots \\ b_k &= 2a_k + R_k(p,q,a_1,\dots,a_{k-1}) = 0, \end{aligned}$$

where every R_i is a certain algebraic expression involving p, q, $a_1, \dots, a_{k-1}$. The first of these equations implies that a_1 can be expressed in terms of p and q; the second equation says that a_2 can be expressed in terms of p, q, and a_1, and hence in terms of p and q only. Proceeding in this way, we conclude that all coefficients of a polynomial Q that commutes with P are uniquely expressed in terms of p and q. And this is precisely what we were supposed to prove.

It is easily verified that a similar argument is valid for any polynomial P of degree greater than 1 (provided that Q is unitary), so that assertion (b) is true for any such polynomial.

Assertion (b) is crucial for the whole problem, since the two remaining assertions (parts (c) and (d)) are its easy corollaries.

Solution to (c). Let us prove that the polynomial $Q(x) = P(P(x))$ commutes with $P(x)$. Indeed, $Q(P(x)) = P(P(P(x))) = P(Q(x))$. This polynomial Q is of degree 4 and, by assertion (b), is the only polynomial of degree 4 that commutes with P. In a similar way, one can prove that the only polynomial of degree 8 that commutes with P is $R(x) = P(P(P(x)))$.

Solution to (d). Set $S(x) = Q(R(x))$ and $T(x) = R(Q(x))$. Since P commutes with both Q and R, we have $P(S(x)) = P(Q(R(x))) = Q(P(R(x))) = Q(R(P(x))) = S(P(x))$. Thus, P commutes with S. For a similar reason, P also commutes with T. Furthermore, both S and T are unitary polynomials of the same degree (if Q and R have degrees k and l, then S and T are of degree kl). Now, assertion (b) implies that $S = T$, i.e., $Q(R(x)) = R(Q(x))$, q.e.d.

As with assertion (b), the present statement remains valid in the case where P is any polynomial of degree greater than 1 if both Q and R are unitary.

Chebyshev Polynomials: Solution to Problem (e).

Problem (e) is much more complicated than the others. We will give several approaches to its solution.

First approach. Let $x = t + t^{-1}$. It is then easy to check that x^k can be written as

$$\begin{aligned} x^k &= \left(t + t^{-1}\right)^k \\ &= \left(t^k + t^{-k}\right) + a_1\left(t^{k-1} + t^{-(k-1)}\right) \\ &\quad + a_2\left(t^{k-2} + t^{-(k-2)}\right) + \dots + a_{k-1}\left(t + t^{-1}\right) + a_k, \end{aligned}$$

where $a_1, \dots, a_k$ are well-defined numbers. By induction on k one can prove that $t^k + t^{-k}$ can be expressed as

$$x^k + b_1x^{k-1} + \dots + b_{k-1}x + b_k,$$

where again $b_1, \dots, b_k$ are certain fixed numbers. Denote this polynomial

$$x^k + b_1 x^{k-1} + \dots + b_{k-1}x + b_k$$

by $P_k(x)$. By definition, $P_k(t + t^{-1}) = t^k + t^{-k}$. Hence

$$P_k\left(P_l\left(t + t^{-1}\right)\right) = P_k\left(t^l + t^{-l}\right) = t^{kl} + t^{-kl} = P_{kl}(t + t^{-1}).$$

It follows that

$$P_k\left(P_l(x)\right) = P_{kl}(x) = P_l\left(P_k(x)\right),$$

i.e., any two of the polynomials P_k commute. Since moreover, $P_2(x) = x^2 - 2$, the desired sequence of polynomials has been constructed.

SECOND APPROACH. Here we explain how to construct polynomials P_k using *Chebyshev polynomials* T_k. Instead of giving a direct definition of these, we will specify a relation that they satisfy (and that determines them uniquely):

$$T_k(\cos t) = \cos kt.$$

It can be shown that T_k is a polynomial of degree k. Furthermore, Chebyshev polynomials commute, $T_k(T_m(x)) = T_{km}(x) = T_m(T_k(x))$. This follows from the simple fact that $\cos[k(mt)] = \cos kmt = \cos[m(kt)]$. However, T_k is not a unitary polynomial. Its leading coefficient is 2^{k-1}. From the point of view of the problem under study, this is a drawback. Fortunately, it can easily be fixed by stretching both the argument and the value of the function by a factor of 2, i.e., setting $P_k(x) = 2T_k\left(\frac{x}{2}\right)$. This procedure preserves the commutativity relations (check this!).

