ENCYCLOPAEDIA OF MATHEMATICS

Volume 5

I – Lituus

ENCYCLOPAEDIA OF MATHEMATICS

Volume 5

I – Lituus

An updated and annotated translation of the Soviet
'Mathematical Encyclopaedia'

KLUWER ACADEMIC PUBLISHERS
Dordrecht / Boston / London

Library of Congress Cataloging-in-Publication Data

CIP

Matematicheskaia entsiklopediia. English.
Encyclopaedia of mathematics.

1. Mathematics—Dictionaries. I. Hazewinkel, Michiel. II. Title.
QA5.M3713 1987 510'.3'21 87-26437
ISBN 1-55608-010-7 (set)
ISBN 1-55608-004-2 (v. 5)

Published by Kluwer Academic Publishers,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Kluwer Academic Publishers incorporates
the publishing programmes of
D. Reidel, Martinus Nijhoff, Dr W. Junk and MTP Press.

Sold and distributed in the U.S.A. and Canada
by Kluwer Academic Publishers,
101 Philip Drive, Norwell, MA 02061, U.S.A.

In all other countries, sold and distributed
by Kluwer Academic Publishers Group,
P.O. Box 322, 3300 AH Dordrecht, The Netherlands.

SOVIET MATHEMATICAL ENCYCLOPAEDIA

Editor-in-Chief

I. M. Vinogradov

Editorial Board

S. I. Adyan, P. S. Aleksandrov, N. S. Bakhvalov, A. V. Bitsadze, V. I. Bityutskov (Deputy Editor-in-Chief), L. N. Bol'shev, A. A. Gonchar, N. V. Efimov, V. A. Il'in, A. A. Karatsuba, L. D. Kudryavtsev, B. M. Levitan, K. K. Mardzhanishvili, E. F. Mishchenko, S. P. Novikov, E. G. Poznyak, Yu. V. Prokhorov (Deputy Editor-in-Chief), A. I. Shirshov, A. G. Sveshnikov, A. N. Tikhonov, P. L. Ul'yanov, S. V. Yablonskiĭ

Translation Arrangements Committee

V. I. Bityutskov, R. V. Gamkrelidze, Yu. V. Prokhorov

'Soviet Encyclopaedia' Publishing House

PREFACE

This ENCYCLOPAEDIA OF MATHEMATICS aims to be a reference work for all parts of mathematics. It is a translation with updates and editorial comments of the Soviet *Mathematical Encyclopaedia* published by 'Soviet Encyclopaedia Publishing House' in five volumes in 1977–1985. The annotated translation consists of ten volumes including a special index volume.

There are three kinds of articles in this ENCYCLOPAEDIA. First of all there are survey-type articles dealing with the various main directions in mathematics (where a rather fine subdivision has been used). The main requirement for these articles has been that they should give a reasonably complete up-to-date account of the current state of affairs in these areas and that they should be maximally accessible. On the whole, these articles should be understandable to mathematics students in their first specialization years, to graduates from other mathematical areas and, depending on the specific subject, to specialists in other domains of science, engineers and teachers of mathematics. These articles treat their material at a fairly general level and aim to give an idea of the kind of problems, techniques and concepts involved in the area in question. They also contain background and motivation rather than precise statements of precise theorems with detailed definitions and technical details on how to carry out proofs and constructions.

The second kind of article, of medium length, contains more detailed concrete problems, results and techniques. These are aimed at a smaller group of readers and require more background expertise. Often these articles contain more precise and refined accounts of topics and results touched upon in a general way in the first kind of article.

Finally, there is a third kind of article: short (reference) definitions.

Practically all articles (all except a few of the third kind) contain a list of references by means of which more details and more material on the topic can be found. Most articles were specially written for the encyclopaedia and in such cases the names of the original Soviet authors are mentioned. Some articles have another origin such as the *Great Soviet Encyclopaedia* (*Bol'shaya Sovetskaya Entsiklopediya* or BSE).

Communication between mathematicians in various parts of the world has certainly greatly improved in the last decennia. However, this does not mean that there are so-to-speak 'one-to-one onto' translations of the terminology, concepts and tools used by one mathematical school to those of another. There also are varying traditions of which questions are important and which not, and what is considered a central problem in one tradition may well be besides the point from the point of view of another. Even for well-established areas of mathematical inquiry, terminology varies across languages and even within a given language domain. Further, a concept, theorem, algorithm, . . . , which is associated with one proper name within one tradition may well have another one in another, especially if the result or idea in question was indeed discovered independently and more-or-less simultaneously. Finally, mathematics is a very dynamic science and much has happened since the original articles were finalized around 1977). This made updates desirable (when needed). All this, as well as providing

additional references to Western literature when needed, meant an enormous amount of work for the board of experts as a whole; some indeed have done a truly impressive amount of work. I must stress though that I am totally responsible for what is finally included and what is not of all the material provided by the members of the board of experts.

Many articles are thus provided with an editorial comment section in a different and somewhat smaller typeface. In particular, these annotations contain additional material, amplifications, alternative names, additional references, ... Modifications, updates and other extra material provided by the original Soviet authors (not a rare occurrence) have been incorporated in the articles themselves.

The final (10-th) volume of the ENCYCLOPAEDIA OF MATHEMATICS will be an index volume. This index will contain all the titles of the articles (some 6600) and in addition the names of all the definitions, named theorems, algorithms, lemmas, scholia, constructions, ..., which occur in the various articles. This includes, but is by no means limited to, all items which are printed in bold or italic. Bold words or phrases, by the way, always refer to another article with (precisely) that title.

All articles have been provided with one or more AMS classification numbers according to the 1980 classification scheme (not, for various reasons, the 1985 revision), as have all items occurring in the index. A phrase or word from an article which is included in the index always inherits all the classification numbers of the article in question. In addition, it may have been provided with its own classification numbers. In the index volume these numbers will be listed with the phrase in question. Thus e.g. the Quillen – Suslin theorem of algebraic K-theory will have its own main classification numbers (these are printed in bold; in this case that number is 18F25) as well as a number of others, often from totally different fields, pointing e.g. to parts of mathematics where the theorem is applied, or where there occurs a problem related to it (in this case e.g. 93D15). The index volume will also contain the inversion of this list which will, for each number, provide a list of words and phrases which may serve as an initial description of the 'content' of that classification number (as far as this ENCYCLOPAEDIA is concerned). For more details on the index volume, its structure and organisation, and what kind of things can be done with it, cf. the (future) special preface to that volume.

Classifying articles is a subjective matter. Opinions vary greatly as to what belongs where and thus this attempt will certainly reflect the tastes and opinions of those who did the classification work. One feature of the present classification attempt is that the general basic concepts and definitions of an area like e.g. 55N (Homology and Cohomology theories) or 60J (Markov processes) have been assigned classification numbers like 55NXX and 60JXX if there was no finer classification number different from ...99 to which it clearly completely belongs.

Different parts of mathematics tend to have differences in notation. As a rule, in this ENCYCLOPAEDIA in a given article a notation is used which is traditional in the corresponding field. Thus for example the (repeated index) summation convention is used in articles about topics in fields where that is traditional (such as in certain parts of differential geometry (tensor geometry)) and it is not used in other articles (e.g. on summation of series). This pertains especially to the more technical articles.

For proper names in Cyrillic the British Standards Institute transcription system has been used (cf. Mathematical Reviews). This makes well known names like S. N. Bernstein come out as Bernshteĭn.

In such cases, especially in names of theorems and article titles, the traditional spelling has been retained and the standard transcription version is given between brackets.

Ideally an encyclopaedia should be complete up to a certain more-or-less well defined level

of detail. In the present case I would like to aim at the completeness level whereby every theorem, concept, definition, lemma, construction which has a more-or-less constant and accepted name by which it is referred to by a recognizable group of mathematicians occurs somewhere, and can be found via the index. It is unlikely that this completeness ideal will be reached with this present ENCYCLOPAEDIA OF MATHEMATICS, but it certainly takes substantial steps in this direction. Everyone who uses this ENCYCLOPAEDIA and finds items which are not covered, which, he feels, should have been included, is invited to inform me about it. When enough material has come in this way supplementary volumes will be put together.

