Trebenko D.Ya., Trebenko O.O.

Existence theorems in Algebra and Number theory course

Trebenko Dmytro Yakovych, Ph. D. in Physics and Mathematics, Associate Professor
Trebenko Oxana Olexandrivna, Ph.D. in Physics and Mathematics, Associate Professor
National Pedagogical Dragomanov University, Kyiv, Ukraine

Abstract. Emphasized in the paper is a fact that an approach proposed in some textbooks in higher algebra for proving existence theorems is not correct. To remedy the situation authors propose to introduce into consideration Theorem 1 (its proof is given). The use of this theorem is illustrated by the following example: considered is a proof of theorem on existence of a ring of polynomials in one variable over a commutative ring with unity. Authors' approach makes it possible to eliminate some logical gaps of the course, provides a means for proving the most complicated theorems of the course by unified scheme (in 5 steps), sets force the exposition of theoretical material in a manner more precise, clear, structured and comprehensible.

***Keywords** and phrases: existence theorem, construction of a ring of polynomials*

Existence theorem is a theorem stating that under certain conditions there exists a solution of a mathematical problem or there exists a certain mathematical object (such as a solution of some equation, a derivative, an expansion of some field). Without any doubt, existence theorems are the highest achievements of mathematical science, because in most cases to investigate a given mathematical object (under certain conditions), to establish its properties is much more easier than to show that such an object exists at all. A proof of such theorems is usually very nice, elegant but at the same time quite complicated. Not infrequently search for a proof of existence theorem lasts for not even decades but centuries; as a result new methods are developed and even new fields of mathematical science emerge.

It is sufficient to recall that such outstanding theorems as Fundamental Theorem of Algebra (on existence of complex root of a non-constant single-variable polynomial with numerical coefficients) and Fermat's Last Theorem (on existing of nontrivial integer solution of the equation $x^n + y^n = z^n$, $n > 2$) are existence theorems. The search for strict proof of Fundamental Theorem of Algebra contributed to the origin of abstract group theory and field theory, and Fermat's Last Theorem spurred the development of ring theory (see, e.g., [3, ch. IV-V]). Still unproven and unanswered problems as Goldbach conjecture (that every even integer greater than 2 can be expressed as the sum of two primes) and twin prime conjecture (that there are infinitely many pairs of primes whose difference is 2), Legendre's conjecture (stating that there is a prime number between n^2 and $(n+1)^2$ for every positive integer n) and Inverse Galois problem (on existence of a field extension of the rational field Q with a given finite group as Galois group) are also existence theorems.

There are quite a lot of existence theorems in Algebra & Number Theory Course. These are theorems asserting an existence of representations of expressions in some specific forms and theorems on existence of certain algebraic objects. From them we set off the following:

A. Theorem on existing of a ring of polynomials in one variable over a commutative ring K with unity;
B. Theorem on existing of an extension field of a field K in which a given polynomial with coefficients in K has a root (Kronecker's Theorem);
C. Theorem on existence of a field of fractions of an integral domain K;
D. Theorem on existence of a ring of polynomials in several variables over a commutative ring K with unity.

To develop methods of studying Theorems A.-D. is a problem that deserves special attention and in-deep study, because of proofs of these theorems being extremely complicated and bulky.

An additional point to emphasize is that in modern Higher Algebra textbooks used in the proofs of mentioned theorems is an approach, though rightful, but not enough well-grounded: a ring (field) L' with required properties is constructed not for the given ring (field) K but for its isomorphic image K' (and besides $L' \cap K = \varnothing$, although by definition an inclusion $L' \supseteq K$ is needed).

To clear essence of the problem let us consider, for example, the proof of Theorem A. in the textbooks [1, 5, 6]. The problem is: *given* a commutative ring K with unity, *prove* that a ring of polynomials in one variable over K exists. To prove this, a set $\tilde{L}$ of infinite sequences $f = (a_0, a_1, a_2, ..., a_n, 0, 0, ...)$ where $a_i \in K$ for all $i \in \overline{0, n}$, $n \in \mathrm{N} \cup \{0\}$, in which all members starting with some one are zeroes (of the ring K), is considered. On this set operations $\oplus, \odot$ are defined (by some rules) and then a proof of the fact that the triaple $\langle L; \oplus, \odot \rangle$ is a commutative ring with unity, containing a subring $\langle K'; \oplus, \odot \rangle$ isomorphic to the ring $\langle K; +, \cdot \rangle$, is carried out.

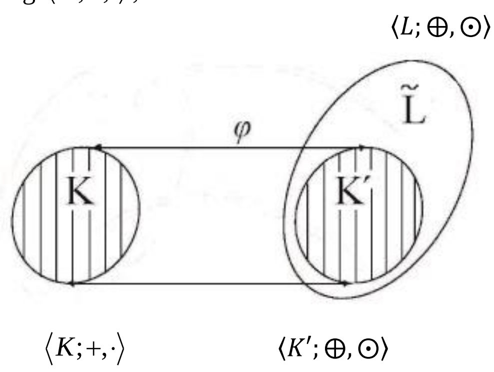

Fig.1

And next ... are isomorphic rings $\langle K'; \oplus, \odot \rangle$ and $\langle K; +, \cdot \rangle$ identified and the ring L' is called a ring of polynomials in one variable (RPOV) over the ring K. (Although, in fact, the ring L' is a RPOV over K', because K' is a subring of the ring L', and not K). In other words, this approach gives a RPOV not for the given ring K but for its isomorphic image K'.

