THE TEACHING OF MATHEMATICS
1999, Vol. II, 2, pp. 65–80

SELECTED CHAPTERS FROM ALGEBRA

I. R. Shafarevich

Abstract. This paper is the third part of the publication "Selected chapters of algebra", the first two being published in the previous issues of the Teaching of Mathematics, Vol. I (1998), 1–22, and Vol. II, 1 (1999), 1–30.

AMS Subject Classification: 00 A 35

Key words and phrases: Set, subset, one-to-one correspondence, combinatorics.

CHAPTER III. SET

1. Sets and subsets

The notion of a set has a somewhat different meaning in mathematics than in everyday language. The ordinary word "set" usually means a large number of certain objects[1]. In mathematics a set is an arbitrary collection of objects defined by a certain property which they all have. The objects which comprise a set are called its *elements*. So, for instance, we may talk about sets of one or two elements. A set is usually denoted by a capital letter (for example, M) and its elements by small letters (for example, a, b, ... , α, β, ...). The fact that a is an element of the set M is written in the form $a \in M$ and we also say that a *belongs* to M. If M consists of elements a_1, ... , a_n, we write $M = \{a_1, \ldots, a_n\}$.

A set containing a finite number of elements is called a *finite* set, while a set containing an infinite number of elements is called an *infinite* set. The number of elements of a finite set M is denoted by $n(M)$.

In this chapter we shall mainly be concerned with finite sets. The finite sets M and M' are said to be *equivalent* (equipotent) if they have the same number of elements, i.e. if $n(M) = n(M')$. We shall now describe the method which is usually used to establish the equivalence of two sets. *One-to-one correspondence* between two sets M and M' is coupling, or pairing off, their elements into pairs (a, a'), where $a \in M$, $a' \in M'$, so that each element a of M is coupled with one and only one element a' of M', and each element a' of M' is coupled with one and

---

This paper is an English translation of: И. Р. Шафаревич, *Избранные главы алгебры*, Математическое образование, 3, окт.--дек. 1997, Москва, стр. 2--45. In the opinion of the editors, the paper merits wider circulation and we are thankful to the author for his kind permission to let us make this version.

[1]This is not so much true for the English language as it is for Russian. The Russian word for the set *множество* has the same root as the word *много* (many).

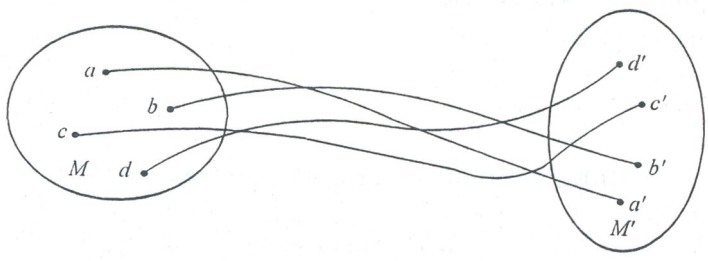


Fig. 1

only one element a of M. If we represent the sets M and M' graphically and draw lines connecting those elements which belong to one pair, we see that each element of M is connected to one and only one element of M' and vice versa (Fig. 1).

For instance, if $n(M) = n$ and if we numerate the elements of M as follows: $M = \{a_1, \ldots, a_n\}$, we have established a one-to-one correspondence between the set M and the set N of numbers 1, 2, ... , n.

If we choose two points O and E on a straight line, then to each point A which lies on that line we can correspond the real number $\dfrac{|OA|}{|OE|}$ with the + sign if A is on the same side of O as E, and with − sign in the opposite case. This establishes a one-to-one correspondence between the set of the points of the straight line and the set of all real numbers which is usually denoted by $\mathbf{R}$. We shall consider this in more detail in one of the subsequent chapters.

If we have a one-to-one correspondence between the sets M and M', and if the elements $a \in M$ and $a' \in M'$ are coupled in the pair (a, a') we say that the element a corresponds to the element a', and that the element a' corresponds to the element a.

Two finite sets are equivalent if and only if it is possible to establish a one-to-one correspondence between them.

This statement is so ovious, that it can hardly be called a theorem. If $n(M) = n(M') = n$, we can write our sets as follows: $M = \{a_1, \ldots, a_n\}$, $M' = \{a'_1, \ldots, a'_n\}$, and by forming pairs (a_i, a'_i) of elements with the same index we establish a one-to-one correspondence between M and M'. Conversely, if there exists a one-to-one correspondence between M and M', and if we write M in the form $M = \{a_1, \ldots, a_n\}$, then each a_i belongs to a pair with one and only one element $a' \in M'$, and we can give it the same index, i.e. we can put $a' = a_i$. By the definition of a one-to-one correspondence, we can numerate in this way all the elements of M', and we obtain that $M' = \{a'_1, \ldots, a'_n\}$.

R. Dedekind (the second part of the 19th century) who did a lot to clear the role which sets have in mathematics, thought that the above statement gives, in a hidden form, the *definition* of a positive integer. According to him, it is first necessary to define the notion of one-to-one correspondence, and then a positive integer is the

general property possessed by all finite sets among which it is possible to establish one-to-one correspondence. This is probably how the notion of a positive integer was formed historically (of course, without the present terminology). For example, the notion "two" was formed, as we said in Section 1 of Chapter I, by abstracting, i.e. by considering the general property shared by the sets consisting of: two eyes, two oars in a boat, two travellers walking along the road, and more generally by all the sets which can be put into a one-to-one correspondence with one of the above.

This means that the notion of a set is the most fundamental notion of mathematics, since the notion of a positive integer is founded upon the notion of a set.

In further text we shall often construct new sets, starting with two given sets.

The *product* of sets M_1 and M_2 is the set whose elements are all the pairs (a, b), where a is an arbitrary element of M_1 and b is an arbitrary element of M_2. The product of M_1 and M_2 is denoted by $M_1 \times M_2$.

For example, if $M_1 = \{1, 2\}$, $M_2 = \{3, 4\}$, then $M_1 \times M_2$ consists of the pairs $(1, 3)$, $(1, 4)$, $(2, 3)$, $(2, 4)$.

If $M_1 = M_2$ is the set $\mathbf{R}$ of all real numbers, $M_1 \times M_2$ is the set of all pairs (a, b), where a and b are real numbers. The coordinate method in the plane establishes a one-to-one correspondence between the set $M_1 \times M_2$ and the set of all points of the plane (Fig. 2).

