INTERNATIONAL SERIES OF MONOGRAPHS IN
PURE AND APPLIED MATHEMATICS

VOLUME 41

THE ALGEBRAIC THEORY OF SWITCHING CIRCUITS

The Algebraic Theory of Switching Circuits

BY

GR. C. MOISIL

Member of the Romanian Academy, Foreign Member of the Polish Academy of Sciences,
Associate Member of the Academy of Science of Bologna, Membre of the International
Institute of Philosophy

PERGAMON PRESS
OXFORD · LONDON · EDINBURGH . NEW YORK
TORONTO · SYDNEY · PARIS . BRAUNSCHWEIG

EDITURA TEHNICĂ
BUCHAREST

Pergamon Press Ltd, Headington Hill Hall, Oxford
4 & 5 Fitzroy Square, London W. 1
Pergamon Press (Scotland) Ltd., 2 & 3 Teviot Place, Edinburgh 1
Pergamon Press Inc., Maxwell House, Fairview Park, Elmsford, New York 10523
Pergamon of Canada Ltd., 207 Queen's Quay West, Toronto 1
Pergamon Press (Aust.) Pty. Ltd., 19a Boundary Street, Rushcutters Bay,
N. S. W. 2011, Australia
Pergamon Press S. A. R. L., 24 rue des Écoles, Paris 5^e
Vieweg & Sohn GmbH, Burgplatz 1, Braunschweig

First English edition 1969

Library of Congress Catalog Card No. 63—10024

This book is the English translation of the Romanian volume TEORIA ALGEBRICĂ A MECANISMELOR AUTOMATE by Gr. C. Moisil, published by Editura Tehnică, Bucharest, with supplements written by the author for the English edition.

Printed in Romania

08 010148 8

CONTENTS

PART ONE

PART TWO

PART THREE

PART FOUR

PART FIVE

PREFACE TO THE ENGLISH EDITION

During the last half century, the mathematical sciences underwent an essential change, by ceasing to be a quantitative science and becoming a structural science. Many people wondered whether the new mathematics would be useful for understanding the world and for its transformations.

Nowadays, the answer to this problem is easy, by giving as examples the mathematical linguistics, the pseudo-Boolean programming, the theory of the programming languages; the promising outset of the mathematical psychology, mathematical sociology and mathematical poetics cannot be left out. But one must not forget that the first technical discipline based on this structural mathematics was the algebraic theory of switching circuits.

The first to introduce the idea of the use of mathematical logic in the theory of networks with contacts and relays was the Russian physicist P. S. EHRENFEST, in a review of the Russian translation of L. COUTURAT's "Algèbre de la Logique" in Журнал русского физико-химического общества, physics section, XLII, section II, no. 10, p. 382, 1910.

EHRENFEST threw into relief the fact that the algebra of logic could be applied to the study of circuits with contacts, for instance to the study of an automatic exchange.

EHRENFEST posed the question :

"Следует ли при решении этих вопросов раз на всегда удовлетвориться гениальным — а по большей части просто рутинным способом пробования на графике?

Правда ли что несмотря на существование уже разработанной 'Алгебры-логики' своего рода 'Алгебра распределительных схем' должна считаться утопией?"

the translation of which is :

"Should we, when resolving these problems, be satisfied, once for all, with the ingenious and in a great measure simple solution, obtained from routine trials on graphs?

Is it reasonable, while an 'algebra of logic' exists, to consider a special 'algebra of switching circuits' as utopian?"

NAKASHIMA and HANZAWA published in December 1936 and in February 1937, in Japanese, in the Journal of the Institute of Engineering and Electrocommunication of Japan, two papers in which several algebraic laws of series and parallel connexions appear, which coincide with the laws of Boolean algebra; the authors, however, do not mention that this algebra is the Boolean algebra. The abstracts in English appeared in 1938—1941, in the Japanese periodical Nippon Electrical Communication Engineering.

These papers were not widely circulated.

In 1938, V. I. Shestakov sustained his Candidate thesis at the University of Moscow:

В. И. Шестаков. Некоторые математические методы конструирования и упрощения двухполюсных электрических схем класса А. (Some mathematical methods for the synthesis and the simplification of electrical two-terminals of class A).

The work was printed later on:

В. И. Шестаков. Алгебра двухполюсных схем постоенных исключительно из двухполюсников (Алгебра А—схем) (The algebra of two-terminal circuits constructed only with two-terminals — Algebra of A-circuits). Журнал технической физики t. XI, 1941 no. 6, p. 532.

В. И. Шестаков. Алгебра двухполюсных схем постоенных исключительно из двухполюсников (Алгебра А-схем) (The algebra of two-terminal circuits constructed only with two terminals — Algebra of A-circuits) Автоматика и телемеханика t. XV, 1941, p. 15.

Also in 1938, Claude Shannon published:

Claude Shannon. A symbolic analysis of relay and switching circuits. Trans. A.I.E.E., 1938, no. 57, p. 713.

In 1950, the volume of M. A. Gavrilov appeared:

М. А. Гаврилов. Теория релейно —контактных схем. Академия Наук СССР, Институт автоматики и телемеханики, Изд. Академии Наук СССР, Москва-Ленинград 1950 г.