But why the existence of RPOV over K' implies the existence of RPOV over K? In the textbooks [1, 5, 6] it is argued as follows: ,,since isomorphic rings K and K' are undifferentiated in terms of addition and multiplication operations defined on them, we can identify each element of the ring K' with its proimage under the isomorphism $\varphi : K \to K'$; assume $(a,0,0,...) = a$ for any $a \in K$. Under such identification of elements of the rings K and K', the ring K *becomes a subring* of the ring L'". Such an argument is not correct! Really, since a subring of the ring is by definition a subset of the ring set, this implies that the set of elements $a_i \in K$ is a subset of the set of sequences $(a_0, a_1, a_2, ..., a_n, 0, 0, ...)$!

To eliminate this logical gap authors propose to introduce into consideration the following proposition.

Theorem 1. Let $\langle K;+,\cdot\rangle$ and $\langle L';\oplus,\odot\rangle$ be rings having no common elements and let the ring L' contain a subring K' isomorphic to the ring K. Then there exists a ring $\langle L;+,\cdot\rangle$ isomorphic to the ring L' for which K is a subring.

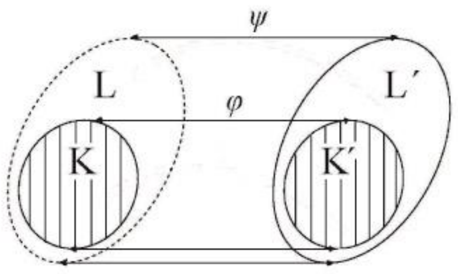

Fig.2

Proof. Since $K' \cong K$, there exists an isomorphism $\varphi : K' \xrightarrow{onto} K$. Let $\varphi(a') = a \in K$ for all $a' \in K'$. Consider a set

$$L = K \cup (L' \setminus K') = \{x \mid x \in K \text{ } or \text{ } x \in L' \setminus K'\}.$$

Under the conditions of the theorem $K \cap (L' \setminus K') = \varnothing$. Put a map $\psi : L' \to L$ in the following way: for an arbitrary $x' \in L'$

$$\psi(x') = \begin{cases} \varphi(x') = x & if \ x' \in K', \\ x' & if \ x' \in L' \setminus K'. \end{cases}$$

Since $K \cap (L' \setminus K') = \varnothing$ and the mapping $\varphi : K' \xrightarrow{onto} K$ is a one-to-one correspondence, it follows that the map ψ from the set L' onto the set L is also a one-to-one correspondence.

On the set L for all elements in K operations $+$ and $\cdot$ are already defined. Define operation on L in such a manner that they agree with ones defined on K. Let x, y be arbitrary elements of L, x', y' be their proimages under the map ψ, i.e. $x = \psi(x')$, $y = \psi(y')$. Set

$$x + y = \psi(x' \oplus y'), \qquad x \cdot y = \psi(x' \odot y'). \qquad (1)$$

Operations introduced in such a way agree with operations defined on K. Indeed, if $x, y \in K$ then in K' there exist elements x', y' such that $x = \varphi(x')$, $y = \varphi(y')$, $x' \oplus y' \in K'$, and hence

$$\psi(x' \oplus y') = \varphi(x' \oplus y') = \varphi(x') + \varphi(y') = x + y.$$

Similarly $\psi(x' \text{e } y') = x \cdot y$. $\psi(x' \odot y') = x \cdot y$

Show that the operations $+$ and $\cdot$ are binary algebraic on L. Indeed, for arbitrary $x, y \in L$ their proimages x' and y' under the map ψ in L' exist (since ψ is a one-to-one correspondence from L' onto L). The operations $\oplus$ and $\odot$ are binary algebraic on the set L' therefore the element $x' \oplus y'$ always exists, is unique and belongs to L'. But then the element $\psi(x' \oplus y') = x + y$ also exists always, is unique and belongs to L. This means that the operation $+$ is closed, has exactly one output and always can be done (i.e. is binary algebraic) on L. Analogously the operation $\cdot$ is binary algebraic on L.

Show that ψ is an isomorphism from L' onto L. Since ψ is one-to-one map from L' onto L, it remains to show that ψ preserves operations. Taking into account the setting of the operations $+$ and $\cdot$ on L (1), for arbitrary $x', y' \in L'$ we have:

$$\psi(x' \oplus y') = x + y \quad \text{where } x = \psi(x'), y = \psi(y'),$$

i.e. $\psi(x' \oplus y') = \psi(x') + \psi(y')$.