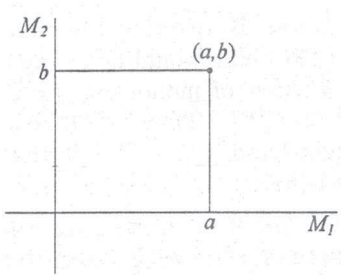


Fig. 2

As another example, suppose that M_1 consists of the numbers $1, 2, \ldots, n$, and M_2 of the numbers $1, 2, \ldots, m$. Introduce two new variables x and y and correspond to a number $k \in M_1$ the monomial x^k and to the number $l \in M_2$ the monomial y^l. An element of the set $M_1 \times M_2$ has the form (k, l) and we can correspond to it the monomial $x^k y^l$. In this way we obtain a one-to-one correspondence between the set $M_1 \times M_2$ and the set of monomials of the form $x^k y^l$, where $k = 1, \ldots, n$; $l = 1, \ldots, m$. In other words this is the set of monomials which stand on the right-hand side of the equality

$$(1) \qquad (x + x^2 + \cdots + x^n)(y + y^2 + \cdots + y^m) = xy + x^2y + xy^2 + \cdots + x^n y^m.$$

Hence, the set of these monomials is equivalent to the set $M_1 \times M_2$.

Analogously, let $M_1, M_2, \ldots, M_r$ be arbitrary sets. Their *product* is the set consisting of all sequences $(a_1, \ldots, a_r)$ where the i-th place is taken by an arbitrary element of the set M_i. The product of the sets $M_1, \ldots, M_r$ is denoted by $M_1 \times \cdots \times M_r$.

For example, if $M_1 = M_2 = M_3$ is the set of all real numbers $\mathbf{R}$, the coordinate method in the space establishes a one-to-one correspondence between the points of the space and the set $M_1 \times M_2 \times M_3$.

But in this chapter we are considered with finite sets.

Theorem 1. *If the sets $M_1, \dots, M_r$ are finite, then the set $M_1 \times \cdots \times M_r$ is also finite, and $n(M_1 \times \cdots \times M_r) = n(M_1) \cdots n(M_r)$.*

We shall first prove the theorem for the case of two sets, i.e. when $r = 2$; this will be the induction basis. If $M_1 = \{a_1, \dots, a_n\}$, $M_2 = \{b_1, \dots, b_m\}$, then all the pairs (a_i, b_j) can be written in the form of a rectangle

$$\begin{array}{ccc} (a_1, b_1) & \dots & (a_n, b_1) \\ (a_1, b_2) & \dots & (a_n, b_2) \\ \dots & \dots & \dots \\ (a_1, b_m) & \dots & (a_n, b_m) \end{array} \tag{2}$$

The j-th row above contains pairs whose last element is always b_j. In each row the number of pairs is equal to the number of all a_i's, i.e. it is n. The number of the rows is equal to the number of all b_j's, i.e. it is equal to m. Hence, the number of pairs is nm. Notice that the rectangle (2) resembles, in a way, Fig. 2. (A different line of reasoning would be to say that the set M_1 is equivalent to the set $\{1, \dots, n\}$ or to the set of monomials $\{x, x^2, \dots, x^n\}$ and that M_2 is equivalent to the set $\{y, y^2, \dots, y^m\}$. Then, $n(M_1 \times M_2)$ is, as we have seen, the number of terms in the right-hand side of (1). Putting $x = 1$, $y = 1$, we conclude that this number of terms is nm.)

The proof of the general case of r sets $M_1, \dots, M_r$ will be carried out by induction on r. In each sequence $(a_1, \dots, a_r)$ we introduce two more brackets, and write it in the form $((a_1, \dots, a_{r-1}), a_r)$. Clearly, this does not alter the number of the sequences. But the sequence $((a_1, \dots, a_{r-1}), a_r)$ is the pair (x, a_r), where $x = (a_1, \dots, a_{r-1})$ can be considered to be an element of the set $M_1 \times \cdots \times M_{r-1}$. Hence, the set $M_1 \times \cdots \times M_r$ is equivalent to the set $P \times M_r$, where $P = M_1 \times \cdots \times M_{r-1}$. We have proved that $n(P \times M_r) = n(P)n(M_r)$, and by the induction hypothesis we have $n(P) = n(M_1) \cdots n(M_{r-1})$. Therefore, $n(M_1 \times \cdots \times M_r) = n(M_1) \cdots n(M_{r-1})n(M_r)$ and the proof is complete.

Using Theorem 1 we can once more form the expression for the number of divisors of a positive integer n. Suppose that n has the cannonical representation

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

In Section 3 of Chapter I we saw that the divisors of n can be written in the form

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

where β_i can take any integral value between 0 and α_i (formula (11) of Chapter I). In other words, the set of divisors is equivalent to the set of sequences $(\beta_1, \dots, \beta_r)$ where β_i takes the above mentioned values. But this is exactly the product $M_1 \times \cdots \times M_r$ of the sets M_i where M_i is the set $\{0, 1, \dots, \alpha_i\}$. Since $n(M_i) = \alpha_i + 1$, according to Theorem 1 the number of divisors is $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$. This formula was derived in a different way in Section 3, Chapter I.

If the sets $M_1, \ldots, M_r$ coincide, i.e. if $M_1 = M_2 = \cdots = M_r = M$ their product $M_1 \times \cdots \times M_r$ is denoted by M^r. Consider the case when $M_1 = \cdots = M_r = I$, and the set I has two elements a and b. An element of I^r is a sequence of r symbols, each one being a or b, e.g. *aababbba* (for shortness sake we omit the commas). This can be considered as a word of r letters written in the alphabet of two letters, a being a dot and b a dash. Therefore, $n(I^r)$ is equal to the number of words of length r, written in Morse's alphabet. As we see, it is equal to 2^r (all $n_i = 2$).