The ENCYCLOPAEDIA is alphabetical. Many titles consist of several words. Thus the problem arises how to order them. There are several systematic ways of doing this of course, for instance using the first noun. All are unsatisfactory in one way or another. Here an attempt has been made to order things according to words or natural groups of words as they are daily used in practice. Some sample titles may serve to illustrate this: **Statistical mechanics, mathematical problems in; Lie algebra; Free algebra; Associative algebra; Absolute continuity; Abstract algebraic geometry; Boolean functions, normal forms of.** Here again taste plays a role (and usages vary). The index will contain all permutations. Meanwhile it will be advisable for the reader to try out an occasional transposition himself. Titles like K-theory are to be found under K, more precisely its lexicographic place is identical with 'K theory', i.e. '-' = 'space' and comes before all other symbols. Greek letters come before the corresponding Latin ones, using the standard transcriptions. Thus χ^2-distribution (chi-squared distribution) is at the beginning of the letter C. A$*$ as in C^*-algebra and $*$-regular ring is ignored lexicographically. Some titles involve Greek letters spelled out in Latin. These are of course ordered just like any other 'ordinary' title.

This volume has been computer typeset using the (Unix-based) system of the CWI, Amsterdam. The technical (mark-up-language) keyboarding was done by Rosemary Daniëls, Chahrzade van 't Hoff and Joke Pesch. To meet the data-base and typesetting requirements of this ENCYCLOPAEDIA substantial amounts of additional programming had to be done. This was done by Johan Wolleswinkel. Checking the translations against the original texts, and a lot of desk editing and daily coordination was in the hands of Rob Hoksbergen. All these persons, the members of the board of experts, and numerous others who provided information, remarks and material for the editorial comments, I thank most cordially for their past and continuing efforts.

The original Soviet version had a printrun of 150,000 and is completely sold out. I hope that this annotated and updated translation will turn out to be comparably useful.

Bussum, August 1987 MICHIEL HAZEWINKEL

I

ICOSAHEDRAL SPACE - The three-dimensional space that is the orbit space of the action of the binary icosahedron group on the three-dimensional sphere. It was discovered by H. Poincaré as an example of a homology sphere of genus 2 in the consideration of Heegaard diagrams (cf. **Heegaard diagram**). The icosahedral space is a p-sheeted covering of S^3 ramified along a torus knot of type (q, r), where p, q, r is any permutation of the numbers 2, 3, 5. The icosahedral space can be defined analytically as the intersection of the surface

$$z_1^2 + z_2^3 + z_3^5 = 0$$

in $\mathbf{C}^2$ with the unit sphere. Finally, the icosahedral space can be identified with the **dodecahedral space**.

A.V. Chernavskiĭ

Editorial comments.

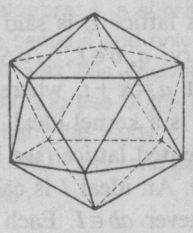
References

[A1] SEIFERT, H. and THRELFALL, W.: *Lehrbuch der Topologie*, Chelsea, reprint, 1947.

AMS 1980 Subject Classification: 57-XX

ICOSAHEDRON - One of the five regular polytopes. An icosahedron has 20 (triangular) faces, 30 edges and 12 vertices (at each of which 5 edges meet). If a is the length of an edge of the icosahedron, then its volume is given by

$$V = \frac{5}{12}a^3(3+\sqrt{5}) \cong 2.1817\,a^3.$$



Editorial comments. The regular polytopes are also called the Platonic solids.

The symmetry group of the icosahedron plays a role in various branches of mathematics, and led F. Klein to his famous book [A2].

References

[A1] COXETER, H.S.M.: *Regular polytopes*, Dover, reprint, 1973.
[A2] KLEIN, F.: *Lectures on the isocahedron and the solution of equations of the fifth degree*, Dover, reprint, 1956 (translated from the German).

AMS 1980 Subject Classification: 51M20, 52A25

IDEAL - A special type of subobject of an algebraic structure. The concept of an ideal first arose in the theory of rings. The name ideal derives from the concept of an **ideal number**.

For an algebra, a ring or a semi-group A, an *ideal* I is a subalgebra, subring or sub-semi-group closed under multiplication by elements of A. Here an ideal is said to be a *left* (or *right*) *ideal* if it is closed under multiplication on the left (or right) by elements of A, that is, if

$$AI = I \quad (\text{or } IA = A),$$

where

$$AI = \{ab : a \in A,\ b \in I\},\quad IA = \{ba : a \in A,\ b \in I\}.$$

An ideal that is simultaneously a left ideal and a right ideal (that is, one that is preserved under multiplication by elements of A) is said to be *two-sided*. These three concepts coincide in the commutative case. Every assertion about left ideals has a corresponding dual assertion about right ideals (subsequent statements will refer only to the 'left case').

Two-sided ideals in rings and algebras play exactly the same role as do normal subgroups (cf. **Normal subgroup**) in groups. For every homomorphism $f : A \to B$, the kernel $\operatorname{Ker} f$ (that is, the set of elements mapped to 0 by f) is an ideal, and conversely every ideal I is the kernel of some homomorphism. Moreover, an ideal I determines a unique **congruence (in algebra)** κ on A of which it is the zero class, and thus determines the image Af of the homomorphism f of which it is the kernel uniquely (up to an isomorphism): Af is isomorphic to the quotient ring or quotient algebra A/κ, denoted also by A/I. Ideals of multi-operator groups have similar properties in relation to homomorphisms. In a

multi-operator Ω-group A an ideal is defined to be a normal subgroup of its additive group satisfying the following property: For every n-ary operator ω, arbitrary elements $b \in I$ and $a_1, \ldots, a_n \in A$, the relation

$$(a_1 \cdots a_n\omega)+(a_1 \cdots a_{i-1}(b+a_i)a_{i+1} \cdots a_n\omega) \in I$$

holds for $i=1, \ldots, n$. (This concept reduces to that of a two-sided ideal for rings and algebras.)

On the other hand, the two-sided ideals of a semi-group do not give a description of all homomorphic images of the semi-group. If a homomorphism f of a semi-group A onto a semi-group B is given, then only in the case where B is a semi-group with zero it is possible to associate with f a two-sided ideal in a natural way, namely $f^{-1}(0)$; however, this association need not determine f uniquely. Nevertheless, if I is an ideal of A, then among the quotient semi-groups of A having the class of I as an element there exists a maximal one, written A/I (and called the *ideal quotient*). The elements of this semi-group are the elements of the set $A \setminus I$ and the ideal I itself, which is the zero in A/I.

For an arbitrary subset $X \subset A$ one can define the *ideal I_X generated by X* as the intersection of all ideals that contain X. The set X is said to be a *basis of the ideal I_X*. Different bases can generate one and the same ideal. An ideal generated by a single element is said to be a **principal ideal**.

The intersection, and for semi-groups also the union, of left (two-sided) ideals is again a left (two-sided) ideal. For rings and algebras, the set-theoretical union of ideals need not be an ideal. Let I_1 and I_2 be left or two-sided ideals in a ring (or algebra) A. The *sum of the ideals* I_1 and I_2 is the ideal $I_1+I_2=\{a+b\colon\ a \in I_1, b \in I_2\}$; it is the smallest ideal of A containing I_1 and I_2. The set of all (left or two-sided) ideals of a ring (or algebra) forms a lattice under the operations of intersection and taking sums. Many classes of rings and algebras are defined by conditions on their ideals or on the lattice of ideals (see **Principal ideal ring**; **Artinian ring**; **Noetherian ring**).

An ideal of the multiplicative semi-group of a ring may or may not be an ideal of the ring. A semi-group A is a group if and only if A has no (left or two-sided) ideal other than A. Thus, the abundance of ideals in a semi-group characterizes the degree to which the semi-group differs from a group.

For a k-algebra A (an algebra over a field k), an ideal of the ring A need not be an ideal of the algebra A. For example, if A is a k-algebra with zero multiplication, the set of ideals of the ring A is the set of subgroups of the additive group of A, while the set of ideals of the algebra A is the set of all subspaces of the vector k-space A. However, when A is an algebra with identity, these concepts of an ideal coincide. Therefore many results have identical statements for rings and algebras.

A ring not having any two-sided ideal is said to be a **simple ring**. A ring without proper one-sided ideals is a **skew-field**. Left ideals of a ring A may also be defined as submodules of the left A-module A. Some properties of rings remain unchanged when right ideals are substituted for left ideals. For example, the **Jacobson radical** defined in terms of left ideals is the same as the Jacobson radical defined in terms of right ideals. On the other hand, a left Noetherian ring can fail to be right Noetherian.