Translations: Relaisschalttechnik für Starkstom- und Schwachstromanlagen. VEB Verlag Technik, Berlin, 1953. Teoria releovych kontaktovych schemat reolozili M. Novotny. E. Prager, Praha, SNTL, 1952.

Shortly afterwards, it was followed by the Harvard University volume† and by that of W. Keister, Alistair Ritchie and Washburn††.

From 1950 on, the theory of switching circuits developed vertiginously. We cannot mention all the books dedicated

---

† Synthesis of electronic computing and control circuits, by the Staff of the Computation Laboratory of Harvard University, vol. 27, 1951.

Translation into Russian:

Синтез электронных вычислительных и управляющих схем. Москва, 1954, Изд. Иностр. Лит. 1954.

†† William Keister, Alistair Ritchie, Seth H. Washburn. The Design of Switching Circuits. The Bell Laboratories Series. D. van Nostrand Company Inc., Princeton, New Jersey, Toronto, New York, London. 1st. Ed. Sep. 1951; 2nd Ed. Feb. 1952; 3rd Ed. Jan. 1953; 4th Ed. May 1955; 5th Ed. March 1956.

to it and not even as much as a part of the published articles, but we cannot omit to mention the volumes of R. GRÉA and R. HIGONNET †, of S. H. CALDWELL ††, of P. NASLIN ††† and of RIGO RIGHI ††††. From 1960 forward, the bibliography of the books published on this subject is particularly abundant.

This first application of structural mathematics to technics constitutes an indisputable success.

The Romanian mathematicians undertook the study of this theory as early as 1949; a survey followed by a bibliography of these researches are given on pp. 677 sqq and 687 sqq of this volume; the titles of the books and of the papers are translated into English.

There were four suitable methods for studying the switching circuits.

One of them was in the way open by V. I. SHESTAKOV and CLAUDE SHANNON : the use of Boolean algebras. All the above mentioned books made use of this method that had something surprising : it made the connection between mathematical logic and the theory of switching circuits. It was very impressive for an enthusiast of mathematical logic to meet again its formulae in a circuit with contacts and relays, with diodes, triodes, transistors, as well as with cryogenic, hydraulic or pneumatic elements. Several books published by Romanian researches are using this method. Their list is given on pp. 687 sqq.

The second method used the still less estimated : many-valued logics. The amazement became complete, when one met again the modern discussions on the tertium non datur

---

† R. GRÉA, R. HIGONNET. Étude logique des circuits electriques et des systèmes binairs. Berger-Levrault, Paris, 1955. Translation into English.

R. A. HIGONNET and R. A. GRÉA. Logical design of electrical circuits, McGraw-Hill, New York.

†† SAMUEL H. CALDWELL. Switching circuits and logical design. John Wiley, 1958.

††† PIERRE NASLIN. Circuits à relais et automatismes à séquences. Paris, Dunod, 1958.

†††† RIGO RIGHI. Algebra booleana. Lezioni tenute all'Instituto superiore delle Poste e Telecomunicazioni. Mimeographed under the supervision of A. Vighi, Rome, 1960.

RIGO RIGHI. Algebra booleana con applicazioni alla teoria degli automatismi a contatti. Lezioni tenute all'Instituto superiore delle Poste e Telecomunicazioni.

RIGO RIGHI. Algebra di Boole ed applicazioni, parte prima. Edizioni scientifiche Siderea. Roma, 1967.

or the Aristotelian naval battle in the hazards of the switching circuits. To this method, I devoted a volume printed in French †.

The third method makes use of graph theory. Issued from the studies on electrical circuits, it was to be expected that the combinational topology as well as the graph theory should not be forgotten by those who studied any category of electrical circuits. The method was much used in many researches. The Romanian investigators and chiefly PAUL CONSTANTINESCU, ST. PANĂ, I. MUNTEAN, L. LIVOVSCHI and I. TOMESCU contributed equally by applying this method.

The fourth is the method of Galois fields. The concept of Galois field belonged to the theory of numbers but nowadays it belongs to algebra. At all events, nobody could ever have presumed that it should build a technical discipline. That is the method made use of in this book.

Since the theory is not too wide-spread among those who do not make a special study of algebra, I endeavoured to expose it leisurely and completed it with immediate examples and applications. The author hopes that the book could be accessible without any schooling.

In the Galois fields, all computations are made exactly as everybody has learned them in college algebra. That is why, each time such a calculation is to be made, this method is very convenient. For instance, every one can try to develop the computations from Chap. XXVIII, § 4; Chap. XXIX, §§ 2, 3; Chap. XXX, §§ 2, 3, 4; Chap. XXXI.

Besides, the method offers the advantage of being uniformly applicable to various types of finite automata. Thus, the same methods used for studying the switching circuits with ordinary relays or with tubes can be used for the study of circuits with bistable relays or with polarized relays. However, though the method is suitable to the study of the operation of these circuits, it is not to the study of the structural problems, such as the problem of the structural synthesis of a two-terminal with contacts, neither to a circuit with tubes, transistors etc., nor to the study of their simplification.