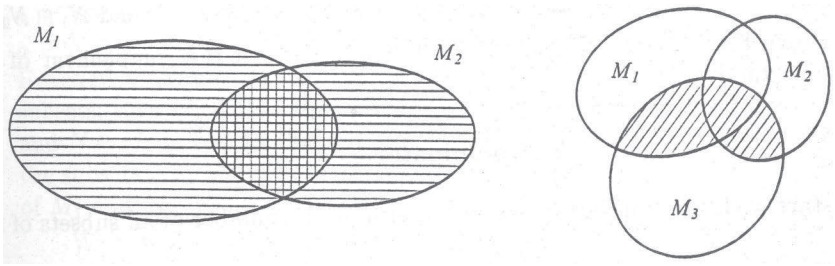
In further text we consider sets contained in a given set M. They are called its *subsets*. This means that a subset N of a set M contains only elements of M, but not necessarily all of them. The fact that N is a subset of M is written as $N \subset M$. We also take that M is a subset of itself. As we shall see later, it is very convenient to consider the subset of M containing no elements—this simplifies greatly many definitions and theorems. This subset is callled the *empty subset* and is denoted by $\varnothing$. By definition we take $n(\varnothing) = 0$.

If $N \subset M$, the set of all elements of M which do not belong to N is called the *complement* of N and is denoted by $\overline{N}$. For instance, if M is the set of all positive integers, and if N is the set of all even positive integers, then $\overline{N}$ is the set of all odd positive integers. If $N = M$, then $\overline{N} = \varnothing$.

If N_1 and N_2 are two subsets of M (i.e. $N_1 \subset M$ and $N_2 \subset M$) then the set of all elements which belong to N_1 and N_2 is called their *intersection* and is denoted by $N_1 \cap N_2$. For example, if M is the set of all positive integers, if N_1 is the subset of all those divisible by 2, and N_2 the subset of all those divisible by 3, then $N_1 \cap N_2$ is the set of all positive integers divisible by 6.

If N_1 and N_2 do not have common elements, then by definition $N_1 \cap N_2 = \varnothing$, the empty set. So, if M and N_1 are the same as in the previous example, and N_2 is the set of odd positive integers, then $N_1 \cap N_2 = \varnothing$.

The set containing elements which belong to the subset N_1 or the subset N_2 is called their *union* and is denoted by $N_1 \cup N_2$. For example, if M is again the set of all positive integers, and N_1 and N_2 are the subsets of all even and odd numbers, respectively, then $N_1 \cup N_2 = M$.



a) b)

Fig. 3

Intersections and unions of sets can be represented graphically as in Figure 3.

In Fig. 3a) $M_1 \cup M_2$ is hatched by horizontal and $M_1 \cap M_2$ by vertical lines. In Fig. 3b) the set $(M_1 \cup M_2) \cap M_3$ is hatched.

In this chapter we shall consider subsets of a finite set M, which satisfy certain conditions and we shall derive formulas for the number of all such subsets. The branch of mathematics concerned with such questions is called *combinatorics*.

Therefore, combinatorics is the theory of arbitrary finite sets. We do not use notions such as distance or the magnitude of an angle, equation or its roots, but only the notion of a subset and the number of its elements. Hence, it is very surprising that, using only such miserly material, we can find many regularities and connections with other branches of mathematics which are not at all obvious.

Problems

1. Let $M = M'$ be the set of all positive integers. Couple into pairs the number $a \in M$ with $b \in M'$ such that $b = 2a$. Is this a one-to-one correspondence between M and M'?

2. Let N be the set of all positive integers, let $M = N \times N$ and let M' be the set of positive rational numbers. Couple into pairs $(n_1, n_2) \in M$ with $a \in M'$ if $a = n_1/n_2$. Is this a one-to-one correspondence?

3. How many different one-to-one correspondences exist between two sets M and M' if $n(M) = n(M') = 3$? Draw them analogously as in Fig. 1.

4. Every one-to-one correspondence between the sets M and M' defines the set of those pairs (a, a'), where $a \in M$ and $a' \in M'$ correspond to each other, i.e. it defines a subset $\Gamma \subset M \times M'$ which is called the *graph of correspondence*. Let Γ_1 and Γ_2 be graphs of two one-to-one correspondences. Prove that $\Gamma_1 \cap \Gamma_2$ is a graph of a one-to-one correspondence if and only if $\Gamma_1 = \Gamma_2$ and the two given correspondences coincide.

5. Let $n(M) = n(M') = n$ and let Γ be the graph of a one-to-one correspondence between M and M' (see Problem 4). Evaluate $n(\Gamma)$.

6. Let M be the set of all positive integers, let $N_1 \subset M$ be the subset of all numbers divisible by a given number a_1 and let $N_2 \subset M$ be the subset of all numbers divisible by a given number a_2. Describe the sets $N_1 \cup N_2$ and $N_1 \cap N_2$.

7. Prove that $\overline{(\overline{N})} = N$, i.e. that the complement of the complement of a subset N is exactly N.

2. Combinatorics

We start with the simplest question: determine the number of all subsets of a finite set.

We first solve the problem for small values of $n(M)$. We will write down the subsets N of M writing in one row all the subsets with the same number of elements (i.e. with the same value of $n(N)$). The rows are arranged in the ascending order

of $n(N)$.

1.	$n(M)=1$,	$M=\{a\}$		
	$n(N)=0$;	$N=\varnothing$		
	$n(N)=1$;	$N=M=\{a\}$		
2.	$n(M)=2$,	$M=\{a,b\}$		
	$n(N)=0$;	$N=\varnothing$		
	$n(N)=1$;	$N=\{a\}$,	$N=\{b\}$	
	$n(N)=2$;	$N=M=\{a,b\}$		
3.	$n(M)=3$,	$M=\{a,b,c\}$		
	$n(N)=0$;	$N=\varnothing$		
	$n(N)=1$;	$N=\{a\}$,	$N=\{b\}$,	$N=\{c\}$
	$n(N)=2$;	$N=\{a,b\}$,	$N=\{a,c\}$,	$N=\{b,c\}$
	$n(N)=3$;	$N=M=\{a,b,c\}$		

Table 1

We see that if $n(M)=1$, the number of subsets is 2, if $n(M)=2$ it is 4 and if $n(M)=3$ it is 8. This suggests the general statement.

Theorem 2. *The number of all subsets of a finite set M is $2^{n(M)}$.*

There is a general method which reduces the investigation of an arbitrary finite set to the investigation of sets with smaller number of elements. The set M is called the *sum* of its two subsets $M_1 \subset M$ and $M_2 \subset M$ if $M_1 \cup M_2 = M$, $M_1 \cap M_2 = \varnothing$. Clearly, this is equivalent to $M_2 = \overline{M_1}$ and $M_1 = \overline{M_2}$. In this case each element of M belongs to one of the subsets M_1 or M_2 (since $M_1 \cup M_2 = M$) and only to one of them (since $M_1 \cap M_2 = \varnothing$). Hence, $n(M) = n(M_1) + n(M_2)$. The fact that M is the sum of M_1 and M_2 is written as $M = M_1 + M_2$. Such a representation is also called a *partition* of M into M_1 and M_2.