Similarly $\psi(x' \odot y') = \psi(x') \cdot \psi(y')$. Thus ψ preserves operations, so that by definition ψ is an isomorphism from the ring $\langle L';\oplus,\odot\rangle$ onto the set L. Since on L operations $+$ and $\cdot$ are binary algebraic, by proposition 5.3.2 ch.II [3] $\langle L;+,\cdot\rangle$ is a ring.

Thus the constructed ring $\langle L;+,\cdot\rangle$ is isomorphic to the ring $\langle L';\oplus,\odot\rangle$ and contains the subring $\langle K;+,\cdot\rangle$. Theorem is proven.

In view of this theorem, to prove for the given ring K an existence of some ring L possessing required properties it is sufficient to show that there exists a ring L', which has a subring K' isomorphic to K and with respect to K' possesses required properties.

Moreover, introduction of this theorem is of high value from the methodological point of view for it gives a possibility to prove Theorems A.-D. by the same scheme (in 5 steps). Namely, to prove an existence of some ring L for the given ring K one need only:

I. To construct a ring L' (to consider some set, to define operations $\oplus$ and $\odot$ on it and to show that $\langle L';\oplus,\odot\rangle$ is a ring).

II.To select some subset K' of the ring L' and to show that

K' is a subring of the ring L'.

III. To prove that $K' \cong K$.

IV. To show that the ring L' possesses required properties with respect to K'.

V. Taking into account Theorem 1, to assert that there exists a ring L which has required properties with respect to the ring K.

The scheme of proof should be formulated separately.

Accentuated scheme enables a partially-searching method to be used to consider the proof of Theorems A.-D. Heuristic conversation when students actively assist in proving some steps, intensifies cognitive activity, leads to insight of learning material, helps to identify causal relationships and to evaluate arguments critically, creates an atmosphere of general interest, influences positively on the development of thinking.

It is necessary to emphasize particular value of the demonstration of Figure 2. As psychologists' investigations indicate, for a considerable percent of people an imaginative thinking predominates over an abstract one, it is difficult for them to perceive an abstract material without relying on images. There are such people among mathematicians as well (in particular, among many geometers). For such students visual interpretation of abstract algebraic relations and dependencies is just a necessity. And generally speaking, as correctly notices V.S.Rotenberg [2], ``thinking, free of imagery elements, has a risk to become dry, formal. Learning, not addressed to imaginative thinking, not only doesn't contribute to its development, but eventually suppresses it".

Figure demonstration should start considering each of Theorems A.-D. In such a way, figure acts as a guiding line for theorems proven by scheme I-V.

As an illustration of approach proposed, let us consider Theorem A.

Introduction of the statement of Theorem A. is carried out using the abstract-deductive method: theorem is formulated by a lecturer. At the same time, a need of consideration of this proposition should be convinced, for example, as follows: "As we see, if for the ring K there exist some ring L containing K as a subring and some transcendental over K element, then for the ring K a ring of polynomials in one variable over K exists. Up till now, we considered only a case when the ring is given in advance. But does such ring L exist for each ring K? Indeed, the following theorem is valid". Formulate a statement of the theorem:

Theorem A. *For any commutative ring K with unity a ring of polynomials in one variable over K exists.*

We propose to organize exposition of the proof in the following way. At first, show schematically:

1) a given ring K;

2) a ring L' (so that $L' \cap K = \varnothing$);

3) a ring K' (shaped like K) (Fig. 3);

4) an isomorphism φ from the ring K' onto the ring K (Fig. 4);

5) draw a ring L, which existence has to be proven, stippled (Fig.5).

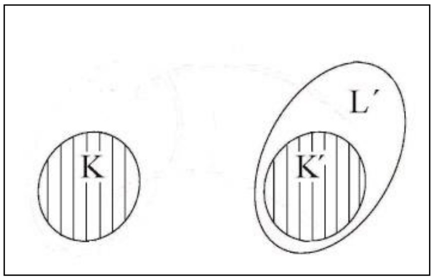

Fig. 3

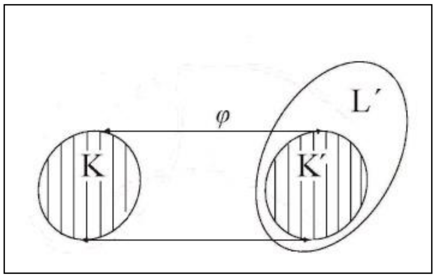

Fig. 4

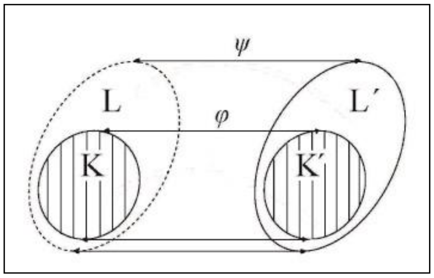

Fig. 5

A lecturer stresses that Theorem A. and similar ones will be proven by scheme I-V. When considering Theorems A.-D. students immediately after the figure demonstration propose the proof scheme.