The Romanian researches in this domain were undertaken by a mixed group formed by the Mathematical Ins-

---

† GR. C. MOISIL. Théorie structurelle des automates finis. Paris, Gauthier-Villars, 1967.

titute of the Academy of the Socialist Republic of Romania and the Mathematical Department of the Bucharest University. Leon Livovschi and the author gave lectures and lessons on this problem, as early as 1949. With Gh. Ioanin we worked since 1953, and together with Paul Constantinescu, Mariana Coroi-Nedelcu and C. Popovici we started to make a methodical work, by meeting ourselves in a research seminar since 1954.

In this seminar participated also E. Goilav, Iulian Pop, and a little later Sergiu Rudeanu, then Toma Gaşpar, I. Muntean, I. Fîlotti, I. Tomescu, V. Căzănescu, Ivo Rosenberg from Brno, Jean Chinal and M. Denouette from Paris.

The author thanks all these collaborators, mathematicians as well as engineers, for their contributions to this seminar, the result of which led to settling quite a number of problems in the theory of switching circuits.

Nor can the author forget that, since a long time ago, he collaborates with the research group that, under the guidance of M. A. Gavrilov, is working at the Moscow Institute of Automatics and Telemechanics. Valentina Ostianu of this Institute, possessing quite as well both the Romanian and the Russian languages, beside knowing the algebraic theory of switching circuits, had a large contribution by making known in Moscow the works of the Bucharest group.

The author does not forget any more the warm interest shown towards the Romanian research group by Rigo Righi from Rome, Mario Villa from Bologna, W. Nowacki from Warsaw, J. Kožešnik from Prague, Jean Ville, Max Namy, P. Naslin et M. Pélegrin from Paris, J. Kuntzman from Grenoble, thanks to whom he was able to give at Rome, Varenna, Bologna, Warsaw (Jablonna), Paris and Grenoble general lectures on the subject and to publish several books containing his own researches.

Since the publication of the Romanian edition, many years ago, no other book applying the method of the Galois fields was published. That is why this volume had to undergo no modifications; the few observations to the unchanged text are given in the Addenda, pp. 671 sqq.

March 1968 Gr. C. MOISIL

PREFACE TO THE ROMANIAN EDITION

The algebraic theory of switching circuits is, no doubt, one of the most unexpected applications of mathematics.

The whole of classical mathematical physics, relativistic and quantum, deterministic and probabilistic, uses infinitesimal analysis as a mathematical instrument, from the respectable differential and integral calculus to the glamorous functional analysis; the physical magnitudes are continuous and the mathematical instrument is the analysis of this continuity; the jumps introduced by quantum mechanics are mathematically subordinated to this type of description. Technology utilizes such physical laws and the theory of Differential Equations, both ordinary or with partial differential coefficients, with its entire development, covers this domain in which, from the abstract mathematician to the designing engineer, a unity of interests is manifest for certain chapters of mathematics.

The algebraic theory of switching circuits exceeds widely this frame. The variables associated with various automation elements, contacts, push-buttons, lamps, relays of different sorts, rotary switches, electronic tubes, transistors, cryotrons, magnetic cores — assume a finite number of values. Often they take on two values: a contact is closed or open, a lamp is switched on or off. The essential feature is not, however, the fact that the variables have two values, but that their domains are finite.

It is therefore not the classical Calculus which will be employed in the study of such electric circuits, but that chapter of mathematics which, by its history, is much more related to the finite: abstract algebra.

In 1910, in a review of the Russian translation of Couturat's book "L'Algèbre de la Logique", the Russian physicist EHRENFEST put forward the idea of applying a chapter of algebra — the algebra of logic —to the study of contact networks.

The idea was rediscovered at a later date. In 1936 NAKASHIMA and HANZAWA published in Japanese a series of papers not widely circulated.

In 1938, V. I. SHESTAKOV in his doctorate thesis at the University of Moscow showed how to apply the rules of the algebra of logic to networks with contacts and relays. Shestakov's discovery developed by M. A. GAVRILOV initiated a large number of researches in this domain, in the USSR.

In the same year 1938 CLAUDE SHANNON, unaware of Shestakov's work, published a study in the A.I.E.E. Transactions in which the algebra of logic is presented as the instrument for investigating networks with contacts and relays. Shannon's work was the starting point of American research in this domain.

In the following twenty years the theory developed and flourished on a large scale.

In Romania, since 1953, several mathematicians and engineers have formed a group which deals with these problems.

So far, several treatises have been published in which the theory is presented. The first is the volume published by M.A. GAVRILOV "Теория релейно контактных схем" in 1950, it was translated into German in 1953, "Relaisschalttechnik für Stark- und Schwachstromanlagen", and into Czech. This volume was the fundamental book employed by the Romanian investigators.

The works of AIKEN, KEISTER-RITCHIE-WASHBURN, GRÉA — HIGONNET, TOUCHAIS, GAVRILOV, CALDWELL and NASLIN followed.

The Romanian Academy has started the publication in Romania of a series of "Monographs on the algebraic theory of switching circuits". The first volume "Scheme cu comandă directă cu contacte şi relee" ("Combinational networks with contacts and relays") was published recently. Volumes dealing with the sequential operation of networks with ordinary relays and with the operation of circuits with electronic elements are in course of preparation.