Let $M = M_1 + M_2$ and let $N \subset M$ be an arbitrary subset. Then any element $a \in N$ belongs either to M_1 (in this case $a \in N \cap M_1$) or to M_2 (in this case $a \in N \cap M_2$), and only one of these cases can take place (since $M_1 \cap M_2 = \varnothing$). Hence $N = (N \cap M_1) + (N \cap M_2)$. Conversely, if $N_1 \subset M_1$ and $N_2 \subset M_2$ are arbitrary subsets, then $N_1 \subset M$, $N_2 \subset M$ and $N = N_1 \cup N_2 \subset M$, whereas $N \cap M_1 = N_1$ and $N \cap M_2 = N_2$. In this way we establish a one-to-one correspondence between the subsets N of M and the pairs (N_1, N_2) where N_1 and N_2 are arbitrary subsets of M_1 and M_2, respectively.

We now formulate this result in terms of sets. Denote by $U(M)$ the set of all subsets of a set M. One should not be alarmed because we consider here subsets as elements of a new set. So, for example, associations of civil or electrical engineers are elements of the general association of engineers. In Table 1 we decribed the sets $U(M)$ when $n(M) = 1$, 2 or 3. The result obtained above can be formulated as

follows: if $M = M_1 + M_2$ is a partition of M, then the set $U(M)$ is in a one-to-one correspondence with the set $U(M_1) \times U(M_2)$. Denote the number $n(U(M))$ by $v(M)$—this is the required number of all subsets. Applying Theorem 1 we deduce that

$$v(M_1 + M_2) = v(M_1)v(M_2). \tag{3}$$

The equality (3) reduces the evaluation of $v(M)$ to the evaluation of $v(M_1)$ and $v(M_2)$ for the sets M_1 and M_2 with smaller number of elements. In order to obtain the final result, consider the partition of M not into two, but into an arbitrary number of subsets. We can define this concept inductively, saying that $M = M_1 + \cdots + M_r$ if $M = (M_1 + \cdots + M_{r-1}) + M_r$, where the expression $M_1 + \cdots + M_{r-1}$ is taken to be already defined. In fact, when we say that $M = M_1 + \cdots + M_r$, this means that $M_1, \ldots, M_r$ are subsets of M and that every element of M belongs to one and only one of the subsets $M_1, \ldots, M_r$. For example, if M is the set of all positive integers, then $M = M_1 + M_2 + M_3$, where M_1 is the subset of all numbers divisible by 3, M_2 is the subset of all numbers of the form $3r + 1$ and M_3 is the subset of all numbers of the form $3r + 2$.

From (3), for finite sets M_i we obtain, by induction

$$v(M_1 + \cdots + M_r) = v(M_1) \cdots v(M_r). \tag{4}$$

If $n(M) = n$, then there exists the "tiniest" partition of M into n subsets M_i, each having only one element, i.e. $M = M_1 + \cdots + M_n$. If $M = \{a_1, \ldots, a_n\}$, then $M_i = \{a_i\}$. The one element set M_i has two subsets: the empty set $\varnothing$ and M_i itself (see Table 1, first row). Hence, $v(M_i) = 2$ and applying formula (4) to the partition $M = M_1 + \cdots + M_n$ we obtain that $v(M) = 2^n$, as stated in Theorem 2.

The question of the number of all subsets of a given set appears in connection with certain problems regarding numbers. For example, consider the following question: in how many ways can a positive integer n be written as a product of two relatively prime factors? Let $n = ab$, where a and b are relatively prime and let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the canonical prime factorization. Then a and b are divisors of n and, as we saw in Section 3 of Chapter I, each one of them has the form $p_1^{\beta_1} \cdots p_r^{\beta_r}$ where $0 \leqslant \beta_i \leqslant \alpha_i$. But since a and b are relatively prime, then if some p_i divides a, then it cannot divide b and hence appears in a with degree α_i. Therefore, in order to obtain the required factorization $n = ab$, it is necessary to choose an arbitrary subset N of the set $M = \{p_1, \ldots, p_r\}$ and to equate a to the product of $p_i^{\alpha_i}$ for $p_i \in N$. Then a divides n and $n = ab$ is the required factorization. According to Theorem 2, the number of all factorizations of n into products of two relatively primer factors is 2^r, where r is the number of different prime factors of n.

It should be noted that in the above evaluation we considered the factorization $n = ab$ and $n = ba$ to be different. In fact, if a, and hence the factorization $n = ab$, corresponds to the subset $N \subset \{p_1, \ldots, p_r\}$, then b corresponds to the subset consisting of those $p_i \in M$ which do not belong to N, i.e. which belong to the complement $\overline{N}$ of N. Therefore, in our evaluation we corresponded the factorizations $n = ab$ and $n = ba$ to two different subsets N and $\overline{N}$. Hence, if we

do not want to make a difference between the factorizations $n = ab$ and $n = ba$, then the two subsets N and $\overline{N}$ should be treated as one, and then the number of all factorizations in this sense would be 2^{r-1}.

We now pass on to a more subtle problem: find the number of subsets of a given finite set M which contain m elements and m is a given number. In order to do this, we again collect all the subsets $N \subset M$ such that $n(N) = m$ into one set denoted by $U(M, m)$. If we put $n(U(M, m)) = v(M, m)$, then this is the number which we wish to find. In Table 1 we wrote the sets which belong to $U(M, m)$ on one row. Hence, we obtain the values of $v(M, m)$ for small values of $n(M)$:

$$\begin{aligned}
&n(M) = 1: \quad && v(M,0) = 1, \quad v(M,1) = 1 \\
&n(M) = 2: \quad && v(M,0) = 1, \quad v(M,1) = 2, \quad v(M,2) = 1 \\
&n(M) = 3: \quad && v(M,0) = 1, \quad v(M,1) = 3, \quad v(M,2) = 3, \quad v(M,3) = 1
\end{aligned}$$