Thus, the remarkable sequence of Chebyshev polynomials, which appears naturally in various problems of calculus, specifically in the theory of approximation of functions by polynomials, turns out to be a sequence of commuting polynomials. It was precisely this method that E. Turkevich used to construct the sequence P_k.

Note that both approaches described so far are based on one and the same idea. Let f be a function that takes an infinite number of values and such that for every natural number n,

$$f(nt) = Q_n(f(t)),$$

where Q_n is a polynomial. Then for any two numbers m and n, the polynomials Q_m and Q_n commute. For example, if $f(t) = e^t$, then we get the sequence of commuting polynomials $F_n(x) = x^n$. If $f(x) = e^t + e^{-t}$, we get the sequence P_n (note that this is our first method of obtaining P_n, with t replaced by e^t). Finally, if $f(t) = \cos t$, we arrive at the sequence of polynomials T_n. Those who are acquainted with complex numbers and the formula

$$\cos\varphi = \frac{e^{i\varphi} + e^{-i\varphi}}{2}$$

will easily find an explanation of the fact that the functions $e^t + e^{-t}$ and $\cos t$ lead to essentially the same system of polynomials.

Both solutions of problem (e) given already are quite elegant, but both are imperfect in one way: It remains absolutely incomprehensible how one could have hit upon such a proof. We are going to give one more proof. It is longer than the first two, but in compensation there are no secrets about how it was discovered. Also, it gives a fast method of computing the sequence of polynomials P_n.

THIRD APPROACH. As we already know from part (b) of the problem, there can exist only one polynomial P_k of degree k that commutes with $P_2(x) = x^2 - 2$. Let us write down the beginning of the series:

$$\begin{aligned}
&P_1(x) = x,\\
&P_2(x) = x^2 - 2,\\
&P_3(x) = x^3 - 3x,\\
&P_4(x) = x^4 - 4x^2 + 2,\\
&P_5(x) = x^5 - 5x^3 + 5x,\\
&P_6(x) = x^6 - 6x^4 + 9x^2 - 2.
\end{aligned}$$

Here $P_4(x) = P_2(P_2(x))$, $P_6(x) = P_2(P_3(x))$, and $P_5(x)$ can be found by the direct procedure of problem (a). Looking at this table, one can guess the underlying rule, which is $P_{k+1}(x) = xP_k(x) - P_{k-1}(x)$. A natural conjecture is that this recurrence formula should be valid for all $k > 1$.

Thus, let us *define* the sequence $P_1, P_2, \dots, P_n, \dots$ inductively, setting

$$P_1(x) = x, \quad P_2(x) = x^2 - 2,$$

and for $k > 1$,

$$P_{k+1}(x) = xP_k(x) - P_{k-1}(x).$$

We are to prove that all these polynomials P_k commute with P_2. It will then follow, by assertion (d) above, that they commute with each other.

We proceed by induction on k. Clearly, the polynomials P_1 and P_2 commute with P_2. Assuming that all polynomials $P_1, P_2, \dots, P_k$ commute with P_2, we will prove that P_{k+1} also commutes with P_2.

We have to show that

$$P_{k+1}(x^2 - 2) = [P_{k+1}(x)]^2 - 2.$$

By virtue of the recurrence relation for P_{k+1}, this equality can be rewritten as

$$(x^2 - 2)P_k(x^2 - 2) - P_{k-1}(x^2 - 2) = \left[xP_k(x) - P_{k-1}(x)\right]^2 - 2.$$

By the induction hypothesis, this is equivalent to

$$(x^2 - 2)\left(\left[P_k(x)\right]^2 - 2\right) - \left(\left[P_{k-1}(x)\right]^2 - 2\right) = \left[xP_k(x) - P_{k-1}(x)\right]^2 - 2.$$