The study of ideals in commutative rings is an important part of commutative algebra. With every commutative ring with identity one can associate the topological space $\operatorname{Spec} A$ whose elements are the proper prime ideals of A. There is a one-to-one correspondence between the set of all radicals of ideals of A and the set of closed subspaces of $\operatorname{Spec} A$.

The concept of an ideal of a field occurs in commutative algebra, more precisely, that of an ideal of a field relative to a ring. Here A is a commutative ring with identity and without zero divisors, and Q is the field of fractions of A. An *ideal of the field Q* is a non-zero subset $I \subset Q$ that is a subgroup of the additive group of Q closed under multiplication by elements of A (that is, $ab \in I$ whenever $a \in A$ and $b \in I$) and such that there exists an element $q \in Q$ such that $qI \subset A$. An ideal is said to be an *integral ideal* if it is contained in A (and then it is an ordinary ideal of A); otherwise it is a **fractional ideal**.

An *ideal of a lattice* is a non-empty subset I of a lattice such that: 1) if $a, b \in I$, then $a+b \in I$; and 2) if $c \leqslant a \in I$, then $c \in I$. A *dual ideal* (or a *filter*) of a lattice is defined in the dual manner ($a, b \in J$ implies $ab \in J$; $c \geqslant a \in J$ implies $c \in J$). The ideals of a lattice also form a lattice under inclusion. A maximal element of the set of all proper ideals of a lattice is called a *maximal ideal*. If f is a homomorphism of a lattice onto a partially ordered set with a zero, then the complete inverse image of the zero is an ideal. It is called the *kernel ideal* of f. An ideal S of a lattice L is said to be a *standard ideal* if for arbitrary $a, b \in L$, $s \in S$, the inequality $a<b+s$ implies that $a=x+t$, where $x \leqslant b$ and $t \in S$. Every standard ideal is a kernel ideal. A kernel ideal of a relatively complemented lattice (see **Lattice with complements**) is standard. An ideal I is called a *prime ideal* if $a \in I$ or $b \in I$ whenever $ab \in I$. Each of the following conditions is equivalent to primality for an ideal I of a lattice L: a) the complement $A \setminus I$ is a filter; or b) I is the complete inverse image of zero under some homomorphism of L onto a two-element lattice. Every maximal ideal of a distributive lattice is prime.

The concept of an *ideal in a partially ordered set* is not in full agreement with the preceding definition. In fact, instead of 1), a stronger condition is required to hold: For every subset of the ideal, the supremum (join) of the set (if it exists) is also in I.

An *ideal object* A of a category with null morphisms is a **subobject** (U, μ) of A such that $\mu = \ker \alpha$ for some morphism $\alpha: A \to B$. This ideal can be identified with the set of all monomorphisms that are kernels of some morphism (see also **Normal monomorphism**). The concept of a co-ideal object of a category is defined in the dual way. The concept of an ideal for Ω-groups is a special case of that of an ideal object in a category.

A *left ideal of a category* $\mathfrak{K}$ is a class of morphisms containing, with every morphism ϕ of it, all products $\alpha\phi$ with $\alpha \in \mathfrak{K}$, if these are defined in $\mathfrak{K}$. *Right ideals of a category* are defined in the dual way. A *two-sided ideal* is a class of morphisms that is both a left ideal and a right ideal.

References

[1] BOREVICH, Z.I. and SHAFAREVICH, I.R.: *Number theory*, Acad. Press, 1966 (translated from the Russian).

[2] BOURBAKI, N.: *Elements of mathematics. Commutative algebra*, Addison-Wesley, 1972 (translated from the French).

[3] WAERDEN, B.L. VAN DER: *Algebra*, 1-2, Springer, 1967-1971 (translated from the German).

[4] CLIFFORD, A.H. and PRESTON, G.B.: *The algebraic theory of semigroups*, 1-2, Amer. Math. Soc., 1961-1967.

[5] KUROSH, A.G.: *Lectures on general algebra*, Chelsea, 1963 (translated from the Russian).

[6] LYAPIN, E.S.: *Semigroups*, Amer. Math. Soc., 1974 (translated from the Russian).

[7] SKORNYAKOV, L.A.: *Elements of lattice theory*, Hindushtan Publ. Comp., 1977 (translated from the Russian).

[8] TSALENKO, M.SH. and SHUL'GEĬFER, E.G.: *Fundamentals of category theory*, Moscow, 1974 (in Russian).

L.V. Kuz'min
T.S. Fofanova
M.Sh. Tsalenko

Editorial comments. There is some disagreement about the correct definition of an ideal I in a partially ordered set A. Instead of the definition given above, some authors would allow I to be an arbitrary *lower set* (if $a \leq b \in I$, then $a \in I$); others require additionally that I be *directed* (if $a \in I$ and $b \in I$, then there exists a $c \in I$ with $a \leq c$ and $b \leq c$). The latter definition has the advantage of agreeing with the usual one in the case when A is a lattice (or a join semi-lattice).

For a **Boolean algebra** A, a subset I of A is an ideal in the lattice-theoretic sense if and only if it is an ideal of the **Boolean ring** A. It was this equivalence which led M.H. Stone [A1] to extend the use of the term 'ideal' from rings to lattices. Since then, the study of ideals has played an important role in lattice theory, and particularly in the theory of distributive lattices.

References

[A1] STONE, M.H.: 'Topological representation of distributive lattices and Brouwerian logics', *Časopis Pešt. Mat. Fys.* 67 (1937), 1-25.

[A2] JOHNSTONE, P.T.: *Stone spaces*, Cambridge Univ. Press, 1982.

[A3] JACOBSON, N.: *Structure of rings*, Amer. Math. Soc., 1956.

[A4] JACOBSON, N.: *The theory of rings*, Amer. Math. Soc., 1943.

AMS 1980 Subject Classification: 06B10, 16A66, 13A15, 20M12

IDEAL NUMBER - An element of the semi-group D of divisors (cf. **Divisor**) of the ring A of integers of an algebraic number field. The semi-group D is a free commutative semi-group with identity; its free generators are called *prime ideal numbers*. In modern terminology, ideal numbers are known as *integral divisors* of A. They can be identified in a natural way with the ideals (cf. **Ideal**) of A.

Ideal numbers were introduced in connection with the absence of uniqueness of factorization into prime factors in the ring of integers of an algebraic number field. For every $a \in A$, the factorization of the corresponding divisor $\phi(a)$ into the product of prime ideal numbers can be looked at as a substitute for unique factorization into prime factors if factorization in A is not unique.

For example, the ring A of integers of the field $\mathbf{Q}(\sqrt{-5})$ consists of the numbers $a + b\sqrt{-5}$ with integers a and b. In this ring, the number 6 has two different factorizations:

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}),$$

where the numbers 2, 3, $1 - \sqrt{-5}$, and $1 + \sqrt{-5}$ are pairwise non-associated irreducible (prime) elements of A; thus factorization into irreducible factors in A is not unique. However, in D the elements $\phi(2)$, $\phi(3)$, $\phi(1 + \sqrt{-5})$, and $\phi(1 - \sqrt{-5})$ are not irreducible; in fact, $\phi(2) = \mathfrak{p}_1^2$, $\phi(3) = \mathfrak{p}_2\mathfrak{p}_3$, $\phi(1 - \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2$, $\phi(1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$, where $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are prime ideal numbers in D. Thus, the two factorizations of 6 into irreducible factors in A give rise to one and the same factorization $\phi(6) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ in D.

The concept of an ideal number was introduced by E. Kummer in connection with his investigation of the arithmetic of cyclotomic fields (see [1], [2]). Let $K = \mathbf{Q}(\zeta)$ be the p-th **cyclotomic field** for some prime number p and let $A = \mathbf{Z}[\zeta]$ be the ring of integers of K. The ideal numbers for A were defined to be the products of prime ideal numbers, and the latter as the 'ideal' prime divisors of natural prime numbers. To construct all the prime ideal numbers contained in a given natural prime number q, Kummer's theorem (cf. **Kummer theorem**) was used. Kummer used the fact that A has basis $1, \zeta, \ldots, \zeta^{p-2}$ over $\mathbf{Z}$ to investigate the factorization of the p-th cyclotomic polynomial $F_p(X)$ in the ring $(\mathbf{Z}/q\mathbf{Z})[X]$. The ideal numbers dividing q are in one-to-one correspondence with the irreducible factors of $F_p(X)$ in $(\mathbf{Z}/q\mathbf{Z})[X]$ (the case $p = q$ required a somewhat different approach). A special method was

applied to determine the exponent with which a given prime ideal number occurs in a given $a \in A$. He developed a similar method for creating a theory of divisibility in fields of the form $\mathbf{Q}(\zeta, m^{1/p})$, where $m \in \mathbf{Q}(\zeta)$.