I. Construct a ring L'.

A set L' and operations $\oplus, \odot$ on it are defined by a lecturer. But to show that, really, the set L' under the operations $\oplus$ and $\odot$ is a ring (field), students are able. They know two main ways to check if a given algebraic structure $\langle L', \oplus, \mathrm{e} \rangle$ is a ring (field): by definition of a ring (field) and by subring (subfield) criterion. The lecturer asks: "How one can prove that $\langle L'; \oplus, \odot \rangle$ is a ring?" and then emphasizes that the subring (subfield) criterion is not applicable in this case: a ring $\langle M; \oplus, \odot \rangle$ such that $M \supseteq L'$ is unknown. Checking the ring (commutative with unity) axioms is carried out collectively.

Let K be a ring with operations $+$ and $\cdot$, 0 and 1 are a zero and a unity of the ring K respectively. Consider a set L' of all infinite sequences

$F = (a_0, a_1, a_2, \ldots)$ where $a_i \in K$ for all $i = 0, 1, ..., n, ...$

every sequence consisting of zeros from some term onwards (this term may be different for different sequences). Clearly, $L' \neq \varnothing$.

Two sequences $F = (a_0, a_1, a_2, \ldots)$ and $G = (b_0, b_1, b_2, \ldots)$ are assumed to be equal iff $a_i = b_i$ for all $i = 0, 1, 2, ...$.

On the set L' define operations $\oplus$ and $\odot$ in the following way: for arbitrary two elements $F = (a_0, a_1, a_2, \ldots)$ and $G = (b_0, b_1, b_2, \ldots)$ of the set L' put:

$$F \odot G = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots$$

$$F \oplus G = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots);$$

$$F \mathrm{e}\, G = (d_0, d_1, d_2, \ldots) \text{ where } d_k = \sum_{i=0}^{k} a_i b_{k-i}$$

(or in the other form $d_k = \sum_{i+j=k}^{k} a_i b_j$)

Show that $\langle L'; \oplus, \odot \rangle$ is a commutative ring with unity. We have:

1) The operation $\oplus$ is binary algebraic on L' since it can always be done and has exactly one output (this follows from the fact that the operation $+$ can always be done on K and has exactly one output). Next, the operation $\oplus$ is closed on L' since $a_i + b_i \in K$ for all $i = 0,1,2,...$ and the sequence $F \oplus G$ consisting of zeros from some term onwards. (Indeed if for sequences F and G conditions $a_r = a_{r+1} = ... = 0$ and $b_l = b_{l+1} = ... = 0$ hold then for $s = \max\{r, l\}$ we obtain: $a_s + b_s = a_{s+1} + b_{s+1} = ... = 0$).

2) Let $H = (c_0, c_1, ..., c_i, ...) \in L'$. The operation $\oplus$ is associative on L':

$(F \oplus G) \oplus H = \big((a_0, a_1, \ldots a_i, \ldots) \oplus \big((b_0, b_1, \ldots b_i, \ldots)\big) \oplus (c_0, c_1, \ldots c_i, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_i + b_i, \ldots) \oplus \big(c_0, c_1, \ldots, c_i, \ldots = \big((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, \ldots, (a_i + b_i) + c_i, \ldots\big) = (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), \ldots a_i + (b_i + c_i\big), \ldots) = F \oplus (G \oplus H)$,

since the operation $+$ is associative on K.

3) An element $O = (0, 0, ..., 0, ...)$ is a zero of L'.

4) An element $! F = (-a_0, -a_1, ..., -a_i, ...)$ is an additive inverse of F in L'.

5) The operation $\oplus$ is commutative on L':

$F \oplus G = (a_0 + b_0, a_1 + b_1, ..., a_i + b_i, ...) = (b_0 + a_0, b_1 + a_1, ..., b_i + a_i, ...) = G \oplus F$,

since the operation $+$ is commutative on K.

6) The operation $\odot$ is binary algebraic on L' since it can always be done and it has exactly one output (because the operation $\cdot$ can always be done on K and has exactly one output). And also it is closed: if d_k is a k-th member of the sequence $F \odot G$ then $d_k = \sum_{i=0}^{k} a_i b_{k-i} \in K$.

Besides, if $a_r = a_{r+1} = ... = 0$, $b_l = b_{l+1} = ... = 0$ then

$$d_{r+l} = \sum_{i=0}^{k} a_i b_{r+l-i} = a_0 b_{r+l} + a_1 b_{r+l-1} + ... + a_r b_l + a_{r+1} b_{l-1} + ... + a_{r+l} b_0 = 0$$

and analogously $d_{r+l+1} = d_{r+l+2} = ... = 0$.