We have no knowledge of mimeographed survey works issued in other countries. In the Romanian People's Republic there appeared the lectures delivered by the author in November-February 1953—1954 at the I.C.E.T.† and those delivered by him in the "Lectures on automation", organized by the Commission of Automation of the Academy and by the A.S.I.T.†† in 1958.

---

† Electrotechnical Research Institute

†† Scientific Association of Engineers and Technicians

The aim of the present volume is in the main to show the contributions brought by the author and his co-workers up to August 1st, 1957. Chapters 1—23, 28—31 were completed by April 1st, 1957 and Chapters 24—27 by August 1st, 1957. The author has endeavoured to keep the bibliographic notes up to date.

The characteristic features of the investigations carried out by the Romanian group are pointed out below.

In the first place the author and his co-workers make use of various algebraic tools; it is not only the Boolean algebra, whose primordial interest is not overlooked, which is applied in this volume, but also the theory of finite fields (Galois fields) is widely used. The computations in a finite field are made in agreement with the established rules of classical algebra, this being of a considerable advantage. In addition, this enables the whole automaton to be conceived as a unit. Accordingly, the author was able to broach problems of general theory, such as those included in Chapters 23—31: the problem of synthesis with given programmes for the output elements, the problem of classification, etc. The author holds the view that this method is efficiently adaptable to computing machines.

In this volume, in order to maintain the unity of the book, other algebraic means such as, for instance, multi-valued logic, have not been employed.

In the second place, this group of research workers has emphasized the importance of the sequential operation of the automata. The opposition between "combinational circuits" and "sequential circuits" is essentially just another aspect of the difference between statics and dynamics.

In the description of sequential operations, the variables associated to the current are separated from those associated to contacts. The recurrence relations which describe operations of the network have also been met with, explicitly or implicitly, in the work of V. I. SHESTAKOV, D. HUFFMAN, H. GRENIEWSKI and D. BASILEVSKI, developed at the same time or subsequently to our work. In our studies, these equations appear as proceeding from the elimination of the current variables from two systems of equations: one system by which the current is determined in terms of the position of the contacts, and another system, introduced by the author, the study of which is peculiar to the research work of our group. In this system the position of the contacts of an element at a given instant is determined by the state of the currents and contacts of that element in the preceding instant (or instants). This system, we have called the "characteristic equations" system, must be established for each secondary element considered : relay, polarizing relay, rotary switch, etc.

The characteristic equations, introduced by us in 1954, have enabled us to study networks with various types of secondary elements. The study of networks with secondary elements other than ordinary relays is a third characteristic feature of the investigations carried out in Romania.

A fourth characteristic of our researches is the attention devoted to the so-called multi-position contacts. V. I. SHESTAKOV and A. DUSCHEK have introduced their study; such multi-position contacts are associated with numerous secondary elements. Moreover, elements which vary continuously can be replaced approximately by multi-position contacts. This fact is significant in the author's concept of the mathematical theory of continuous automation in relation to the discrete case. Sometimes the mathematical theory of servo-mechanisms is opposed to that of circuits with contacts and relays. The author does not believe that this opposition should refer to the object of the study, but only to the problems which are under analysis. The algebraic theory, when sufficiently developed, shows the general concept of the automaton, as well as the position and connections of the various elements, while the quantitative study of the stability of operation is incumbent upon the infinitesimal theory.

The author takes the liberty of giving certain indications on the research carried out in Romania after the ultimate elaboration of this volume.

The author has successfully carried out the study of what he calls the "actual operation" of relays. This study is of importance since in certain cases it is necessary to take into consideration the transient position of the contact armature. This is mainly done by means of three-valued logic. Five valued logic is likewise applied in this study.

The author has also studied bridge networks. A. G. LUNTS has shown that the study of the multi-terminals with contacts and possibly with rectifiers is algebraically translated by the study of matrices with their elements in a Boolean algebra. However, when the multi-terminals also have secondary and output elements, the problem takes on a more delicate character.

Numerous examples are given in the book of V. N. ROGINSKII and A. Д. KHARKEVICH "Релейные схем в телефонии". The investigations of M. A. GAVRILOV concerning multiterminals and their transformations have not yet been algebraically interpreted. It is necessary to include in this study the networks with several current levels. This set of problems is, at present, in the process of being worked out.

Finally, the author has studied circuits with electronic elements : triodes, pentodes, transistors, cryotrons. On the one hand, Sheffer's functions have been studied in order to simplify the circuits ; on the other hand, the analysis of the sequential operation of the electronic circuits is achieved by methods similar to those applied to networks with electromagnetic elements.

This volume is intended, as will be seen when reading it, for mathematicians who desire to study an interesting modern application of algebra, which is highly useful to engineers working in the domain of automation with contacts and relays. Furthermore, it will also prove of practical use to those working in the field of computers. The technician must, however, not expect fo find practical indications as the author claims no technical ability of any kind.

Fortunately, the gaps left by my technical insufficiency were filled up by the contribution of several engineers who attended a free course on the algebraic theory of switching circuits.