The extension of the theory of ideal numbers to the case of arbitrary algebraic fields is due mainly to L. Kronecker and R. Dedekind. A division of the theory of ideal numbers into the theory of divisors (the approach of Kronecker) and the theory of ideals begins to appear in their papers. Dedekind associated with every ideal number a unique *ideal* of the ring A, which was defined by him as the subset of A consisting of 0 together with all a that are divisible by this ideal number. If $a_1, \ldots, a_n$ are generators for the ideal I, then the ideal number corresponding to I is the greatest common divisor of the ideal numbers $\phi(a_1), \ldots, \phi(a_n)$.

Later, the concept of an ideal was extended to the case of an arbitrary ring A; rings for which the concepts of an ideal and a divisor coincide are now called Dedekind rings (cf. **Dedekind ring**).

References

[1A] KUMMER, E.: 'Zur Theorie der complexen Zahlen', *J. Reine Angew. Math.* **35** (1847), 319-326.

[1B] KUMMER, E.: 'Ueber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren', *J. Reine Angew. Math.* **35** (1847), 327-367.

[2] KUMMER, E.: 'Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers', *J. Math. Pures Appl.* **16** (1851), 377-498.

[3] EDWARDS, H.M.: 'The background of Kummer's proof of Fermat's last theorem for regular primes', *Arch. Hist. Exact Sci.*, no. 3 (1975), 219-236.

[4] BOURBAKI, N.: *Elements of mathematics. Commutative algebra*, Addison-Wesley, 1972 (translated from the French).

[5] BOURBAKI, N.: *Outline of the history of mathematics*, Springer, to appear (translated from the French).

L.V. Kuz'min

AMS 1980 Subject Classification: 13F05, 13F15, 12-XX

IDEAL POINT, *improper point, point at infinity, infinitely-distant point* - A point that completes the plane in order to describe certain geometrical relations and systems. For example, an **inversion** is a one-to-one mapping of the Euclidean plane completed by an ideal point; completion of the affine plane by ideal points leads to the concept of a **projective plane**. See also **Infinitely-distant elements.**

A.B. Ivanov

AMS 1980 Subject Classification: 51NXX

IDEAL SERIES *of a semi-group* S - A sequence of sub-semi-groups

$$A_1 \subset A_2 \subset \cdots \subset A_m = S \qquad (*)$$

such that A_i is a (two-sided) ideal of A_{i+1}, $i = 1, \ldots, m-1$. The sub-semi-group A_1 and the Rees factor semi-groups A_{i+1}/A_i (see **Semi-group**) are called the *factors* of the series (*). Two ideal series are said to be *isomorphic* if a one-to-one correspondence can be established between the factors such that corresponding factors are isomorphic. An ideal series

$$B_1 \subset B_2 \subset \cdots \subset B_n = S$$

is said to be a *refinement* of (*) if every A_i occurs among the B_j. An ideal series is a *composition series* if it does not have proper refinements. Any two ideal series of a semi-group have isomorphic refinements; in particular, in a semi-group having a composition series all such series are isomorphic (the analogue of the theorems of Schreier and Jordan–Hölder for normal series in groups, see [1], [2]). An ideal series is a *chief series* if its terms are ideals in the whole semi-group and if it has no proper refinements consisting of ideals of the semi-group. If a semi-group has a composition series, then it also has a chief series; the converse is false. In a semi-group with a chief series, its factors are isomorphic to the chief factors (cf. **Principal factor**) of S.

As for normal series in groups, the concepts mentioned above (as well as their properties) naturally generalize to the case of infinite systems of nested sub-semi-groups. In particular, an *ascending ideal series* in a semi-group S is a totally ordered sequence

$$A_1 \subset \cdots \subset A_\alpha \subset A_{\alpha+1} \subset \cdots \subset A_\beta = S,$$

where at limit points there stand the unions of the preceding members, and A_α is an ideal of $A_{\alpha+1}$ for all $\alpha < \beta$.

References

[1] KUROSH, A.G.: *The theory of groups*, 1-2, Chelsea, 1955-1956 (translated from the Russian).

[2] CLIFFORD, A.H. and PRESTON, G.B.: *The algebraic theory of semigroups*, 1-2, Amer. Math. Soc., 1961-1967.

L.N. Shevrin

AMS 1980 Subject Classification: 20M12

IDÈLE - An invertible element of the ring of adèles (cf. **Adèle**). The set of all idèles forms a group under multiplication, called the *idèle group*. The elements of the idèle group of the field of rational numbers are sequences of the form

$$a = (a_\infty, a_2, \ldots, a_p, \ldots),$$

where a_∞ is a non-zero real number, a_p is a non-zero **p-adic number**, $p = 2, 3, 5, 7, \ldots$, and $|a_p| = 1$ for all but finitely many p (here $|x|_p$ is the p-adic norm). A sequence of idèles

$$a^{(n)} = (a_\infty^{(n)}, a_2^{(n)}, \ldots, a_i^{(n)}, \ldots)$$

is said to converge to an idèle a if it converges to a componentwise and if there exists an N such that $|a_p^{-1} a_p^{(n)}|_p = 1$ for $n > N$ and all p. The idèle group is a

此为试读，需要完整PDF请访问：www.ertongbook.com

locally compact topological group in this topology. The idèle group of an arbitrary number field is constructed in an analogous way.

The multiplicative group of the field of rational numbers is isomorphically imbedded in the idèle group of this field. Every rational number $r \neq 0$ is associated with the sequence

$$(r, r, \ldots, r, \ldots),$$

which is an idèle. Such an idèle is said to be a *principal idèle*. The subgroup consisting of all principal idèles is a discrete subgroup of the idèle group.

The concepts of an idèle and an adèle were introduced by C. Chevalley in 1936 for the purposes of algebraic number theory. The new language proved useful in the study of arithmetic aspects of the theory of algebraic groups. To those ends, A. Weil generalized the definitions of an adèle and an idèle to the case of an arbitrary linear algebraic group defined over a number field.

References

[1] WEIL, A.: *Basic number theory*, Springer, 1973.

[2] CASSELS, J.W.S. and FRÖHLICH, A. (EDS.): *Algebraic number theory*, Acad. Press, 1986.

V.L. Popov

Editorial comments. Let I be an index set and for each $i \in I$ let there be given a locally compact topological ring or group G_i and an open compact subring or subgroup B_i. The *restricted direct product* $G = \prod' G_i$ of the G_i with respect to the B_i consists of all families $(g_i)_{i \in I}$ such that $g_i \in B_i$ for all but finitely many i. G becomes a locally compact group (ring) by taking as a basis of open neighbourhoods of the identity (zero) the sets $\prod_i U_i$ with U_i open in G_i for all i and $U_i = B_i$ for all but finitely many i. For each finite set $S \subset I$ let $G_S = \prod_{i \in S} G_i \times \prod_{i \notin S} B_i$. Then G is the union (direct limit) of the G_S.

Now let k be a number field (or, more generally, a global field). Let I be the set of all prime divisors of k (both finite and infinite ones). For each $\mathfrak{p} \in I$ let $k_{\mathfrak{p}}$ be the completion of k with respect to the norm of $\mathfrak{p}$, and let $A_{\mathfrak{p}}$ be the ring of integers of $k_{\mathfrak{p}}$. (Set $A_{\mathfrak{p}} = k_{\mathfrak{p}}$ if $\mathfrak{p}$ is infinite.) Then the restricted product of the $k_{\mathfrak{p}}$ with respect to the $A_{\mathfrak{p}}$ is the *ring of adèles* $\mathbf{A}_k$ of k.

Now for each $\mathfrak{p} \in I$ let $k_{\mathfrak{p}}^*$ be the group of non-zero elements of $k_{\mathfrak{p}}$ and let $U_{\mathfrak{p}}$ be the group of units of $k_{\mathfrak{p}}^*$ (if $\mathfrak{p}$ is infinite take $U_{\mathfrak{p}} = k_{\mathfrak{p}}^*$). The restricted product of the $k_{\mathfrak{p}}^*$ with respect to the $U_{\mathfrak{p}}$ is the *group of idèles* of k. As a set the group of idèles $\mathbf{I}_k$ is the set of invertible elements of $\mathbf{A}_k$. But the topology on $\mathbf{I}_k$ is stronger than that induced by $\mathbf{A}_k$.

