Applications to ring theory and some history

A. Belov, M. Kharitonov

August 2, 2012

We consider a set S with a binary operation "+" such that

1. for any $a, b, c \in S$, we have $a + b = b + a$, $(a + b) + c = a + (b + c)$;
2. there exists a special element $0 \in S$ such that $a + 0 = a$ for all $a \in S$;
3. for any $a \in S$, there exists an element, denoted by $(-a)$, such that

$$(-a) + a = a + (-a) = 0.$$

Examples: remainders modulo some number; rotations of a plane with a fixed point.

We say that a set with an addition is a *ring*, if it has a multiplication, i.e. a binary operation which satisfies the following conditions

1. $a(bc) = (ab)c$ for all a, b, $c \in S$ (associativity);
2. $a(b + c) = ab + ac, (b + c)a = ba + ca$ for all a, b, $c \in S$ (distributivity).

Examples: remainders modulo some number; polynomials of one or more variables.

Problem 1.1. Provide an example of a ring with a zero-divisor, i.e. such ring that there exists two non-zero elements a, b such that $ab = 0$.

Definition 1.1. *We call an element a* unit of a ring R *or a* neutral element of R *(and denote it 1), if we have $1A = A1 = A$ for all $A \in R$. We say that an element of R is an inverse to A (and denote it A^{-1}), if $AA^{-1} = A^{-1}A = 1$.*

Problem 1.2. Prove that in a ring with a unit commutativity axiom for an operation "+" follows from the other axioms.

Problem 1.3. Construct a ring R with 4 elements such that any non-zero element of R has an inverse.

Problem 1.4. Construct a non-commutative ring R, i.e. such ring R that $ab \neq ba$ for some $a, b \in R$.

Let R be a ring with a unit. Let $n \in \mathbb{Z}_{\geq 1}$ be the smallest number such that

$$1 + 1 + 1 + ... + 1(n \text{ times}) = 0.$$

Then n is called *the order of the unit of R*. If such number n does not exist, we assume that the order of the unit of R equals 0.

Problem 1.5. Let R be a ring such that the order of the unit of R equals 0. Assume that there exist elements $e, f, g \in R$ such that $e^2 = e, f^2 = f, g^2 = g$ and $e + f + g = 0$. Prove that $e = f = g = 0$.

Definition 1.2. *A non-commutative polynomial $f = f(x_1, ..., x_n)$ is called* an identity *of a ring R, if $f(x_1, ..., x_n) = 0$ for any $x_1, ..., x_n \in R$. We say that the identity $f(x_1, ..., x_n)$ follows from a set of identities $\{g_i\}$, if one can deduce $f(x_1, ..., x_n) = 0$ from $g_i(x_1, ..., x_n) = 0$ algebraically.*

Problem 1.6. Provide an example of a ring with a non-zero multiplication in which the identities $x^2 = 0$ and $xy = yx$ are satisfied.

Definition 1.3. *If any non-zero element of a ring R is invertible, then R is called a skew-field. A ring R is called commutative, if R satisfies the identity $xy - yx = 0$. A commutative skew-field is called a field.*

Examples.

1. Field of real numbers, field of complex numbers, ring of polynomials, ring $\mathbb{Z}_n$ of remainders modulo n. If n is prime, then $\mathbb{Z}_n$ is a field.

2. A fundamental example of a non-commutative ring is a ring of matrices. We construct it now. The elements of this ring is $n \times n$ tables filled by numbers. We use index A_{ij} to denote the number puted in i-th line and j-th column. We put

$$(A + B)_{ij} = A_{ij} + B_{ij} \text{ (pointwise addition).}$$

To define multiplication we put

$$(AB)_{ik} = (\sum_j A_{ij} B_{jk}).$$

3. The skew-field of quaternions is a set of elements $ai + bj + ck + d$, where a, b, c, d are real numbers, with a pointwise addition and multiplication defined by the following relations:

$$ij = -ji = k, ki = -ik = j, jk = -kj = i, i^2 = j^2 = k^2 = -1.$$

Problem 1.7. Check that all mentioned sets with addition and multiplication are rings.

Definition 1.4. *By definition, an N-free associative algebra over ring A (or the ring of non-commutative polynomials of the ring R), is a set $\sum_i a_i v_i$, where $a_i \in R$, and v_i are words in alphabet $\{a_1, ..., a_N\}$. If $v = \sum_i a_i v_i$, $u = \sum_i b_i v_i$, then we set*

$$u + v = \sum_i (a_i + b_i) v_i,\ uv = \sum_{i,j} (a_i b_j)(v_i v_j).$$

Remark 1.1. In the rest of the problem set any algebra considered is an associative algebra with a unit.

We put $[a, b] := ab - ba$.

Examples.

1. Commutativity identity $[a, b] = ab - ba$ is satisfied by definition in all commutative rings.

2. Let p be a prime number. Identity $x^p - x = 0$ is satisfied for a ring of remainders modulo p (small Ferma's theorem).

3. Hence $ab+ba=(a+b)^2-a^2-b^2$, the identity $ab+ba=0$ follows from the identity $a^2=0$.

Problem 1.8. 1. Prove that Hall's identity $[[x,y]^2,z]=0$ holds for 2×2 matrices.