Our group received considerable assistance from the group led by M. A. GAVRILOV, doctor of technical sciences of the Institute of Automation and Telemechanics of the USSR Academy of Sciences.

The present volume has been read with particular attention by C. POPOVICI ; many omissions were corrected thanks to his conscientiousness and competence.

May 1959 Gr. C. MOISIL

PART ONE

CHAPTER 1

INTRODUCTION

1. Congruences of integers

It is said that two integers† a and b are congruent modulo m (m being an integer) if the difference $a-b$ is divisible by m, i.e. if it is a multiple of m. If a and b are congruent modulo m, we shall write

$$a \equiv b \pmod{m}.$$

This means that there exists an integer k such as

$$a - b = km.$$

If a and b are not congruent modulo m, we write

$$a \not\equiv b \pmod{m}.$$

Example 1. *Modulo* 2 : *any integer is congruent to* 0 *or* 1 ; in other words : *for any integer* a, *we have*

$$a \equiv 0 \pmod{2}$$

or

$$a \equiv 1 \pmod{2},$$

but

$$0 \not\equiv 1 \pmod{2}.$$

For, if a is even, $a = 2h$ and the first congruence is valid. If a is odd, $a = 2h + 1$ and the second congruence is valid.

Example 2. *Modulo* 3 : *any integer is congruent to* 0 *or* 1 *or* 2 ; in other words : *for any integer* a, *we have*

$$a \equiv 0 \pmod{3}$$

or

$$a \equiv 1 \pmod{3}$$

or

$$a \equiv 2 \pmod{3}.$$

---

† By *integer* we understand a positive or negative integer including 0.

For, any number divided by 3 gives as remainder 0 *or* 1 *or* 2, i.e. it is of the form $3h$ or $3h + 1$ or $3h + 2$.

One can see that

$$0 \not\equiv 1 \pmod{3},$$

$$0 \not\equiv 2 \pmod{3},$$

$$1 \not\equiv 2 \pmod{3}.$$

Example 3. *Modulo* 4 : *any integer is congruent to* 0 *or* 1 *or* 2 *or* 3 ; in other words : *for any integer a, we have*

$$a \equiv 0 \pmod{4}$$

or

$$a \equiv 1 \pmod{4}$$

or

$$a \equiv 2 \pmod{4}$$

or

$$a \equiv 3 \pmod{4}.$$

Example 4. *Modulo* m : *any integer is congruent to one of the numbers* $0, 1, 2, \ldots, m - 1$; *no two of the numbers* $0, 1, \ldots, m-1$ *are congruent modulo* m.

Here are a few immediate properties of congruence.

Theorem I. *Any integer is congruent with itself with respect to any modulus* ; in other words : *whatever the integers a and m are, we have* :

$$a \equiv a \pmod{m}.$$

For, $a - a = 0 = 0 \cdot m$, therefore the above definition is satisfied.

Theorem II. *If*

$$a \equiv b \pmod{m},$$

then

$$b \equiv a \pmod{m}.$$

For, if $a \equiv b \pmod{m}$, then $a - b = km$, k being an integer, hence $b - a = (-k)\,m$, hence $b-a$ is the multiple $(-k)\,m$, and hence $b \equiv a \pmod{m}$.

Theorem III. *If*

$$a \equiv b \pmod{m},$$

and

$$b \equiv c \pmod{m},$$

then

$$a \equiv c \pmod{m}.$$

For, if $a \equiv b \pmod{m}$, there exists an integer h such that

$$a - b = hm$$

and if $b \equiv c \pmod{m}$, there exists an integer k such that

$$b - c = km,$$

therefore,

$$a - c = (a - b) + (b - c) = (h + k)\ m,$$

and $h + k$ is an integer, therefore $a \equiv c \pmod{m}$.

Consequence. *Two integers congruent to a third are congruent to one another.* In other words : *if we have*

$$a \equiv c \pmod{m},$$

$$b \equiv c \pmod{m},$$

then

$$a \equiv b \pmod{m}.$$

Indeed, let

$$a \equiv c \pmod{m},$$

$$b \equiv c \pmod{m}.$$

The latter congruence gives, by virtue of Theorem II,

$$c \equiv b \pmod{m}.$$

This, together with the first congruence gives, by virtue of Theorem III,

$$a \equiv b \pmod{m}.$$

Theorem IV. *Congruences with respect to the same modulus may be added term by term* ; in other words : *if*

$$a \equiv b \pmod{m},$$

$$c \equiv d \pmod{m},$$

then

$$a + c \equiv b + d \pmod{m}.$$

Indeed, the two congruences show that $a - b = hm$, and $c - d = km$, h and k being integers, hence

$$(a + c) - (b + d) = (a - b) + (c - d) = (h + k)\,m,$$

which justifies the last congruence.

Example 1. Let us determine to which integer $a + b$ is congruent modulo 2.

If $a \equiv 0$, $b \equiv 0 \pmod 2$, then $a + b \equiv 0 \pmod 2$.

If $a \equiv 0$, $b \equiv 1 \pmod 2$, then $a + b \equiv 1 \pmod 2$.

If $a \equiv 1$, $b \equiv 0 \pmod 2$, then $a + b \equiv 1 \pmod 2$.