The quotient of $\mathbf{I}_k$ by the diagonal subgroup $k^* = \{(\alpha)_{i \in I}\}$ of principal idèles is called the *idèle class group*; it is important in **class field theory**.

The name idèle derives from *ideal element*. This got abbreviated id.el., which, pronounced in French, gave rise to idèle.

AMS 1980 Subject Classification: 12A85, 22E55, 20GXX

IDEMPOTENT, *idempotent element* - An element e of a ring, semi-group or groupoid equal to its own square: $e^2 = e$. An idempotent e is said to contain an idempotent f (denoted by $e \geqslant f$) if $ef = e = fe$. For associative rings and semi-groups, the relation $\geqslant$ is a partial order on the set E of idempotent elements, called the *natural partial order* on E. Two idempotents u and v of a ring are said to be orthogonal if $uv = 0 = vu$. With every idempotent of a ring (and also with every system of orthogonal idempotents) there is associated the so-called **Peirce decomposition** of the ring. For an n-ary algebraic relation ω, an element e is said to be an idempotent if $(e \cdots e)\omega = e$, where e occurs n times between the brackets.

O.A. Ivanova

Editorial comments. An algebraic operation ω is sometimes said to be *idempotent* if every element of the set on which it acts is idempotent in the sense defined above. Such operations are also called *affine operations*; the latter name is preferable because an affine unary operation is not the same thing as an idempotent element of the semi-group of unary operations. In the theory of R-modules, the affine operations are those of the form

$$(x_1, \ldots, x_n) \mapsto \sum_{i=1}^{n} r_i x_i$$

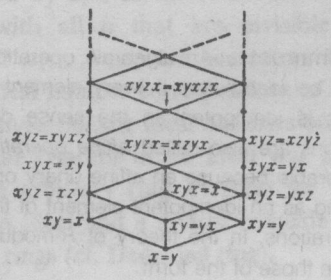
with $\sum_{i=1}^{n} r_i = 1$.

AMS 1980 Subject Classification: 16A32, 08A40

IDEMPOTENTS, SEMI-GROUP OF, *idempotent semi-group* - A semi-group each element of which is an **idempotent**. An idempotent semi-group is also called a *band* (this is consistent with the concept of a **band of semi-groups**: An idempotent semi-group is a band of one-element semi-groups). A commutative idempotent semi-group is called a *semi-lattice*; this term is consistent with its use in the theory of partially ordered sets: If a commutative idempotent semi-group S is considered with respect to its natural partial order, then $\overline{ab}$ is the greatest lower bound of the elements $a, b \in S$. Every semi-lattice is a subdirect product of two-element semi-lattices. A semi-group S is said to be *singular* if S satisfies one of the identities $xy = x$, $xy = y$; in the first case S is said to be *left-singular*, or to be a *semi-group of left zeros*, in the second case it is called *right-singular*, or a *semi-group of right zeros*. A semi-group is said to be *rectangular* if it satisfies the identity $xyx = x$ (this term is sometimes used in a wider sense, see [1]). The following conditions are equivalent for a semi-group S: 1) S is rectangular; 2) S is an ideally-simple idempotent semi-group (see **Simple semi-group**); 3) S is a **completely-simple semi-group** of idempotents; and 4) S is isomorphic to a direct product $L \times R$, where L is a left-singular and R is a right-singular semi-group. Every idempotent semi-group is a **Clifford semi-group** and

splits into a semi-lattice of rectangular semi-groups (see **Band of semi-groups**). This splitting is the starting point for the study of many properties of idempotent semi-groups. Every idempotent semi-group is locally finite.

Idempotent semi-groups have been studied from various points of view, including that of the theory of varieties. The lattice of all subvarieties of the variety $\mathfrak{V}$ of all idempotent semi-groups has been described completely in [4] - [6]; it is countable and distributive, and every subvariety of $\mathfrak{V}$ is defined by one identity. See the figure for the diagram of this lattice; also indicated in this figure are the identities giving in $\mathfrak{V}$ the varieties on some of the lower 'floors'.



References

[1] CLIFFORD, A.H. and PRESTON, G.B.: *The algebraic theory of semigroups*, 1-2, Amer. Math. Soc., 1961-1967.

[2] MCLEAN, A.D.: 'Idempotent semigroups', *Amer. Math. Monthly* **61**, no. 2 (1954), 110-113.

[3] KIMURA, N.: 'The structure of idempotent semigroups', *Pacific J. Math.* **8** (1958), 257-275.

[4] BIRYUKOV, A.P.: 'Varieties of idempotent semigroups', *Algebra and Logic* **9**, no. 3 (1970), 153-164. (*Algebra i Logika* **9**, no. 3 (1970), 255-273)

[5] GERHARD, J.: 'The lattice of equational classes of idempotent semigroups', *J. of Algebra* **15**, no. 2 (1970), 195-224.

[6] FENNEMORE, C.: 'All varieties of bands I, II', *Math. Nachr.* **48**, no. 1-6 (1971), 237-252; 253-262.

L.N. Shevrin

AMS 1980 Subject Classification: 20M07

IDENTICAL TRUTH, *logical truth, tautology* - A property of formulas in the language of predicate calculus, meaning that the formulas are true in all interpretations and for all admissible values of their free variables. For example, for a formula containing only one 2-place predicate symbol ρ and variables of one sort (that is, variables which are interpreted in the same domain of variation), any pair (M, R), where M is an arbitrary non-empty set and $R \subseteq M \times M$ is an arbitrary binary relation on M, is an **interpretation**. Arbitrary elements of M are admissible values for the free variables. Truth of a formula $\phi(x_1, \ldots, x_n)$ at values $a_1, \ldots, a_n$ $(n \geq 0)$ of the variables $x_1, \ldots, x_n$, respectively, is defined by induction on the structure of the formula, as follows. (Here the free variables run through the set M and the predicate symbol ρ denotes the relation R.)

Suppose that a formula ϕ is given, as well as a finite sequence $\bar{x} = (x_1, \ldots, x_n)$ of variables containing all the free variables of ϕ; let $|\phi; \bar{x}|$ denote the set of all finite sequences $(a_1, \ldots, a_n)$ of elements of M at which ϕ is true in (M, R). A set of the form $|\phi; \bar{x}|$ can be constructed inductively as follows (here it is assumed that the logical symbols in ϕ are $\wedge$, $\neg$, $\exists$):

$$|\phi; \bar{x}| = \{(a_1, \ldots, a_n): (a_i, a_j) \in R\}$$

if ϕ has the form $\rho(x_i, x_j)$;

$$|\phi_1 \wedge \phi_2; \bar{x}| = |\phi_1; \bar{x}| \cap |\phi_2; \bar{x}|;$$

$$|\neg\phi; \bar{x}| = M^n \setminus |\phi; \bar{x}|;$$

$$|\exists y\, \phi; \bar{x}| = \mathrm{pr}_{n+1} |\phi; \bar{x}y|,$$

where $\cap$, $\setminus$, pr_{n+1} denote, respectively, intersection, difference and projection along the $(n+1)$-st coordinate (that is, the image with respect to the mapping $(a_1, \ldots, a_n, a_{n+1}) \mapsto (a_1, \ldots, a_n)$) of sets.

Identical truth for a formula ϕ with free variables $x_1, \ldots, x_n$ then means that for any interpretation (M, R), every sequence $(a_1, \ldots, a_n)$ of elements of M belongs to the set $|\phi; x_1, \ldots, x_n|$. For $n = 0$ the set $|\phi; \bar{x}|$ is either empty or a singleton. For example, the formula

$$\exists y\, \forall x\, \rho(x, y) \supset \forall x\, \exists y\, \rho(x, y)$$

is an identical truth. The converse implication is not an identically-true formula.

In the case where an interpretation is fixed, a formula is sometimes called identically true if it is true in the given interpretation for any values of its free variables.

References

[1] KLEENE, S.C.: *Introduction to metamathematics*, North-Holland, 1951.

[2] SHOENFIELD, J.R.: *Mathematical logic*, Addison-Wesley, 1967.

V.N. Grishin

AMS 1980 Subject Classification: 03A05

IDENTITY PROBLEM - The **algorithmic problem** of recognizing the equality (identity) of words in an algebraic system (**group**; **semi-group**, and others) with given generators and defining relations.

Editorial comments. This problem is better known as the *word problem* or *word identity problem*.