After removal of brackets and parentheses and trivial simplifications, this becomes

$$[P_k(x)]^2 - xP_k(x)P_{k-1}(x) + [P_{k-1}(x)]^2 = 4 - x^2.$$

Let $S_k(x)$ be the left-hand side of this equation. It remains to prove that $S_k(x)$ does not depend on k (and equals $4 - x^2$). Indeed, suppose that $k > 2$. Then

$$\begin{aligned}
S_k(x) &= [P_k(x)]^2 - xP_k(x)P_{k-1}(x) + [P_{k-1}(x)]^2\\
&= P_k(x)[P_k(x) - xP_{k-1}(x)] + [P_{k-1}(x)]^2\\
&= -P_k(x)P_{k-2}(x) + [P_{k-1}(x)]^2\\
&= [P_{k-2}(x)]^2 - xP_{k-1}(x)P_{k-2}(x) + [P_{k-1}(x)]^2\\
&= S_{k-1}(x).
\end{aligned}$$

Thus, $S_k(x) = S_{k-1}(x)$, and since $S_2(x) = 4 - x^2$, we have $S_k(x) = 4 - x^2$ for all $k \geq 2$. And this completes the proof.

Other Problems on Commuting Polynomials.

We will discuss several other problems related to the following general question: *Describe all pairs of commuting* (not necessarily unitary) *polynomials P and Q.*

PROBLEM 1. Prove that two polynomials P and Q of degree 1 commute if and only if either $P(x) = x + \alpha$, $Q(x) = x + \beta$ or there exists a number x_0 such that $P(x_0) = Q(x_0) = x_0$ (i.e., a common fixed point of the mappings P and Q).

PROBLEM 2. Find the answer to the general question in the case where the degree of one of the polynomials P and Q is 1.

In what follows, we will assume that both P and Q are polynomials of degree greater than 1.

Let

$$P(x) = a_0x^k + a_1x^{k-1} + \cdots + a_{k-1}x + a_k,$$
$$Q(x) = b_0x^l + b_1x^{l-1} + \cdots + b_{l-1}x + b_l.$$

Note first of all that it suffices to solve the problem in the case where both coefficients a_1 and b_1 are zero (polynomials with this property are referred to as *reduced*). This can be shown with the help of the following operation. Fix a number a, and for a given polynomial $R(x)$, define the new, *shifted* polynomial $R^{(a)}(x)$ according to the formula $R^{(a)}(x) = R(x-a)+a$. Clearly, the polynomial R can be recovered from the polynomial $R^{(a)}$: $R(x) = R^{(a)}(x+a) - a$.

PROBLEM 3.

(a) Prove that if the two polynomials P and Q commute, then the same is true of the two polynomials $P^{(a)}$ and $Q^{(a)}$.

(b) Prove that any pair of commuting polynomials P and Q of degree greater than 1 has the form $P = S^{(a)}$, $Q = T^{(a)}$, where a is a certain number, while S and T are a pair of commuting *reduced* polynomials.

In what follows, we will assume that both polynomials P and Q are reduced. Furthermore, we will suppose that they are unitary, i.e., have leading coefficient 1. This is the most interesting particular case. Furthermore, an argument similar to the one carried out above shows that the general problem can be reduced to the case where the leading coefficients of both P and Q are ± 1, so that this particular case does not differ much from the general case. (Instead of the shift operation, one must use the *stretching* operation defined by the formula $R^{\{\lambda\}}(x) = \lambda R\left(\frac{x}{\lambda}\right)$.) Here are several series of commuting polynomials:

1. Let R be a polynomial of degree r. Consider the polynomial sequence

$$P_0(x) = x,$$
$$P_1(x) = R(x),$$
$$P_2(x) = R(R(x)),$$
$$P_3(x) = R(R(R(x))),$$

and in general,

$$P_{i+1}(x) = P_i(R(x)).$$

Clearly, all the polynomials P_i commute, and the degree of P_i is r^i.