If $a \equiv 1$, $b \equiv 1 \pmod 2$, then $a + b \equiv 1 + 1$
$\equiv 0 \pmod 2$.

These results can be tabulated

+	0	1
0	0	1
1	1	0

writing the number congruent to $a+b$ in row a and column b. This table is called the *addition table modulo* 2.

Example 2. Let us determine to which integer $a + b$ is congruent modulo 3. The result is given by the table

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

made up as above. Its justification is easy; for instance, $2 + 2 \equiv 4 \equiv 1 \pmod 3$.

Example 3. Let us determine to which integer $a + b$ is congruent modulo 4. The result is given by the table

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Example 4. Let us determine to which integer $a + b$ is congruent modulo 5. The result is given by the table

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Theorem V. *Congruences may be multiplied term by term.* In other words: *if*

$$a \equiv b \pmod{m},$$

$$c \equiv d \pmod{m},$$

then

$$ac \equiv bd \pmod{m}.$$

Indeed, the two congruences show that $a - b = hm$, and $c - d = km$, hence $a = b + hm$, and $c = d + km$, hence $ac = bd + (bk + dh + hkm)m$, hence, $bk + dh + hkm$ being an integer, $ac \equiv bd \pmod{m}$.

Example 1. To which integer is ab congruent modulo 2? The result is given by the table

	0	1
0	0	0
1	0	1

Indeed,

if $a \equiv 0$, $b \equiv 0 \pmod{2}$, then $ab \equiv 0 \cdot 0 \equiv 0 \pmod{2}$;

if $a \equiv 0$, $b \equiv 1 \pmod{2}$, then $ab \equiv 0 \cdot 1 \equiv 0 \pmod{2}$;

if $a \equiv 1$, $b \equiv 0 \pmod{2}$, then $ab \equiv 1 \cdot 0 \equiv 0 \pmod{2}$;

if $a \equiv 1$, $b \equiv 1 \pmod{2}$, then $ab \equiv 1 \cdot 1 \equiv 1 \pmod{2}$.

Example 2. To which integer is *ab* congruent modulo 3? The result is given by the table

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example 3. To which integer is *ab* congruent modulo 4? The result is given by the table

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Example 4. To which integer is *ab* congruent modulo 5? The result is given by the table

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Theorem VI. *We have*

$$-x \equiv m - x \pmod{m}.$$

This property is obvious. It allows us to write the integer to which $-x$ is congruent, the result being a positive integer.

Example 1. To which integer is $-x$ congruent modulo 2? We have

$$-0 \equiv 0 \pmod{2},$$

$$-1 \equiv 1 \pmod{2}.$$

We group these results in the table

x	0	1
$-x$	0	1

Example 2. To what is $-x$ congruent modulo 3? The result is given by the table

x	0	1	2
$-x$	0	2	1

Example 3. To what is $-x$ congruent modulo 4? The result is given by the table

x	0	1	2	3
$-x$	0	3	2	1

Example 4. To what is $-x$ congruent modulo 5? The result is given by the table

x	0	1	2	3	4
$-x$	0	4	3	2	1

Theorem VII. *Congruences can be subtracted term by term.* In other words: *if*

$$a \equiv b \pmod{m},$$

$$c \equiv d \pmod{m},$$

then

$$a - c \equiv b - d \pmod{m},$$

since from $c \equiv d \pmod{m}$, we deduce $c = d + km$, hence $-c = -d + (-k)m$, hence $-c \equiv -d \pmod{m}$, hence $a - c \equiv a + (-c) \equiv b + (-d) \equiv b - d \pmod{m}$.

This theorem will not be used frequently since we can replace $-x$ by $m - x$.

Hereafter, we shall denote by $\mathfrak{J}/(m)$ the set formed by the m numbers

$$0, 1, \ldots, m-1.$$

If p is prime[†], $\mathfrak{J}/(p)$ will be called $\mathfrak{GF}(p)$.

[†] For the importance of the case of a prime modulus, cf. Chapter 18.

For instance $\mathfrak{G}\mathfrak{J}(2)$ is made up of 0 and 1; $\mathfrak{G}\mathfrak{J}(3)$ is made up of 0, 1, 2; $\mathfrak{G}\mathfrak{J}(5)$ of 0, 1, 2, 3, 4; however, the set made up of 0, 1, 2, 3 will be called $\mathfrak{J}/(4)$.

With the numbers

$$0, 1, \dots, m-1$$

we can, in accordance with the Theorems IV, VII and V, carry out operations of addition, subtraction, multiplication† and obtain tables like the ones in the foregoing examples.