AMS 1980 Subject Classification: 08A50, 03D40, 20F10

ILL-POSED PROBLEMS, *incorrectly-posed problems, improperly-posed problems* - Problems for which at least one of the conditions below, which characterize *well-posed problems*, is violated. The problem of determining a solution $z = R(u)$ in a metric space Z (with metric $\rho_Z(\,,\,)$) from 'initial data' u in a metric space U (with metric $\rho_U(\,,\,)$) is said to be *well-posed* on the pair of spaces (Z, U) if: a) for every $u \in U$ there exists a solution $z \in Z$; b) the solution is uniquely determined; and

c) the problem is stable on the spaces (Z, U), i.e.: For every $\epsilon>0$ there is a $\delta(\epsilon)>0$ such that for any $u_1, u_2 \in U$ it follows from $\rho_U(u_1, u_2)\leq\delta(\epsilon)$ that $\rho_Z(z_1, z_2)\leq\epsilon$, where $z_1=R(u_1)$ and $z_2=R(u_2)$.

The concept of a well-posed problem is due to J. Hadamard (1923), who took the point of view that every mathematical problem corresponding to some physical or technological problem must be well-posed. In fact, what physical interpretation can a solution have if an arbitrary small change in the data can lead to large changes in the solution? Moreover, it would be difficult to apply approximation methods to such problems. This put the expediency of studying ill-posed problems in doubt.

However, this point of view, which is natural when applied to certain time-depended phenomena, cannot be extended to all problems. The following problems are unstable in the metric of Z, and therefore ill-posed: the solution of integral equations of the first kind; differentiation of functions known only approximately; numerical summation of Fourier series when their coefficients are known approximately in the metric of l_2; the Cauchy problem for the Laplace equation; the problem of analytic continuation of functions; and the inverse problem in gravimetry. Other ill-posed problems are the solution of systems of linear algebraic equations when the system is ill-conditioned; the minimization of functionals having non-convergent minimizing sequences; various problems in linear programming and optimal control; design of optimal systems and optimization of constructions (synthesis problems for antennas and other physical systems); and various other control problems described by differential equations (in particular, differential games). Various physical and technological questions lead to the problems listed (see [7]).

A broad class of so-called inverse problems that arise in physics, technology and other branches of science, in particular, problems of data processing of physical experiments, belongs to the class of ill-posed problems. Let z be a characteristic quantity of the phenomenon (or object) to be studied. In a physical experiment the quantity z is frequently inaccessible to direct measurement, but what is measured is a certain transform $Az=u$ (also called outcome). For the interpretation of the results it is necessary to determine z from u, that is, to solve the equation

$$Az = u. \tag{1}$$

Problems of solving an equation (1) are often called *pattern recognition problems*. Problems leading to the minimization of functionals (design of antennas and other systems or constructions, problems of optimal control and many others) are also called *synthesis problems*.

Suppose that in a mathematical model for some physical experiments the object to be studied (the phenomenon) is characterized by an element z (a function, a vector) belonging to a set Z of possible solutions in a metric space $\tilde{Z}$. Suppose that z_T is inaccessible to direct measurement and that what is measured is a transform, $Az_T=u_T$, $u_T \in AZ$, where AZ is the image of Z under the operator A. Evidently, $z_T=A^{-1}u_T$, where A^{-1} is the operator inverse to A. Since u_T is obtained by measurement, it is known only approximately. Let $\tilde{u}$ be this approximate value. Under these conditions the question can only be that of finding a 'solution' of the equation

$$Az = \tilde{u}, \tag{2}$$

approximating z_T.

In many cases the operator A is such that its inverse A^{-1} is not continuous, for example, when A is a completely-continuous operator in a Hilbert space, in particular an integral operator of the form

$$\int_a^b K(x, s)z(s)\,ds.$$

Under these conditions one cannot take, following classical ideas, an exact solution of (2), that is, the element $z=A^{-1}\tilde{u}$, as an approximate 'solution' to z_T. In fact: a) such a solution need not exist on Z, since $\tilde{u}$ need not belong to AZ; and b) such a solution, if it exists, need not be stable under small changes of $\tilde{u}$ (due to the fact that A^{-1} is not continuous) and, consequently, need not have a physical interpretation. The problem (2) then is ill-posed.

Numerical methods for solving ill-posed problems. For ill-posed problems of the form (1) the question arises: What is meant by an approximate solution? Clearly, it should be so defined that it is stable under small changes of the original information. A second question is: What algorithms are there for the construction of such solutions? Answers to these basic questions were given by A.N. Tikhonov (see [1], [2]).

The *selection method*. In some cases an approximate solution of (1) can be found by the selection method. It consists of the following: From the class of possible solutions $M \subset Z$ one selects an element $\tilde{z}$ for which $A\tilde{z}$ approximates the right-hand side of (1) with required accuracy. For the desired approximate solution one takes the element $\tilde{z}$. The question arises: When is this method applicable, that is, when does

$$\rho_U(A\tilde{z}, Az_T) \leq \delta$$

imply that

$$\rho_Z(z, z_T) \leq \epsilon(\delta),$$

where $\epsilon(\delta)\to 0$ as $\delta\to 0$? This holds under the conditions that the solution of (1) is unique and that M is compact (see [3]). On the basis of these arguments one has for-

mulated the concept (or the condition) of being *Tikhonov well-posed*, also called *conditionally well-posed* (see [4]). As applied to (1), a problem is said to be *conditionally well-posed* if it is known that for the exact value of the right-hand side $u=u_T$ there exists a unique solution z_T of (1) belonging to a given compact set M. In this case A^{-1} is continuous on M, and if instead of u_T an element u_δ is known such that $\rho_U(u_\delta, u_T)\leqslant\delta$ and $u_\delta\in AM$, then as an approximate solution of (1) with right-hand side $u=u_\delta$ one can take $z_\delta=A^{-1}u_\delta$. As $\delta\to 0$, z_δ tends to z_T.

In many cases the approximately known right-hand side $\tilde{u}$ does not belong to AM. Under these conditions equation (1) does not have a classical solution. As an approximate solution one takes then a generalized solution, a so-called quasi-solution (see [5]). A *quasi-solution* of (1) on M is an element $\tilde{z}\in M$ that minimizes for a given $\tilde{u}$ the functional $\rho_U(Az, \tilde{u})$ on M (see [6]). If M is compact, then a quasi-solution exist for any $\tilde{u}\in U$, and if in addition $\tilde{u}\in AM$, then a quasi-solution $\tilde{z}$ coincides with the classical (exact) solution of (1). The existence of quasi-solutions is guaranteed only when the set M of possible solutions is compact.

The *regularization method.* For a number of applied problems leading to (1) a typical situation is that the set Z of possible solutions is not compact, the operator A^{-1} is not continuous on AZ, and changes of the right-hand side of (1) connected with the approximate character can cause the solution to go out of AZ. Such problems are called *essentially ill-posed.* An approach has been worked out to solve ill-posed problems that makes it possible to construct numerical methods that approximate solutions of essentially ill-posed problems of the form (1) which are stable under small changes of the data. In this context, both the right-hand side u and the operator A should be among the data.

In what follows, for simplicity of exposition it is assumed that the operator A is known exactly. At the basis of the approach lies the concept of a regularizing operator (see [2], [7]). An operator $R(u, \delta)$ from U to Z is said to be a *regularizing operator* for the equation $Az=u$ (in a neighbourhood of $u=u_T$) if it has the following properties: 1) there exists a $\delta_1>0$ such that the operator $R(u, \delta)$ is defined for every δ, $0\leqslant\delta\leqslant\delta_1$, and for any $u_\delta\in U$ such that $\rho_U(u_\delta, u_T)\leqslant\delta$; and 2) for every $\epsilon>0$ there exists a $\delta_0=\delta_0(\epsilon, u_T)\leqslant\delta_1$ such that $\rho_U(u_\delta, u_T)\leqslant\delta\leqslant\delta_0$ implies $\rho_Z(z_\delta, z_T)\leqslant\epsilon$, where $z_\delta=R(u_\delta, \delta)$.