Table 2

Theorem 3. *If $n(M) = n$, the number of subsets $N \subset M$ of the set M which contain m elements (i.e. such that $n(N) = m$) is equal to the binomial coefficient C_n^m. In other words, $v(M, m) = C_n^m$.*

The proof is based upon the same idea as the proof of Theorem 2. Namely, suppose that the set M is the sum of two subsets: $M = M_1 + M_2$ and we shall express the number $v(M, m)$ in terms of the numbers $v(M_1, m)$ and $v(M_2, m)$. If $M = M_1 + M_2$, then each subset $N \subset M$ can be written in the form $N = N_1 + N_2$, where $N_1 = N \cap M_1$, $N_2 = N \cap M_2$. If we take into account the condition $n(N) = m$, then we must have $n(N_1) + n(N_2) = m$. Let k and l be two nonnegative integers such that $k + l = m$. Consider all subsets $N \subset M$ such that $n(N \cap M_1) = k$, and $n(N \cap M_2) = l$, denote the set of all these subsets by $U(k, l)$ and put $n(U(k, l)) = v(M, k, l)$. Then in the same way as in the proof of Theorem 2 we see that

$$v(M, k, l) = v(M_1, k)v(M_2, l). \tag{5}$$

The set $U(M, m)$ can clearly be partitioned into sets $U(M, k, l)$ for various pairs of numbers k, l, such that $k + l = m$. Therefore the number of its elements $v(M, m)$ is equal to the sum of all numbers $v(M, k, l)$ for all k and l such that $k + l = m$, i.e. for all the values: $k = 0$, $l = m$; $k = 1$, $l = m - 1$; ... ; $k = m$, $l = 0$. From the relation (5) we obtain

$$v(M, m) = v(M_1, m)v(M_2, 0) + v(M_1, m-1)v(M_2, 1) + \cdots + v(M_1, 0)v(M_2, m). \tag{6}$$

Of course, if in the product $v(M_1, k)v(M_2, l)$ it turns out that $k > n(M_1)$, we have to take $v(M_1, k) = 0$ and the same holds for $v(M_2, l)$.

We have obtained a relation analogous to the relation (3), although it is more complicated.

We have met the relation (6) in connection with a completely different problem. This is, in fact, the coefficient of x^m in the product of two polynomials $f(x)$ and $g(x)$ if the coefficient of x^k in $f(x)$ is $v(M_1, k)$ and the coefficient of x^l in $g(x)$

is $v(M_2, l)$; see formula (1) od Chapter II. In order to establish the connection between these two statements, define for an arbitrary finite set M the polynomial $f_M(x)$ whose coefficients are $v(M, s)$:

$$f_M(x) = v(M,0) + v(M,1)x + \cdots + v(M,n)x^n, \tag{7}$$

where $n = n(M)$.

For instance, according to Table 2, if $n(M) = 1$, then $f_M(x) = 1 + x$, if $n(M) = 2$ then $f_M(x) = 1 + 2x + x^2$, if $n(M) = 3$, then $f_M(x) = 1 + 3x + 3x^2 + x^3$. Now comparing the relations (6) and (7) we can write

$$f_M(x) = f_{M_1}(x) \cdot f_{M_2}(x), \quad \text{if } M = M_1 + M_2. \tag{8}$$

Hence, if we introduce polynomials $f_M(x)$ instead of the numbers $v(M)$ we obtain a complete similarity with the formula (3). We see that the polynomial $f_M(x)$ turns out to be a just replacement for the number $v(M)$ in our more complicated problem. This is not a rare thing to happen. If we have to deal not with one number, but with a finite sequence of numbers $(a_0, \ldots, a_n)$, then its properties are often well expressed by means of the polynomial $a_0 + a_1x + \cdots + a_nx^n$. We shall see that later, in other examples.

It remains literally to repeat the end of the proof of Theorem 2. If $M = M_1 + \cdots + M_r$, then from (8) we obtain, by induction,

$$f_M(x) = f_{M_1}(x) \cdots f_{M_r}(x).$$

Now put $n(M) = n$ and partition the set M into n subsets each containing one element: $M = M_1 + \cdots + M_n$, $n(M_i) = 1$. The one element set M_i has two subsets: the empty set $\varnothing$ with $n(\varnothing) = 0$ and M_i with $n(M_i) = 1$. Therefore, $v(M_i, 0) = 1$, $v(M_i, 1) = 1$, $v(M_i, k) = 0$ for $k > 1$, $f_{M_i} = 1 + x$ and we conclude that for any finite set M we have

$$f_M(x) = (1 + x)^{n(M)}.$$

The expression $(1 + x)^{n(M)}$ can be written in the form of a polynomial in x by means of the binomial formula. We have seen (formulas (20) and (24) of Chapter II) that for $n = n(M)$:

$$(1 + x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + \cdots + C_n^n x^n, \quad \text{where } C_n^m = \frac{n!}{m!\,(n-m)!}.$$

Therefore, recalling the definition of the polynomial $f_M(x)$ (formula (7)), we obtain

$$v(M, m) = C_n^m = \frac{n!}{m!\,(n-m)!} \quad \text{for } n = n(M). \tag{9}$$

This is the answer to our question.

By counting the subsets of M containing 0, 1, 2, ... , n elements where $n = n(M)$, we have counted all the subsets of M. Therefore, $v(M,0) + v(M,1) + \cdots + v(M,n) = v(M)$, or using (9) and Theorem 2, $C_n^0 + C_n^1 + \cdots + C_n^n = 2^n$. This relation for the binomial coefficients is easily obtained from the binomial formula, as we have done in Section 3 of Chapter II.

A subset of m elements of the set $\{a_1, \ldots, a_n\}$ is sometimes called a *combination* of n elements, taken m at a time. Hence, the binomial coefficient C_n^m is the number of all such combinations.

The above question of the number of subsets $N \subset M$, if $n(M) = n$, $n(N) = m$, is connected with some questions regarding positive integers. For example, consider the question: in how many ways can we write a positive integer n in the form of r summands, where r is a given number? In other words, what is the number of solutions of the equation $x_1 + \cdots + x_r = n$ in positive integers $x_1, \ldots, x_r$? Solutions with different order of the unknowns are considered to be different. For example, if $n = 4$, $r = 2$, we have $4 = 1 + 3 = 2 + 2 = 3 + 1$, and hence there are three solutions: $(1, 3)$, $(2, 2)$, $(3, 1)$.