7) Let $H = (c_0, c_1, c_2, ...) \in L'$. Then $F \odot G = (d_0, d_1, d_2, \ldots)$ where $d_k = \sum_{i+j=k} a_i b_j$ and

$$(F \odot G) \odot H = (d_0, d_1, d_2, \ldots) \odot (c_0, c_1, c_2, \ldots) = \\ = (u_0, u_1, u_2, \ldots)$$

where $u_s = \sum_{k+l=s} d_k c_l = \sum_{k+l=s} \sum_{i+j=k} (a_i b_j) c_l = \sum_{i+j+l=s} (a_i b_j) c_l$.

From the other hand, $G \odot H = (q_0, q_1, q_2, \ldots)$ where $q_k = \sum_{j+l=k} b_j c_l$ and

$$F \odot (G \odot H) = (a_1, a_2, a_3, \ldots) \odot (q_1, q_2, q_3, \ldots) = \\ = (v_1, v_2, v_3, \ldots)$$

where $v_s = \sum_{i+k=s} a_i v_k = \sum_{i+k=s} \sum_{j+l=k} a_i (b_j c_l) = \sum_{i+j+l=s} a_i (b_j c_l)$.

Since the operation $\cdot$ is associative on K, namely $(a_i b_j) c_l = a_i (b_j c_l)$ for all $i, j, l \in \mathrm{N} \cup \{0\}$, then $u_s = v_s$ for all $s = 0, 1, 2, \ldots$, hence $(F \odot G) \odot H = F \odot (G \odot H)$.

8) The operation $\odot$ is distributive over the operation $\oplus$. Indeed, if

$$F \odot (G \odot H) = F \odot (b_0 + c_0, b_1 + c_1, b_2 + c_2, \ldots) = \\ = (p_0, p_1, p_2, \ldots$$

where $p_k = \sum_{i=0}^{k} a_i (b_{k-i} + c_{k-i})$,

$$(F \odot G) \oplus (F \odot H) = (d_0, d_1, d_2, \ldots) \oplus (w_0, w_1, w_2, \ldots) = \\ = (z_0, z_1, z_2, \ldots)$$

where $d_k = \sum_{i=0}^{k} a_i b_{k-i}$, $w_k = \sum_{i=0}^{k} a_i c_{k-i}$, $z_k = d_k + w_k$,

then $z_k = d_k + w_k = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i} = \sum_{i=0}^{k} (a_i b_{k-i} + a_i c_{k-i})$.

Since the operation $\cdot$ is distributive over the operation $+$ on K, we have $a_i b_{k-i} + a_i c_{k-i} = a_i (b_{k-i} + c_{k-i})$, this implies

$z_k = \sum_{i=0}^{k} (a_i b_{k-i} + a_i c_{k-i}) = \sum_{i=0}^{k} a_i (b_{k-i} + c_{k-i}) = p_k$ for all $k = 0, 1, 2, ...$ Thus $F \odot (G \oplus H) = (F \odot G) \oplus (F \odot H)$.

9) The operation e is commutative on L' since if $F \odot G = (d_0, d_1, d_2, \ldots)$ where $d_k = \sum_{i+j=k} a_i b_j$, and $G \odot F = (m_0, m_1, m_2, \ldots)$ where $m_k = \sum_{j+i=k} b_j a_i$, taking into account that the operation $\cdot$ is commutative on K we obtain that

$$m_k = \sum_{j+i=k} b_j a_i = \sum_{i+j=k} a_i b_j = d_k \text{ for all } k = 0, 1, 2, ...$$

10) The sequence $E = (1, 0, 0, ...)$ is a unity.

Since K is a ring with unity, this implies $1 \neq 0$, therefore $O \neq E$. By definition $\langle L'; \oplus, \odot \rangle$ is a commutative ring with unity.

II. As an experience shows, in proving Theorem A. students aren't able to select a subset K' of the ring L' satisfying the conditions: 1) $\langle K'; \oplus, \odot \rangle$ is a ring and 2) $K' \cong K$. Perhaps, an intuition will suggest the right way in proving Theorems B.-D., but it is unlikely to occur dealing with this kind of proof for the first time (in addition to that the operation e is defined a bit unusual, bulky). Therefore a subset K' is suggested by a lecturer. But on the other hand a proof of K' to be a subring of the ring L' is conducted collectively.

In the ring L' select a subset K' consisting of the elements $(a,0,0,...)$. Show that K' is a subring of the ring L'. Since $K' \neq \varnothing$ (e.g., $O \in K'$), use a subring criterion.

Let $A, B \in K'$, then $A = (a,0,0,...)$, $a \in K$, $B = (b,0,0,...)$, $b \in K$. We have:

1) $A \oplus B = (a+b,0,0,...) \in K'$ since $a+b \in K$.

2) For the element A in L' the element $! A = (-a,0,0,...)$ is an additive inverse. Since $-a \in K$ it follows that $(-a,0,0,...) \in K'$.

3) $A \odot B = (ab, 0,0, ...) \in K$ since $ab \in K$.

The conditions 1)-3) of the subring criterion are satisfied, therefore K' is a subring of the ring L'.