Sometimes it is convenient to use another definition of a regularizing operator, comprising the previous one. An operator $R(u, \alpha)$ from U to Z, depending on a parameter α, is said to be a *regularizing operator* (or *regularization operator*) for the equation $Az=u$ (in a neighbourhood of $u=u_T$) if it has the following properties: 1) there exists a $\delta_1>0$ such that $R(u, \alpha)$ is defined for every α and any $u_\delta\in U$ for which $\rho_U(u_\delta, u_T)<\delta\leqslant\delta_1$; and 2) there exists a function $\alpha=\alpha(\delta)$ of δ such that for any $\epsilon>0$ there is a $\delta(\epsilon)\leqslant\delta_1$ such that if $u_\delta\in U$ and $\rho_U(u_\delta, u_T)\leqslant\delta(\epsilon)$, then $\rho_z(z_\delta, z_T)<\epsilon$, where $z_\delta=R(u_\delta, \alpha(\delta))$. In this definition it is not assumed that the operator $R(u, \alpha(\delta))$ is globally single-valued.

If $\rho_U(u_\delta, u_T)\leqslant\delta$, then as an approximate solution of (1) with an approximately known right-hand side U_δ one can take the element $z_\alpha=R(u_\delta, \alpha)$ obtained by means of the regularizing operator $R(u, \alpha)$, where $\alpha=\alpha(\delta)$ is compatible with the error of the initial data u_δ (see [1], [2], [7]). This is said to be a *regularized solution* of (1). The numerical parameter α is called the *regularization parameter.* As $\delta\to 0$, the regularized approximate solution $z_\alpha(\delta)=R(u_\delta, \alpha(\delta))$ tends (in the metric of Z) to the exact solution z_T.

Thus, the task of finding approximate solutions of (1) that are stable under small changes of the right-hand side reduces to: a) finding a regularizing operator; and b) determining the regularization parameter α from additional information on the problem, for example, the size of the error with which the right-hand side u is given.

The *construction of regularizing operators.* It is assumed that the equation $Az=u_T$ has a unique solution z_T. Suppose that instead of $Az=u_T$ the equation $Az=u_\delta$ is solved and that $\rho_U(u_\delta, u_T)\leqslant\delta$. Since $\rho_U(Az_T, u_\delta)\leqslant\delta$, the approximate solution of $Az=u_\delta$ is looked for in the class Z_δ of elements z_δ such that $\rho_U(Az, u_\delta)\leqslant\delta$. This Z_δ is the set of possible solutions. As an approximate solution one cannot take an arbitrary element z_δ from Z_δ, since such a 'solution' is not unique and is, generally speaking, not continuous in δ. As a selection principle for the possible solutions ensuring that one obtains an element (or elements) from Z_δ depending continuously on δ and tending to z_T as $\delta\to 0$, one uses the so-called *variational principle* (see [1]). Let $\Omega[z]$ be a continuous non-negative functional defined on a subset F_1 of Z that is everywhere-dense in Z and is such that: a) $z_1\in F_1$; and b) for every $d>0$ the set of elements z in F_1 for which $\Omega[z]\leqslant d$, is compact in F_1. Functionals having these properties are said to be *stabilizing functionals* for problem (1). Let $\Omega[z]$ be a stabilizing functional defined on a subset F_1 of Z. (F_1 can be the whole of Z.) Among the elements of $F_{1,\delta}=F_1\cap Z_\delta$ one looks for one (or several) that minimize(s) $\Omega[z]$ on $F_{1,\delta}$. The existence of such an element z_δ can be proved (see [7]). It can be regarded as the result of applying a certain operator $R_1(u_\delta, d)$ to the right-hand side of the equation $Az=u_\delta$, that is, $z_\delta=R_1(u_\delta, d)$. Then $R_1(u, \delta)$ is a regularizing operator for equation (1). In practice the search for z_δ can be

carried out in the following manner: under mild additional restrictions on $\Omega[z]$ (quasi-monotonicity of $\Omega[z]$, see [7]) it can be proved that $\inf \Omega[z]$ is attained on elements z_δ for which $\rho_U(Az_\delta, u_\delta)=\delta$. An element z_δ is a solution to the problem of minimizing $\Omega[z]$ given $\rho_U(Az, u_\delta)=\delta$, that is, a solution of a problem of conditional extrema, which can be solved using Lagrange's multiplier method and minimization of the functional

$$M^\alpha[z, u_\delta] = \rho_U^2(Az, u_\delta)+\alpha\Omega[z].$$

For any $\alpha>0$ one can prove that there is an element z_α minimizing $M^\alpha[z, u_\delta]$. The parameter α is determined from the condition $\rho_U(Az_\alpha, u_\delta)=\delta$. If there is an α for which $\rho_U(Az_\alpha, u_\delta)=\delta$, then the original variational problem is equivalent to that of minimizing $M^\alpha[z, u_\delta]$, which can be solved by various methods on a computer (for example, by solving the corresponding Euler equation for $M^\alpha[z, u_\delta]$). The element z_α minimizing $M^\alpha[z, u_\delta]$ can be regarded as the result of applying to the right-hand side of the equation $Az=u_\delta$ a certain operator $R_2(u_\delta, \alpha)$ depending on α, that is, $z_\alpha=R_2(u_\delta, \alpha)$ in which α is determined by the discrepancy relation $\rho_U(Az_\alpha, u_\delta)=\delta$. Then $R_2[u, \alpha]$ is a regularizing operator for (1). Equivalence of the original variational problem with that of finding the minimum of $M^\alpha[z, u_\delta]$ holds, for example, for linear operators A. For non-linear operators A this need not be the case (see [8]).

The so-called *smoothing functional* $M^\alpha[z, u_\delta]$ can be introduced formally, without connecting it with a conditional extremum problem for the functional $\Omega[z]$, and for an element z_α minimizing it sought on the set $F_{1,\delta}$. This poses the problem of finding the regularization parameter α as a function of δ, $\alpha=\alpha(\delta)$, such that the operator $R_2(u, \alpha(\delta))$ determining the element $z_\alpha=R_2(u_\delta, \alpha(\delta))$ is regularizing for (1). Under certain conditions (for example, when it is known that $\rho_U(u_\delta, u_T)\leqslant\delta$ and A is a linear operator) such a function exists and can be found from the relation $\rho_U(Az_\alpha, u_\delta)=\delta$. There are also other methods for finding $\alpha(\delta)$.

Let T_{δ_1} be a class of non-negative non-decreasing continuous functions on $[0, \delta_1]$, z_T a solution of (1) with right-hand side $u=u_T$, and A a continuous operator from Z to U. For any positive number ϵ and functions $\beta_1(\delta)$ and $\beta_2(\delta)$ from T_{δ_1} such that $\beta_2(0)=0$ and $\delta^2/\beta_1(\delta)\leqslant\beta_2(\delta)$, there exists a $\delta_0=\delta_0(\epsilon, \beta_1, \beta_2)$ such that for $u_\delta\in U$ and $\delta\leqslant\delta_0$ it follows from $\rho_U(u_\delta, u_T)\leqslant\delta$ that $\rho_Z(z^\delta, z_T)\leqslant\epsilon$, where $z^\alpha=R_2(u_\delta, \alpha)$ for all α for which $\delta^2/\beta_1(\delta)\leqslant\alpha\leqslant\beta_2(\delta)$.

Methods for finding the regularization parameter depend on the additional information available on the problem. If the error of the right-hand side of the equation for u_δ is known, say $\rho_U(u_\delta, u_T)\leqslant\delta$, then in accordance with the preceding it is natural to determine α by the discrepancy, that is, from the relation $\rho_U(Az_\alpha^\delta, u_\delta)=\phi(\alpha)=\delta$.

The function $\phi(\alpha)$ is monotone and semi-continuous for every $\alpha>0$. If A is a linear operator, Z a Hilbert space and $\Omega[z]$ a strictly-convex functional (for example, quadratic), then the element z_{α_δ} is unique and $\phi(\alpha)$ is a single-valued function. Under these conditions, for every positive number $\delta<\rho_U(Az_0, u_\delta)$, where $z_0\in\{z: \Omega[z]=\inf_{y\in F}\Omega[y]\}$, there is an $\alpha(\delta)$ such that $\rho_U(Az_\alpha^\delta, u_\delta)=\delta$ (see [7]).

However, for a non-linear operator A the equation $\phi(\alpha)=\delta$ may have no solution (see [8]).

The regularization method is closely connected with the construction of splines (cf. **Spline**). For example, the problem of finding a function $z(x)$ with piecewise-continuous second-order derivative on $[a, b]$ that minimizes the functional $\Omega[z]=\int_a^b (z'')^2\,dx$ and takes given values $\{z_i\}$ on a grid $\{x_i\}$, is equivalent to the construction of a spline of the second degree.