Consider the segment AB of length n. Its points whose distance from the initial point A are integers will be called integral. Clearly, to each solution of the equation $x_1 + \cdots + x_r = n$ corresponds a partition of the segment AB into r segments with integral end points of length $x_1, x_2, \ldots, x_r$ (Fig. 4).

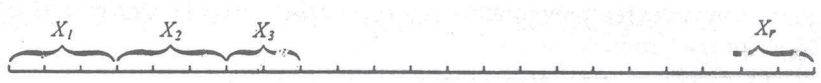


Fig. 4

In its turn, such a partition is defined by the end points of the first $r - 1$ segments (the end point of the last one is B). These end points define a subset N of the set M of integral points of the segment AB which are different from B. Clearly, $n(N) = r - 1$, and in this way we have defined a one-to-one correspondence between the integer solutions of the equation $x_1 + \cdots + x_r = n$ and the subsets $N \subset M$, where $n(N) = r - 1$, $n(M) = n - 1$. Therefore, the number of such solutions is equal to the number of such subsets. Applying formula (9) we conclude that the number of these subsets is C_{n-1}^{r-1}. If we do not fix the number of summands into which the number n is decomposed, then the number of all partitions is evidently equal to the sum of partitions into r summands for $r = 1, 2, \ldots, n$. Therefore, the number of partitions is equal to the sum of all binomial coefficients C_{n-1}^{r-1} where $r = 1, 2, \ldots, n$. We know that this sum is 2^{n-1}. In other words, a positive integer n can be partitioned into integer summands in 2^{n-1} ways (if we allow arbitrary number of summands, and take into account their order).

Return now to the derivation of formula (9). The method used—the introduction of the polynomials $f_M(x)$—turns out to be very useful in other cases, and we shall come back to it later. But formula (9) which connects the numbers $v(M, m)$ with binomial coefficients can be derived in another way. Consider the expression $(1 + x)^n$ as the product of n equal factors

$$(1 + x)^n = (1 + x)(1 + x) \cdots (1 + x) \tag{10}$$

and let us expand the product on the right-hand side of (10). We numerate its factors, i.e. we give them numbers $1, 2, \dots, n$ which form the set $M = \{1, 2, \dots, n\}$. In order to expand the product (10) we have to multiply each time n terms 1 or x, taking them from one of the brackets. Hence, each term of the expanded expression (10) is defined by indicating from which brackets with m numbers $i_1, i_2, \dots, i_m$. Then 1 is taken from the remaining $n - m$ brackets, and as a result we obtain the term x^m. We see that each term of the expanded expression (10) is defined by the subset $N = \{i_1, \dots, i_m\}$ of M which gives the number of brackets from which x is taken. From the remaining brackets we take 1. The remaining brackets have those numbers which belong to the complement $\overline{N}$ of N. Therefore, the number of appearences of the term x^m is equal to the number of subsets $N \subset M$ containing m elements, and this is $v(M, m)$. Hence, the expression (10) in the expanded form is the sum of the terms of the form $v(M, m)x^m$:

$$(1 + x)^n = v(M, 0) + v(M, 1)x + \cdots + v(M, n)x^n.$$

Comparing this with the definition of binomial coefficients (formula (20) of Chapter II) we obtain a new proof of the equality $v(M, m) = C_n^m$.

The same reasoning can be applied to a more general case. Consider the product of first degree polynomials $x + a_i$, where the coefficient of x is 1. Let us try to write the product

$$(x + a_1)(x + a_2) \cdots (x + a_n) \tag{11}$$

in the form of a polynomial in x. As before we numerate the n factors. Then each term in the expanded product (11) is obtained by taking $a_{i_1}, a_{i_2}, \dots, a_{i_m}$ from the factors numerated $i_1, i_2, \dots, i_m$ and taking x from the remaining $n - m$ factors. The obtained term has the form $a_{i_1}a_{i_2} \cdots a_{i_m}x^{n-m}$ and if all the terms of degree $n - m$ are collected together we get $\sigma_m(a_1, \dots, a_n)x^{n-m}$ where $\sigma_m(a_1, \dots, a_n)$ is the sum of all products of the form $a_{i_1} \cdots a_{i_m}$ where $\{i_1, \dots, i_m\}$ runs over all sets of indices formed from $1, \dots, n$. Hence, the polynomial $\sigma_m(a_1, \dots, a_n)$ has C_n^m terms. For example, $\sigma_1(a_1, \dots, a_n) = a_1 + \cdots + a_n$, and $\sigma_2(a_1, \dots, a_n) = a_1a_2 + a_1a_3 + \cdots + a_2a_3 + \dots a_{n-1}a_n$—it is the sum of all products a_ia_j with $i < j$. The last polynomial σ_n has the form $\sigma_n(a_1, \dots, a_n) = a_1 \cdots a_n$. This is the first time that we encounter polynomials in an arbitrary number n of variables. Polynomials $\sigma_1, \dots, \sigma_n$ have a very important role in algebra. In particular, we have proved the formula

$$(x + a_1) \cdots (x + a_n) = \\ x^m + \sigma_1(a_1, \dots, a_n)x^{n-1} + \sigma_2(a_1, \dots, a_n)x^{n-2} + \cdots + \sigma_n(a_1, \dots, a_n). \tag{12}$$

It is called Viète's formula.

Viète's formula expresses an important property of polynomials. Suppose that the polynomial $f(x)$ of degree n has n roots $\alpha_1, \dots, \alpha_n$. Then, as we have seen more than once, it is divisible by the product $(x - \alpha_1) \cdots (x - \alpha_n)$, and since this product is also of degree n, then $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, where c is a number.

Suppose that the coefficient of the leading term of $f(x)$ is 1. Then the number c must also be 1, and we have

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

We can apply Viète's formula (12) to it by putting $a_i = -\alpha_i$. Since all the terms of the polynomial σ_k are products of k variables taken from $a_1, \ldots, a_n$, then replacing a_i by $-\alpha_i$ gives rise to a factor $(-1)^k$, namely: $\sigma_k(-\alpha_1, \ldots, -\alpha_n) = (-1)^k \sigma_k(\alpha_1, \ldots, a_n)$. Hence, from (12) we obtain

$$(13)\quad (x-\alpha_1)\cdots(x-\alpha_n) = x^n - \sigma_1(\alpha_1, \ldots, \alpha_n)x^{n-1} + \cdots + (-1)^n \sigma_n(\alpha_1, \ldots, \alpha_n).$$

This formula expresses the coefficients of the polynomial $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ in terms of its roots and it is also called Viète's formula. You know its special case for the quadratic equation: in that case there are only two polynomials σ_1 and σ_2, $\sigma_1 = \alpha_1 + \alpha_2$, $\sigma_2 = \alpha_1\alpha_2$.