III. Show that the ring K' is isomorphic to the ring K.

What element of K is a sequence $(a,0,0,...)$ from K' to be mapped into? Naturally the first idea is to check if the map φ defined by the rule: $\varphi\big((a,0,0,...)\big) = a$ is an isomorphism. Algorithm to check (by definition) is known to students, they actively help.

1) for an arbitrary element $(a,0,0,...) \in K'$ its image $\varphi\big((a,0,0,...)\big)$ belongs to K (by setting of the rule φ); since $(a,0,0,...) = (b,0,0,...)$ iff $a = b$, the image $\varphi\big((a,0,0,...)\big)$ is unique;

2) for an arbitrary element $c \in K$ the element $(c,0,0,...)$ is its proimage in K';

3) let $(a,0,0,...),(b,0,0,...) \in K'$ then

$$\varphi\big((a,0,0,...) \oplus (b,0,0,...)\big) = \varphi\big((a+b,0,0,...)\big) = a+b,$$

$$\varphi((a,0,0,...) \text{ e } (b,0,0,...)) = \varphi(ab,0,0,...) = ab;$$

$$\varphi\big((a,0,0,...) \oplus (b,0,0,...)\big) = \varphi\big((a+b,0,0,...)\big) = a+b,$$

$$\varphi\big((a,0,0,...) \odot (b,0,0,...)\big) = \varphi\big((ab,0,0,...)\big) = ab;$$

4) let $(a,0,0,...),(b,0,0,...) \in K'$, $(a,0,0,...) \neq (b,0,0,...)$. Then, taking into account the condition of two sequences to be equal, $a \neq b$, hence $\varphi\big((a,0,0,...)\big) \neq \varphi\big((b,0,0,...)\big)$.

By definition, φ is an isomorphism from the ring K onto the ring K', i.e. $K \cong K'$.

It is relevant to remark that although proof algorithms for steps I-III (namely, checking axioms of the ring definition (I), conditions of the subring criterion (II), axioms of homomorphism definition (III)) are well known to students, it is not advisable to leave these steps to independent study. The way to organize notes when proving Theorem A. should be a pattern to theorems having proof by scheme I-V. Moreover, thorough, detailed proof provides education links between individual chains of proof.

IV. Show that the ring L' is a ring of polynomials in one variable (RPOV) over K'.

At this stage, no sufficient condition is known for students apart from definition, therefore the right way to prove (checking the conditions of the definition) is immediately offered by them.

Remark that in most textbooks the definition of RPOV is introduced implicitly (that is the content of RPOV concept is established through context): primarily a set $K[x]$ is constructed, then it is proven that $K[x]$ is a ring (under some operations), the ring obtained is called a ring of polynomials in one variable x over K ([1,5,6]). This definition does not give a direct indication of essential characteristics of RPOV concept.

There is no single, unified approach to introduction of RPOV concept, also there are different RPOV definitions. For example, in the textbook [6] for RPOV over K a simple transcendental extension of the ring K is called, in the textbook [5] -- a ring of sequences is termed. Accordingly, different conditions are set for checking.

In this paper we take as a basis an authors' approach to introduce RPOV concept (which was proposed in [4]). In accordance with it, given a commutative ring K with unity, a ring of polynomials in one variable x over K is a ring $\langle K[x];+,\cdot\rangle$ possessing the following properties:

1) $K[x]$ contains the ring K as a subring;

2) in $K[x]$ there exists a transcendental over K element x;

3) each element f of the ring $K[x]$ can be presented in the form $f = a_0 + a_1 x + ... + a_n x^n$ where $a_i \in K$ for all $i = 0,1,...,n$, $n \in \mathrm{N} \cup \{0\}$.

The conditions 1)-3) are reproduced by students and a lecturer concretizes them on the case of Theorem A.: to prove that constructed ring L' is a RPOV over K', it is sufficient to show that:

1) L' contains K' as a subring;

2) in L' there exists a transcendental over the ring K' element X;

3) an arbitrary element f of the ring L' can be presented in the form $F = A_0 \oplus A_1 \odot X \oplus ... \oplus A_n \odot X$ where $a_i \in K$ where $A_i \in K'$ for all $i = 0,1,...,n$, $n \in \mathrm{N} \cup \{0\}$.

Validity of condition 1) is already established (p.**II**). It remains to check if the conditions 2) and 3) hold. The most difficult thing here is, certainly, to choose a transcendental element X. Problem exposition can be organized, for example, in the following manner.

Lecturer: What elements of the ring L' aren't transcendental over K' definitely and therefore they cannot be chosen for X?

Students: Elements of the ring K'.

L: That is, elements of the form

S: $(a_0,0,0,0,...)$ where $a_0 \in K$.

L: Thus a transcendental element should be searched among sequences having at least one coordinate a_i, $i \neq 0$, nonidentity. Let's investigate some sequence of such kind. For example, try the element $(0,1,0,0,...)$.

(Remark that in such a way there is also a possibility to emphasize that actually in L' not only one transcendental over K' element may exist).

L: How to determine if the element $X = (0,1,0,0,...)$ is algebraic over K' or transcendental?