Example 5. Let us determine the number to which $a+b$ is congruent modulo m. The result is given by the table

$+$	0	1	2	3	4...	$m-3$	$m-2$	$m-1$
0	0	1	2	3	4...	$m-3$	$m-2$	$m-1$
1	1	2	3	4	5...	$m-2$	$m-1$	0
2	2	3	4	5	6...	$m-1$	0	1
3	3	4	5	6	7...	0	1	2
4	4	5	6	7	8...	1	2	3
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
$m-3$	$m-3$	$m-2$	$m-1$	0	1...	$m-6$	$m-5$	$m-4$
$m-2$	$m-2$	$m-1$	0	1	2...	$m-5$	$m-4$	$m-3$
$m-1$	$m-1$	0	1	2	3...	$m-4$	$m-3$	$m-2$

This arithmetic, which we can call "arithmetic modulo m", does not coincide with the usual arithmetic of integers. Indeed, on the one hand, only m elements enter into this arithmetic instead of an infinity of integers. On the other hand, the addition, carried out according to the above table, is not the usual addition. For instance, this addition yields

---

† We consider the elements $0, \dots, m-1$ as given elements for which we define two operations that we have denoted by "$+$" and "$\cdot$"

$2+(m-1)^{\dagger}=1$. The same applies to multiplication, which is not the usual multiplication. Nevertheless the computations modulo m are easy to perform.

On the other hand, when we have to carry out a series of operations practically, we can perform them without any difficulty, by replacing any number obtained by its remainder modulo m. For instance, modulo 3,

$$E = [(2+3+2)\ (1+2+1)+(1+2+2)](1+1)$$

$$= (7\cdot 4+5)\cdot 2 \equiv (1\cdot 1+2)\cdot 2 \pmod 3,$$

since $7\equiv 1,\ 4\equiv 1,\ 5\equiv 2 \pmod 3$. Hence

$$E\equiv (1+2)\cdot 2\equiv 0 \pmod 3.$$

On the other hand, all the rules of computation regarding addition, subtraction and multiplication, e.g. changing the order of the terms of a sum, changing the order of the factors in a product, the substitution in a sum of a number of terms by their sum, the substitution in a product of a number of factors by their product, the suppression of brackets, are all valid in arithmetic modulo m. These rules are transcribed by

$$a+b=b+a,\quad ab=ba,$$

$$a+b+c=(a+b)+c=a+(b+c),$$

$$abc=(ab)c=a(bc),$$

$$a(b+c)=ab+ac.$$

The validity of these rules will not be proved in this book. The reader can verify them for $m=2$, 3, 5, with the help of the tables on pages 26 – 28.

With respect to the following rules : a product is not null unless one of its factors is null, and from $ax=ay$ $(a\neq 0)$ we deduce $x=y$, which is not always valid, we refer the reader to page 373 of this book.

---

† We shall use the "$=$" sign between the abstract elements $0\ldots m-1$ and the "$\equiv$" sign between the ordinary integers $\ldots, -1, 0, 1\ldots, m-1$, n, $m+1$, ... This ambiguity of the signs of "0"... "$m-1$" will not lead o any difficulties in what follows.

Likewise, we shall use the "$\equiv \pmod m$" sign when remembering the nodulus m.

2. Variables associated to elements of switching circuits

A variable which can take on n values will be called n-valued (two-valued, three-valued, four-valued, five-valued, etc.).

Variables associated to contacts. A contact can have two positions : open or closed. We shall associate to a contact (Fig. 1) a variable a to which we assign two values, 0 and 1, namely :

$$a = 0, \text{ if the contact is open,}$$

$$a = 1, \text{ if the contact is closed.}$$

We may say that we associate to a contact a variable in $\mathfrak{G}\mathfrak{F}(2)$.

Variables associated to a relay contact armature. An ordinary relay consists of an electromagnet which attracts an armature with contacts (Fig. 2). When no current passes through the relay winding, the armature is in a position I, where some of the contacts x^- are closed, others x^+, are open. When current passes through the winding, the armature, attracted by the electromagnet, takes another position, II, where the x^- contacts are open, while the x^+ contacts are closed.

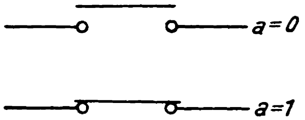

Fig. 1

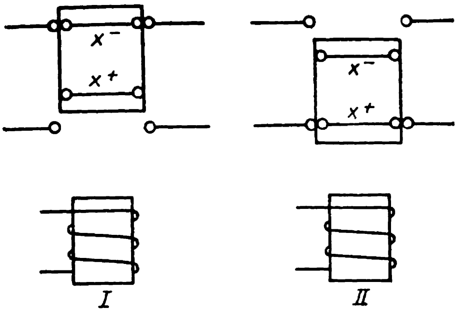

Fig. 2

We shall assign three variables to this armature. The variable x will indicate the position of the armature :

$$x = 0, \text{ if the armature is at rest, i.e. in position } I\,;$$

$$x = 1, \text{ if the armature is attracted, i.e. in position } II.$$

The variable x^+ is associated to the contacts x^+, which are called *closing contacts.* It can be seen that

$x^+ = 0$, if the closing contact is open, that is if the armature is at rest (position *I*), that is if $x = 0$;

$x^+ = 1$, if the closing contact is closed, that is if the armature is attracted (position *II*), that is if $x = 1$.

The variable x^- is associated to the contacts x^- which are called *opening contacts.* It can be seen that we have:

$x^- = 1$, if the opening contact is closed, that is if the armature is at rest (position *I*), that is if $x = 0$;

$x^- = 0$, if the opening contact is open, that is if the armature is attracted (position *II*), that is if $x = 1$.