A regularizing operator can be constructed by spectral methods (see [7], [8]), by means of the classical integral transforms in the case of equations of convolution type (see [10], [7]), by the method of quasi-mappings (see [11]), or by the iteration method (see [12]). Necessary and sufficient conditions for the existence of a regularizing operator are known (see [13]).

Next, suppose that not only the right-hand side of (1) but also the operator A is given approximately, so that instead of the exact initial data (A, u_T) one has (A_h, u_δ), where

$$\rho_U(u_\delta, u_T)\leqslant\delta,$$

$$h = \sup_{\substack{z\in F_1\\ \Omega[z]\neq 0}} \frac{\rho_U(A_h z, Az)}{\{\Omega[z]\}^{1/2}} < \infty.$$

Under these conditions the procedure for obtaining an approximate solution is the same, only instead of $M^\alpha[z, u_\delta]$ one has to consider the functional

$$M^\alpha[z, u_\delta, A_h] = \rho_U^2(A_h z, u_\delta)+\alpha\Omega[z],$$

and the parameter α can be determined, for example, from the relation (see [7])

$$\rho_U^2(A_h z, u_\delta) = (\delta+h\{\Omega[z_\alpha]\}^{1/2})^2.$$

If (1) has an infinite set of solutions, one introduces the concept of a *normal solution*. Suppose that Z is a normed space. Then one can take, for example, a solution $\bar{z}$ for which the deviation in norm from a given element $z_0\in Z$ is minimal, that is,

$$\|\bar{z}-z_0\|_Z = \inf_{z\in Z}\|z-z_0\|_Z.$$

An approximation to a normal solution that is stable under small changes in the right-hand side of (1) can be found by the regularization method described above.

The class of problems with infinitely many solutions includes degenerate systems of linear algebraic equations. So-called badly-conditioned systems of linear algebraic equations can be regarded as systems obtained from degenerate ones when the operator A is replaced by its approximation A_h. As a normal solution of a corresponding degenerate system one can take a solution z of minimal norm $\| z \|$. In the smoothing functional one can take for $\Omega[z]$ the functional $\Omega[z]=\| z \|^2$. Approximate solutions of badly-conditioned systems can also be found by the regularization method with $\Omega[z]=\| z \|^2$ (see [7]).

Similar methods can be used to solve a Fredholm integral equation of the second kind in the spectrum, that is, when the parameter λ of the equation is equal to one of the eigen values of the kernel.

Instability problems in the minimization of functionals. A number of problems important in practice leads to the minimization of functionals $f[z]$. One distinguishes two types of such problems. In the first class one has to find a minimal (or maximal) value of the functional. Many problems in the design of optimal systems or constructions fall in this class. For such problems it is irrelevant on what elements the required minimum is attained. Therefore, as approximate solutions of such problems one can take the values of the functional $f[z]$ on any minimizing sequence $\{z_n\}$.

In the second type of problems one has to find elements z on which the minimum of $f[z]$ is attained. They are called *problems of minimizing over the argument*. E.g., the minimizing sequences may be divergent. In these problems one cannot take as approximate solutions the elements of minimizing sequences. Such problems are called *unstable* or *ill-posed*. These include, for example, problems of optimal control, in which the function to be optimized (the object function) depends only on the phase variables.

Suppose that $f[z]$ is a continuous functional on a metric space Z and that there is an element $z_0 \in Z$ minimizing $f[z]$. A minimizing sequence $\{z_n\}$ of $f[z]$ is called *regularizing* if there is a compact set Z in Z containing $\{z_n\}$. If the minimization problem for $f[z]$ has a unique solution z_0, then a regularizing minimizing sequence converges to z_0, and under these conditions it is sufficient to exhibit algorithms for the construction of regularizing minimizing sequences. This can be done by using stabilizing functionals $\Omega[z]$.

Let $\Omega[z]$ be a stabilizing functional defined on a set $F_1 \subset Z$, let $\inf_{z \in F_1} f[z]=f[z_0]$ and let $z_0 \in F_1$. Frequently, instead of $f[z]$ one takes its δ-approximation $f_\delta[z]$ relative to $\Omega[z]$, that is, a functional such that for every $z \in F_1$,

$$| f_\delta[z]-f[z] | \leqslant \delta\Omega[z].$$

Then for any $\alpha>0$ the problem of minimizing the functional

$$M^\alpha[z, f_\delta] = f_\delta[z]+\alpha\Omega[z]$$

over the argument is stable.

Let $\{\delta_n\}$ and $\{\alpha_n\}$ be null-sequences such that $\delta_n / \alpha_n \leqslant q<1$ for every n, and let $\{z_{\alpha_n,\delta_n}\}$ be a sequence of elements minimizing $M^{\alpha_n}[z, f_{\delta_n}]$. This is a regularizing minimizing sequence for the functional $f_\delta[z]$ (see [7]), consequently, it converges as $n \to \infty$ to an element z_0. As approximate solutions of the problems one can then take the elements z_{α_n,δ_n}.

Similarly approximate solutions of ill-posed problems in optimal control can be constructed.

In applications ill-posed problems often occur where the initial data contain random errors. For the construction of approximate solutions to such classes both deterministic and probability approaches are possible (see [7], [15]).

References

[1] TIKHONOV, A.N.: 'Solution of incorrectly formulated problems and the regularization method', *Soviet Math. Dokl.* **4** (1963), 1035-1038. (*Dokl. Akad. Nauk SSSR* **151**, no. 3 (1963), 501-504)

[2] TIKHONOV, A.N.: 'Regularization of incorrectly posed problems', *Soviet Math. Dokl.* **4** (1963), 1624-1627. (*Dokl. Akad. Nauk SSSR* **153**, no. 1 (1963), 49-52)

[3] TIKHONOV, A.N.: 'On stability of inverse problems', *Dokl. Akad. Nauk SSSR* **39**, no. 5 (1943), 176-179 (in Russian).

[4] LAVRENTIEV, M. [M.A. LAVRENT'EV]: *Some improperly posed problems of mathematical physics*, Springer, 1967 (translated from the Russian).

[5] IVANOV, V.K.: 'On ill-posed problems', *Mat. Sb.* **61**, no. 2 (1963), 211-223 (in Russian).

[6] IVANOV, V.K.: 'On linear problems which are not well-posed', *Soviet Math. Dokl.* **3** (1962), 981-983. (*Dokl. Akad. Nauk SSSR* **145**, no. 2 (1962), 270-272)

[7] TIKHONOV, A.N. and ARSENIN, V.YA.: *Solutions of ill-posed problems*, Wiley, 1977 (translated from the Russian).

[8] GONCHARSKIĬ, A.V., LEONOV, A.S. and YAGODA, A.G.: 'On the residual principle for solving nonlinear ill-posed problems', *Soviet Math. Dokl.* **15** (1974), 166-168. (*Dokl. Akad. Nauk SSSR* **214**, no. 3 (1974), 499-500)

[9] BAKUSHINSKIĬ, A.B.: 'A general method for constructing regularizing algorithms for a linear ill-posed equation in Hilbert space', *USSR Comp. Math. Math. Phys.* **7**, no. 3 (1968), 279-287. (*Zh. Vychisl. Mat. i Mat. Fiz.* **7**, no. 3 (1967), 672-677)

[10] ARSENIN, V.YA.: 'On a method for obtaining approximate solutions to convolution integral equations of the first kind', *Proc. Steklov Inst. Math.* **133** (1977), 31-48. (*Trudy Mat. Inst. Steklov.* **133** (1973), 33-51)

[11] LATTES, R. and LIONS, J.L.: *Méthode de quasi-réversibilité et applications*, Dunod, 1967.

[12] KRYANEV, A.V.: 'The solution of incorrectly posed problems by methods of successive approximations', *Soviet Math. Dokl.* **14** (1973), 673-676. (*Dokl. Akad. Nauk SSSR* **210**, no. 1, 20-22)

[13] VINOKUROV, V.A.: 'On the regularization of discontinuous mappings', *USSR Comp. Math. Math. Phys.* **11**, no. 5 (1971), 1-21. (*Zh. Vychisl. Mat. i Mat. Fiz.* **11**, no. 5 (1971), 1097-1112)

[14] TIKHONOV, A.N.: 'On the stability of the functional optimization problem', *USSR Comp. Math. Math. Phys.* **6**, no. 4 (1966), 28-33. (*Zh. Vychisl. Mat. i Mat. Fiz.* **6**, no. 4 (1966), 631-634)

此为试读，需要完整PDF请访问：www.ertongbook.com