In conclusion, consider again formula (9) for the number of subsets (or the number of combinations). We deduced it from the binomial formula, which was, in turn, proved in Section 3 of Chapter II using the properties of the derivative. That is a rather involved method. It would be desirable to have another proof of this formula based only upon combinatorial reasoning. We shall give such a proof of an even more general formula. Notice that each subset N of the set M defines a partition $M = N + \overline{N}$ where $\overline{N}$ is the complement of N. We consider a more general case: an arbitrary partition $M = M_1 + \cdots + M_r$ into subsets with prescribed number of elements: $n(M_1) = n_1, \ldots, n(M_r) = n_r$. The sequence $(n_1, \ldots, n_r)$ will be called the *type* of the partition $M = M_1 + \cdots + M_r$. We suppose that none of the sets M_i is empty, i.e. that all $n_i > 0$.

Since we are dealing all the time with one and only set M where $n(M) = n$, it shall not always be present in our notations. Denote the number of all possible partitions of our set M which have the prescribed type $(n_1, \ldots, n_r)$ by $C(n_1, \ldots, n_r)$. Of course, we must have $n_1 + \cdots + n_r = n$. Notice also that we are taking into account the order of the sets $M_1, \ldots, M_r$. For instance, for $r = 2$ and given n_1 and n_2, $n_1 + n_2 = n$, we take the partitions $M = M_1 + M_2$ and $M = M_2 + M_1$, with $n(M_1) = n_1$ and $n(M_2) = n_2$, to be different. Indeed, if $n_1 \neq n_2$ these partitions are of different types. Owing to this, each partition $M = M_1 + M_2$ defines one subset M_1 (the first one) and we have a connection with the previously considered problem: $C(n_1, n_2) = v(M, n_1)$. In other words, for any $m < n$, we have $v(M, m) = C(m, n - m)$. We shall now derive an explicit formula for the number $C(n_1, \ldots, n_r)$. Consider an arbitrary partition $M = M_1 + \cdots + M_r$ of type $(n_1, \ldots, n_r)$. Suppose that at least one of the numbers $n_1, \ldots, n_r$ is different from 1. For instance, suppose that $n_1 > 1$ and choose an arbitrary element $a \in M_1$. Denote by M_1' the set of all elements of M_1 different from a (this is the complement of the set $\{a\}$ taken as a subset of M_1). Then we have the partition $M_1 = M_1' + \{a\}$ and to our partition $M = M_1 + \cdots + M_r$ corresponds a new partition $M = M_1' + \{a\} + M_2 + \cdots + M_r$ of type $(n_1 - 1, 1, n_2, \ldots, n_r)$. In this way from all partitions of type $(n_1, n_2, \ldots, n_r)$ we obtain all partitions of

type $(n_1 - 1, 1, n_2, \dots, n_r)$: the partition $M = M_1' + \{a\} + M_2 + \cdots + M_r$ is obtained from the partition $M = M_1 + \cdots + M_r$, where $M_1 = M_1' + \{a\}$. Moreover, one partition of type $(n_1, n_2, \dots, n_r)$ gives rise to n_1 different partitions of type $(n_1 - 1, 1, n_2, \dots, n_r)$, depending on the choice of $a \in M_1$. Hence, we have

$$n_1 C(n_1, n_2, \dots, n_r) = C(n_1 - 1, 1, n_2, \dots, n_r). \tag{14}$$

Applying the same method to partitions of type $(n_1 - 1, 1, n_2, \dots, n_r)$ we obtain that $(n_1 - 1)C(n_1 - 1, 1, n_2, \dots, n_r) = C(n_1 - 2, 1, 1, n_2, \dots, n_r)$, i.e. that $n_1(n_1 - 1)C(n_1, n_2, \dots, n_r) = C(n_1 - 1, 1, 1, n_2, \dots, n_r)$ and

$$n_1!\, C(n_1, n_2, \dots, n_r) = C(\underbrace{1, \dots, 1}_{n_1 \text{ times}}, n_2, \dots, n_r).$$

We now apply the same reasoning to the parameter n_2 in $C(1, \dots, 1, n_2, \dots, n_r)$. In the same way as before we obtain the relation $n_2!\, C(1, \dots, 1, n_2, n_3, \dots, n_r) = C(1, \dots, 1, n_3, \dots, n_r)$ where 1 appears in the first $n_1 + n_2$ places, that is to say

$$n_1!\, n_2!\, C(n_1, n_2, \dots, n_r) = C(\underbrace{1, \dots, 1}_{n_1 + n_2 \text{ times}}, n_3, \dots, n_r).$$

Finally, if we apply the procedure to all the parameters n_1, n_2, ..., n_r we obtain the formula

$$n_1!\, n_2! \cdots n_r!\, C(n_1, n_2, \dots, n_r) = C(\underbrace{1, 1, \dots, 1}_{n \text{ times}}), \tag{15}$$

since $n_1 + n_2 + \cdots + n_r = n$. It remains to find the value of the expression $C(1, \dots, 1)$. In order to do so notice that the above formula was proved for partitions of all types $(n_1, \dots, n_r)$. Apply it to the simplest type (n). There is only one partition of this type, namely $M = M$, and so $C(n) = 1$. On the other hand, formula (15) gives

$$n!\, C(n) = C(\underbrace{1, 1, \dots, 1}_{n \text{ times}}).$$

Therefore $C(1, \dots, 1) = n!$ and substituting this into (15) we obtain the final expression

$$C(n_1, \dots, n_r) = \frac{n!}{n_1!\, n_2! \cdots n_r!}, \quad \text{where } n = n_1 + \cdots + n_r. \tag{16}$$

For $n = 2$ instead of (n_1, n_2), $n_1 + n_2 = n$ it is more usual to write $(n, m - n)$. Since $C(m, n - m) = v(M, m)$, formula (16) reduces to the relation (9).