It can be seen that there exists a correspondence among the 3 variables x, x^+, x^- given by the table

x	0	1
x^+	0	1
x^-	1	0

It can also be seen that we have

$$x^+ \equiv x \pmod{2}.$$

It can be seen, by comparing this table with the table of Example 1, page 26, that we have

$$x^- \equiv x + 1 \pmod{2}.$$

A relay of the type described above will be called an *ordinary relay with ideal contacts.* The above discussion shows us that *a variable x in $\mathfrak{GF}$ (2) will be associated to the armature of an ordinary relay with ideal contacts; the variable x^+ which describes the situation of the closing contacts is given by*

$$x^+ \equiv x \pmod{2}$$

and the variable x^- which describes the situation of the opening contacts is given by

$$x^- \equiv x + 1 \pmod{2}.$$

However, let us note that, while being attracted, the armature has a transient position, in which both the closing and the opening contacts are open (Fig. 3).

Likewise, when the armature comes back to its rest position, the change from position *III* to position *I* is through the transient position *II* where all the contacts

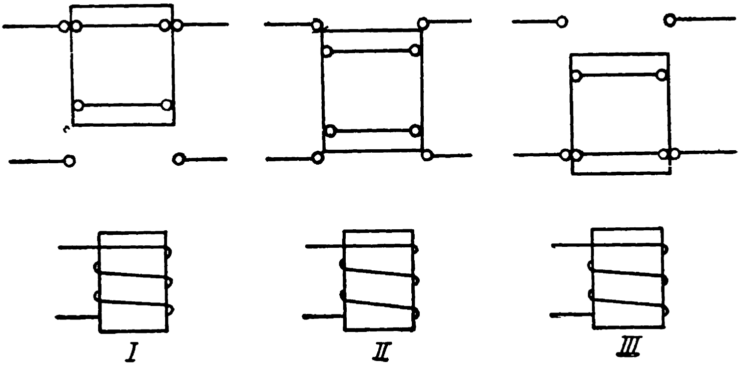

Fig. 3

are open. This type of relay is called an *ordinary relay with real contacts.*

We see that in order to describe the position of its armature it is necessary for the variable to take on three different values, hence : *we shall associate a variable in* $\mathfrak{G}\mathfrak{F}$ (3) *to the armature of an ordinary relay with real contacts.*

There are relays for which one cannot consider only one transient position of the contacts, namely relays in which

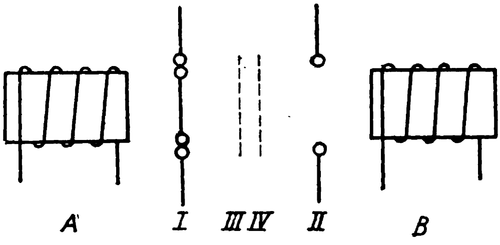

Fig. 4

there are two electromagnets (Fig. 4); if the current flows through the winding of the electromagnet *A*, the armature is attracted by this electromagnet and takes on position *I*; if the current flows through the winding of the electromagnet *B*, the latter attracts the armature, which takes on position *II*; if the current does not flow through any of the windings, the armature remains in the position *I* or *II* in which it was; if the current stops flowing before the armature has reached one of the positions *I* or *II*, it comes to position *I* if it was in position *III*; if it was in position *IV* however, it comes to position *II*. That is the actual operation of bistable relays.

Polarized relays are also made, the armature of which, being magnetic, is attracted or repelled by the relay electromagnet according to the direction of the current flowing through the winding (Fig. 5).

For such a relay, the contact armature will have three positions: "at rest", "attracted" and "repelled". This type of relay will be called a *polarized relay with ideal contacts.* We see that a *variable in* $\mathfrak{G}\mathfrak{F}$ (3) *must be associated to the armature of a polarized relay with ideal contacts.*

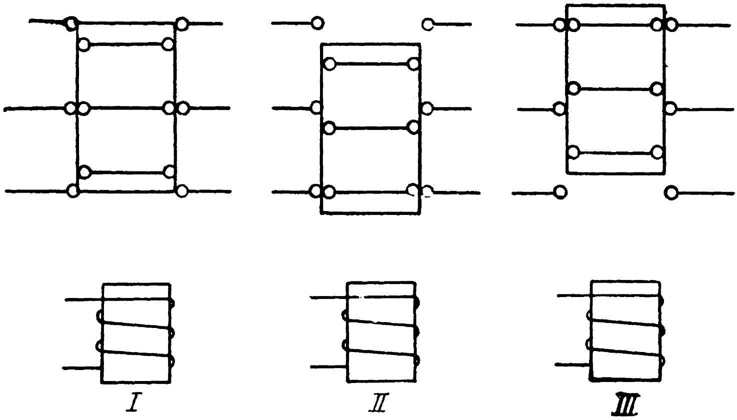

Fig. 5

If, however, we must take into account the transient positions, the latter will be two in number: a transient position between the "at rest" and the "attracted" position and another between the "at rest" and the "repelled" position; hence, for these relays, which we call *polarized relays with actual contacts*, we shall have to consider five positions of the armature, and hence *we shall associate a variable in* $\mathfrak{G}\mathfrak{F}$ (5) *to the armature of a polarized relay with actual contacts.*