S: To consider the equality

$$B_0 \oplus B_1 \odot X \otimes \dots \otimes B_m \odot X^m = O \qquad (2)$$

where $B_i \in K'$ for all $i = 0,1,\dots,m$.

L: Expand this equality. Since $B_i \in K'$ then $B_i = (b_i, 0, 0, \dots)$ for some $b_i \in K$. Find the powers X^i. We have:

$X^2 = X \odot X = (0,1,0,0,\dots) \odot (0,1,0,0,\dots) = (0,0,1,0,0,\dots)$,
$X^3 = X^2 \odot X = (0,0,1,0,0,\dots) \odot (0,1,0,0,\dots) =$
$= (0,0,0,1,0,0,\dots), \dots$

What is X^i in your opinion?

S: $X^i = (\underbrace{0,0,\dots 0}_{i},1,0,\dots)$.

L: Let's prove it. We may proceed

S: by induction.

Show that $X^i = (\underbrace{0,0,\dots 0}_{i},1,0,\dots)$ for all $i \in \mathrm{N}$. For $i = 1$ this equality is valid. Assume that for $i - 1 \geq 1$ the following holds: $X^{i-1} = (\underbrace{0,0,\dots 0}_{i-1},1,0,\dots)$. Then

$$X^1 = (X^{i-1}) \odot X = (\underbrace{0,0,\dots 0,}_{i-1} 1,0,\dots) = (\underbrace{0,0,\dots 0}_{i}, 1,0,\dots)$$

By principle of mathematical induction the equality is valid for an arbitrary $i \in \mathrm{N}$.

L: Now find the product $B_i \odot \mathrm{X}^i$:

$$B_i \odot X^i = (b_i, 0,0,\dots) \odot (\underbrace{0,0,\dots 0}_{i}, 1,0,\dots) =$$
$$= (\underbrace{0,0,\dots 0}_{i}, b_i, 0, \dots)$$

Then

$$B_0 \oplus B_1 \odot X \oplus \dots \oplus B_m \odot X^m =$$
$$= (b_0, 0,0,\dots) \oplus (0, b_0, 0, \dots) \oplus \dots \oplus (\underbrace{0,0,\dots 0}_{m}, b_m, 0, \dots) =$$
$$= (b_0, b_1, \dots, b_{im}, \dots)$$

From (2) we have: $(b_0, b_1, \dots, b_m, 0, \dots) = (0,0,\dots)$ whence $b_0 = b_1 = \dots = b_m = 0$. Then $B_i = (0,0,0,\dots) = O$ for all $i = 0,1,2,\dots$. Thus the equality (2) is possible if and only if $B_0 = B_1 = \dots = B_m = O$. This means that

S: X is transcendental over K'.

L: Thus the condition 2) of RPOV definition holds. Show that the condition 3) is valid.

3) Let $F = (a_0, a_1, a_2, \dots)$ be an arbitrary element of the ring L'. If $F = O$ then proposition is correct (for example, under $n = 0$ and $A_0 = O$). Let $F \neq O$ then there is an index $n \in \mathrm{N} \cup \{0\}$ such that $a_n \neq 0$ and $a_{n+1} = a_{n+2} = \dots = 0$. We have:

$$F = (a_0, a_1, \dots, 0, \dots)$$
$$= (a_0, 0,0,\dots) \oplus (0, a_1, 0, \dots) \oplus \dots \oplus \left(\underbrace{0,0,\dots,0}_{mn}, a_n, 0, \dots\right)$$
$$= A_0 \oplus A_1 \odot X \oplus \dots \oplus A_n \odot X^n$$

where $A_i = (\underbrace{0,0,\dots,0}_{i}, a_i, 0, \dots) \in K'$ for all $i = 0,1,\dots,n$.

The condition 3) of RPOV definition holds, thus L' is a ring of polynomials in one variable over K'.

V. To complete the proof, it is sufficient to refer to Theorem 1.

Since $K' \cong K$ (p.**III**), by Theorem 1 there exists a ring L such that $L \cong L'$, for which K is a subring. The ring L, in view of p.**IV**, is a ring of polynomials in one variable over K. The theorem is proven.

For students to master the proof, when ending with its consideration a lecturer briefly repeats an analysis of the proof structure emphasizing those mathematical facts that were used to argue each step by itself (of course, it is advisable to involve students at most in discussions). Final discussion promotes conscious perception of the proof, provides fundamental understanding of the main relationships in general.