Remark 1. Consider again the expression $C(1, \dots, 1)$ which appeared at the end of the above proof. What is a partition of type $(1, \dots, 1)$? It is a partition of M into one element sets. But recall that we must take into account the order of the sets in the partition $M = M_1 + \cdots + M_r$. Hence, a partition $M = \{a_1\} + \cdots + \{a_n\}$ gives a numertaion of the elements of M. The number $C(1, \dots, 1)$ shows in how many

ways we can numerate the elements of M. It can be said that $C(1,\dots,1)$ gives the number of different arrangements of the elements of M. As we know, the number of such arrangements is $n!$. Various arrangements are also called *permutations*. For example, if $M=\{a,b,c\}$, which means that $n=3$, we have 6 permutations

$$(a,b,c),\quad (a,c,b),\quad (b,a,c),\quad (b,c,a),\quad (c,a,b),\quad (c,b,a).$$

REMARK 2. In the case $r=2$, the expression $C(n_1,n_2)$ coincides with the binomial coeffcient—we have already given two proofs of this fact. An analogous interpretation has the expression $C(n_1,\dots,n_r)$ for any r. It can be proved that if $x_1,\ \dots\ ,x_r$ are variables, then in the expansion of $(x_1+\dots+x_r)^n$ we obtain terms of the form $x_1^{n_1}\cdots x_r^{n_r}$ with $n_1+\dots+n_r=n$, n_i nonnegative integers, and that the coefficient of $x_1^{n_1}\cdots x_r^{n_r}$ is $C(n_1,\dots,n_r)$. We have only to return to our first definition of a partition, allowing the empty set to appear among M_i's and hence allowing zero to be among the numbers n_i. It is easily seen that (16) remains valid in this case also, provided we take $0!=1$. The proof of this generalization of the binomial formula to the case of r variables is perfectly analogous to the second (combinatorial) proof of the relation $v(M,m)=C_n^m$ (where $n=n(M)$) given above.

For instance, this formula gives that $(x_1+x_2+x_3)^3$ is equal to the sum of terms $C(n_1,n_2,n_3)x_1^{n_1}x_2^{n_2}x_3^{n_3}$ where (n_1,n_2,n_3) runs over all triplets of nonnegative integers such that $n_1+n_2+n_3=3$, and $C(n_1,n_2,n_3)$ is evaluated by formula (16) (with the condition $0!=1$). Substitution gives

$$(x_1+x_2+x_3)^3=$$
$$x_1^3+x_2^3+x_3^3+3x_1^2x_2+3x_1x_2^2+3x_1^2x_3+3x_1x_3^2+3x_2^2x_3+3x_2x_3^2+6x_1x_2x_3.$$

PROBLEMS

1. Let $I=\{p,q\}$ be a set containing two elements and let $M=\{a_1,\dots,a_n\}$ be a set of n elements. To each subset $N\subset M$ correspond the following element: a word from I^n where on the i-th place stands p if $a_i\in N$, and q if a_i does not belong to N. Prove that this establishes a one-to-one correspondence between the sets $U(M)$ and I^n. Use this to derive Theorem 2 from Theorem 1.

2. How can the intersection and the union of subsets N_1 and N_2 of the set M be expressed in terms of their corresponding words from I^n (see Problem 1)?

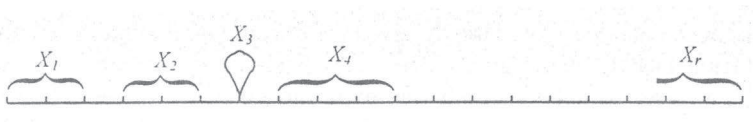
3. Find the number of all partitions $M_1+\dots+M_r$ of all types, but for a fixed number r. Verify that for $r=2$ the answer is given by Theorem 2.

4. Find the sum of all numbers $C(n_1,\dots,n_r)$ for all $n_i\geqslant 0$, $n_1+\dots+n_r=n$, for given r and n. Give two solutions: one based upon Problem 3 and the other based upon the statement given in Remark 2.

5. Find the number of factorizations of a given positive integer n into a product of r factors: $n=a_1\cdots a_r$, which are mutually relatively prime.

6. What is the number of solutions of the equation $x_1+\dots+x_r=n$, for given n and r, in integers $x_i\geqslant 0$? Use the following graphic interpretation of solutions,

which is a modification of the interpretation given in Fig. 4. Let AB be a segment of length $n+r$. Correspond to a solution $(x_1, \ldots, x_r)$ the partition of this segment consisting of the segment of length x_1 starting at A, the segment of length x_2, starting at the first integral point after the end of the first segment, etc; see the figure in which we have $x_3 = 0$.



7. Find the number of different partitions $M = M_1 + M_2$ of type (m, m) if $n(M) = 2m$ and the partitions $M = M_1 + M_2$ and $M = M_2 + M_1$ are not taken to be different. The same question for the partitions $M = M_1 + M_2 + M_3$ of type (m, m, m) if $n(M) = 3m$ and if partitions with different order of M_1, M_2, M_3 are not taken to be different. Finally, the same question for the partitions of type (k, k, l, l, l), $n(M) = 2k + 3l$ and partitions in which equivalent subsets have different order are not taken to be different.

8. What is the form of the term of the polynomial $(x_1 + \cdots + x_n)^2$? The same question for the polynomial $(x_1 + \cdots + x_n)^3$.

9. How many terms are there in the polynomial $(x_1 + \cdots + x_r)^n$, supposing that similar terms are grouped together?

10. Express the polynomial $a_1^2 + a_2^2 + \cdots + a_n^2$ in terms of polynomials σ_1 and σ_2. Suppose that the polynomial $x^n + ax^{n-1} + bx^{n-2} + \cdots$ has n real roots. Prove that $a^2 \geqslant 2b$. When does the equality $a^2 = 2b$ take place? Hint: use Bézout's theorem from Section 1 of Chapter II and the fact that a sum of squares of real numbers cannot be negative.

11. Give a combinatorial proof of the relation $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ for binomial coefficients (formula (26) of Chapter II), interpreting C_n^k as $v(M, k)$ where $n(M) = n$. Generalize this relation to the numbers $C(n_1, \ldots, n_r)$.

12. Give a combinatorial proof of the relation $C_n^m = C_n^{n-m}$ for binomial coefficients.

(to be continued in the next issue)

I. R. Shafarevich,
Russian Academy of Sciences,
Moscow, Russia