2. Prove that standard identity of degree 4

$$\sum_{\sigma\in S_4}(-1)^\sigma x_{\sigma(1)}\cdots x_{\sigma(4)}=0$$

holds for 2×2 matrices.

For any algebra for which some non-trivial identity is satisfied, is satisfied the standard identity of some degree. An algebra of $n\times n$ matrices satisfies the standard identity of degree $2n$.

It is known that for algebra of 2×2 matrices all identities follows from the Hall's identity and the standard identity of degree 4 (this is quite complicated theorem which is proven by Yu. Razmislov in 1973). Even for 3×3-matrices the basis of identities is not known yet.

Definition 1.5. *An algebra is called a nil-algebra, if there exist a function $n: A\to \mathbf{N}$ such that, for all $x\in A$, we have $x^{n(x)}=0$. If for some n the algebra satisfies identity x^n, then it is called a nil-algebra of index n.*

Definition 1.6. *An algebra A is called nilpotent, if the identity $x_1...x_k=0$ is satisfied for some k.*

Definition 1.7. *An element $\tau\in A$ is called algebraic of index k, if $\sum\limits_{i=1}^{k}\tau^i a_i=0$ for some $a_1,...,a_k\in\mathbb{Z}$. An algebra A is called algebraic of index k if any element of A is algebraic of index k. An algebra A is called algebraic if any element of A is algebraic of some index (depending on the element).*

Problem 1.9. 1. Prove that any algebraic algebra of index k satisfies a non-trivial identity.

2. * Prove that algebra of $n\times n$-matrices is algebraic of index n.

3. Fix $n\in\mathbb{Z}_{\geq 0}$. We denote by SS_n the set of all subsets of $\{1,...,n\}$. For a $\tau\in\mathrm{SS}_n$ we put $S_\tau:=\sum_{i\in\tau}x_i$. Prove the following equation (is called polarization):

$$\sum_{\tau\in\mathrm{SS}_n}(-1)^{|\tau|}(S_\tau)^n=\sum_{\sigma\in S_n}x_{\sigma(1)}\cdots x_{\sigma(n)}.$$

(If we assume that x_i commutes on with each other, then the right-hand side will equal $n!x_1\cdots x_n$.)

4. Prove that from the identity x^n follows the identity $\sum_{\sigma\in S_n}x_{\sigma(1)}\cdots x_{\sigma(n)}$.

5. Prove that any identity has a polylinear (i.e. linear over any variable) analogue of the same degree.

Let $a_1, ..., a_l$ be some elements of some algebra A with a unit and $w = a_{i_1}a_{i_2}...a_{i_s}$ be a word of alphabet with letters $\{a_1, ..., a_l\}$. We denote by $w(a)$ the element $a_{i_1} \cdot a_{i_2} \cdot ... \cdot a_{i_s}$ of A.

Problem 1.10. Let A be an algebra which satisfies an identity of degree n and $a_1, ..., a_l$ be some elements of A. Let w be an n-divisible word of alphabet $\{a_1, ..., a_l\}$. Prove that $w(a) = \sum\limits_{w_i \prec w} c_i w_i(a)$. For some finite set of words w_i and some $c_i \in \mathbb{Z}$ [1].

A. Kurosh have posed in 1941 the following question.

Kurosh's problem. *Is it true that any algebraic finitely generated algebra, which satisfies some identity of degree n, is finite-dimensional?*

First solution of Kurosh's problem, obtained by Levitskii and Kaplanskii in 1951, and use highly non-elementary methods. In 1957, A. Shirshov develops purely combinatorial technique, which provides another approach to Kurosh's and other nilpotency-related problems.

Problem 1.11. a) Resolve Kurosh's problem using Shirshov's theorem of height.
b)* Prove that l-generated nil-algebras are n-nilpotent of index $k(n, l)$.

Our next goal is to receive estimates for a function $k(n, l)$. Estimates for height in combinatorics of words straightforwardly leads to estimates of $k(n, l)$. First estimate of A. Shirshov are extremely overwhelming but his works contains deep ideas which still stay in focus of researchers. A. Kolotov receives in 1982 twice exponential estimate for $k(n, l)$ of type (l^{l^n}), where l is a number of generators and n is a degree of identity. A. Belov receives exponential estimate $n^3 l^{3n}$ in 1992, this estimate has been upgraded in works of A. Klein in 2000.

E. Zelmanov have posed the following question in 1991.

Problem 1.12. Let $F_{2,m}$ be a free 2-generated associative ring with the identity $x^m = 0$. Is it true that the nilpotency class of $F_{2,m}$ depends exponentially on m?

Problem 1.13. Prove that the last problem from Section "Exponential estimates" provides a positive answer to Zelmanov's question.

A.Belov and M. Kharitonov receive in 2012 a subexponential estimate for a height. In connection with these results appear the following problem:

Problem 1.14. Receive a polynomial estimate for height.

And another one.

Problem 1.15. Does there exist an estimate for a height which is polynomial with respect to degree and linear with respect to the number of letters in an alphabet?

And the last one.

Problem 1.16. Receive lower height estimate.

[1] Вообще говоря, алгебра определена над полем и над ним же определены соотношения. У нас об этом разговора нет и потому вопрос о том, где живут c_i — сложен.