2. The series $F_k(x) = x^k$. All the polynomials F_k commute, and the degree of F_k is k.
3. The series $\{P_k\}$ constructed above as the solution to problem (e). These polynomials are defined by the condition $P_k(t+t^{-1}) = t^k+t^{-k}$. The degree of P_k is k.
4. The sequence of polynomials $H_1, H_3, H_5, \dots$ defined by the condition $H_k(t-t^{-1}) = t^k - t^{-k}$ for odd k. You can check that these polynomials exist and are uniquely determined by the condition mentioned. All these polynomials commute, and the degree of H_k is k.

Actually, examples 3 and 4 are particular cases of a more general construction. To describe it, we need to make a remark concerning the coefficients of polynomials. So far, we have tacitly supposed all coefficients to be real numbers. However, in a large class of algebraic problems it is better to work with complex numbers instead. Therefore, let us assume from now on that the coefficients of the polynomials under study are arbitrary complex numbers.

5. Fix a natural number m and a complex number λ such that $\lambda^m = 1$ (for any m, there exist $m-1$ such numbers different from 1).

   Consider the pairs of numbers (u, v) such that $u \cdot v = \lambda$ and put $x = u+v$. It is readily verified that

$$u^k + v^k = x^k + a_1x^{k-1} + \cdots + a_k,$$

   where $a_1, \dots, a_k$ are certain numbers determined by λ. Set

$$P_k(x) = x^k + a_1x^{k-1} + \cdots + a_k.$$

   The polynomial P_k is characterized by the property $P_k(u+v) = u^k+v^k$ whenever $uv = \lambda$.

   Let l be any number having remainder 1 after division by m. Then $u^lv^l = (uv)^l = \lambda^l = \lambda$, so that $P_k(u^l + v^l) = u^{kl} + v^{kl}$. Therefore, if both k and l have remainder 1 upon division by m, we have

$$P_k(P_l(u+v)) = u^{kl} + v^{kl} = P_l(P_k(u+v)),$$

   which means that the polynomials P_k and P_l commute. From a given λ, we have thus constructed the following series of commuting polynomials: P_1, P_{m+1}, $P_{2m+1}, \dots$. All these polynomials are unitary and reduced, and the degree of P_k is k. When $m = 1$, $\lambda = 1$, we get example 3; when $m = 2$, $\lambda = -1$, we get example 4.

Examples 1 through 5 include all known examples of commuting polynomials, so that we can make the following conjecture: If P and Q are two commuting polynomials with complex coefficients of degree greater than 1, then they form part of a series of polynomials that falls under the construction of one of the examples 1, 2, or 5 above.

Instead of trying to solve the general problem, another thing we might do is to find an answer to the following partial questions:

1. For what values of α does there exist a polynomial of odd degree that commutes with the polynomial $P(x) = x^2 - \alpha$?
2. Let P be a unitary polynomial of degree greater than 1. Consider the set of degrees of all polynomials that commute with P. What kind of subsets of

the natural numbers can occur in this way? For instance, in example 1 we had a geometric progression, and in example 5, an arithmetic progression.

3. Let P and Q be commuting polynomials of degrees k and l, respectively. Suppose that k divides l. Is it true that Q must be of the form $Q(x) = P(R(x))$, where R is a unitary polynomial that commutes with P?

One can also consider a more general problem—that of finding all pairs of *rational functions* P and Q that commute. In this case, many new and fascinating examples come into view.

The general approach we mentioned while discussing the problem (e) above is also valid here. Suppose that f is a function that takes infinitely many values and has the property

$$f(nt) = P_n(f(t)),$$

where P_n is a rational function. Then for arbitrary n and m the functions P_n and P_m commute.

An exciting question is to find the functions f with the property that for any n there exists a rational function P_n such that $P_n(f(t)) = f(nt)$. You can easily check that one example is given by the function $f(t) = \tan t$.

Other examples of such functions can be constructed using the theory of elliptic functions. Since the latter is essentially nonelementary, we will not touch upon it here.

All these examples show that the problem of describing all pairs of commuting polynomials (and, more generally, rational functions) is directly related to profound and beautiful mathematical theories. A complete solution of this problem, when found, will reveal some unknown facts. In short, this is a problem worth working on.

Translated by N. K. KULMAN