Note that in consideration of the proof of existence theorem the use of partially searching method is not even desirable but just needed. Such extensive proof without discussion will scare off students, they will copy notes from the blackboard without trying to catch an idea. This will be just a waste of time (for, as it is known from the psychological investigations, to make two kinds of activity each requiring full concentration – to take notes and to penetrate into the essence of the proof – is impossible). On the contrary, accentuated proof scheme with the instructions on the way of proof for each separate step and the propositions used allows one to reduce such complex proof to the consideration of standard problems with a method of solution well-known for students. These are such problems as:

Problems:	Method of solution:
1. Show that $\langle L'; \oplus, \odot \rangle$is a ring (field).	By ring (field) definition: Show that the axioms of the ring (field) definition are valid.
2. Show that a subset K' of the ring $\langle L'; \oplus, \odot \rangle$is a subring (subfield) of this ring (field).	By subring (subfield) criterion: Show that the conditions of the subring (subfield) criterion are fulfilled.
3. Show that a subring (subfield) K' is isomorphic to the given ring (field) K.	By isomorphism definition: put a map $\varphi : K' \to K$; show by definition that φ is an isomorphism from the ring K' onto the ring K.
4. Show that L' possesses properties required with respect to K' (i.e., L' is RPOV over K').	By definition (RPOV,…).

As we see, the approach proposed:

1) gives broad possibilities to enhance students' cognitive activity, use of partially-searching method promotes creative activity (herewith one should not think that accentuated scheme of proof of Theorem A. depresses creativity – straight conversely, as psychologists' investigations show, mastering algorithms creates the conditions for creativity and helps in solving creatively, nonstandard problems);

2) proof structuring, accentuated scheme of proof promotes more conscious assimilation of the proof and provides general understanding of connections between individual steps of the proof;

3) allows to reduce complex proof to the consideration of the set of standard problems;

and, what is especially important,

4) eliminates a logical gap of the course arguing a possibility to prove some propositions not for the given algebraic objects but for ones isomorphic to them (a method of attack widely used in modern algebraic science).

Experience shows that only the first theorem proven in the way proposed (namely, Theorem A.) is hard for apprehension. Therefore it is better to consider it in the first semester. In exam preparation students will have appreciated the proof, will have understood its idea. Practice identifies that when considering the remaining theorems (theorems A.-D.) in the second semester students actively assist. Once a lecturer shows the picture-guide, the proof idea appears (by the scheme I-V), students formulate the scheme of proof and then prove its separate steps (solving, in fact, standard problems 1-4 mentioned above).

Difficult Theorems A.-D. deserve students' special attention and deep study in exam preparation. Therefore in our opinion it's quite reasonable to divide theorems submitted for the exam in the 2-nd semester into 2 groups (the first one containing the simpler theorems while the second one -- more complex) and correspondingly to provide different evaluation of the answer (to give more points for the proof of more complicated theorems). It may seem strange, but most students demonstrate better knowledge and understanding of more complicated theorems (including Theorems A.-D.) than of simpler ones. They say that senior students have advised them to pay special attention to Theorems A.-D., because it is quite enough to understand once the proof idea and then to use the scheme to prove as many as four theorems.

The major points covered by this paper may be summarized as follows. Emphasized in the paper is a fact that the approach proposed in some textbooks in higher algebra for proving existence theorems is not correct. To remedy the situation authors propose to introduce into consideration Theorem 1 (its proof is given). The use of this theorem is illustrated by the example: considered is a proof of theorem on existence of a ring of polynomials in one variable over a commutative ring with unity. The approach proposed makes it possible to eliminate some logical gaps of the course, provides a means for proving, in particular, Theorems A.-D. by the unified scheme (in 5 steps), set force the exposition of theoretical material in a manner more precise, clear, structured and comprehensible.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kostrikin A.I. Introduction to Algebra. − Moscow: Nauka, 1977. − 496 p. (In Russian)
2. Rotenberg V.S., Bondarenko S.M. Brains. Education. Health. − Moscow: Prosveshchenie, 1989. − 240 p. (in Russian)
3. Trebenko D.Ya., Trebenko O.O. Algebra and Number Theory, P.1. −, Kyiv: NPDU, 2009. − 420 p. (In Ukrainian)
4. Trebenko D.Ya.,Trebenko O.O. On the concept of a polynomial studying in the Higher Algebra course // Vesti BDPU, Ser. 3, 2014, №2. − P.41-47. (In Russian)
5. Zavalo S.T. Algebra course. − Kyiv: Vyshcha shk., 1985. − 500 p. (In Ukrainian)
6. Zavalo S.T., Kostarchuk V.M., Hatset B.I. Algebra and Number Theory, P.2. − Kyiv: Vyshcha shk., 1976. − 384 p. (In Ukrainian)

Требенко Д.Я., Требенко О.А. Теоремы существования в курсе алгебры и теории чисел

Аннотация. В статье акцентировано внимание на некорректности предлагаемого в некоторых учебниках по высшей алгебре подхода для доказательства теорем существования. Для устранения отмеченной некорректности авторы предлагают ввести в рассмотрение теорему 1 (и приводят ее доказательство). Использование данной теоремы показано на примере доказательства теоремы о существовании кольца многочленов от одной переменной. Предлагаемый подход позволяет устранить некоторые логические пробелы курса, дает возможность доказывать, в частности, отмеченные теоремы A.-D. по единой схеме (в 5 этапов), делает изложение учебного материала более четким, структурированным и понятным.

Ключевые слова*: теорема существования, построение кольца многочленов*