Oblast vzdělávání MATHEMATICS

A general remark, valid for all programmes in Mathematics

A part of the study plan of each student of the doctoral study in the framework of the study programmes in Mathematics should be an active participation in a conference. An appropriate preparation for the participation in an international conference is an active participation in the internal conference Day of Doctoral Students of the School of Mathematics (DDS-M) which is organized by the School of Mathematics for this purpose every year, see `http://karlin.mff.cuni.cz/wds-m/`. An active participation in DDS-M is not a general duty of all students, however, it becomes obligatory if an active participation in DDS-M is contained in the individual study plan of the student for the respective academic year. Thus, the obligation of an active participation in DDS-M is mainly given by the decision of the supervisor, resp. by his or her agreement with the respective student.

Study programme P4M1 Algebra, number theory and mathematical logic

Subject-area board

Current composition of the board is at the address `http://mff.cuni.cz/phd/or/p4m1`.

Cooperating institutes

- Institute of Mathematics of the CAS, v.v.i.
  Žitná 25, 115 67 Praha 1
  `http://www.math.cas.cz`

- Institute of Computer Science of the CAS, v.v.i.
  Pod Vodárenskou věží 2, 182 07 Praha 8
  `http://www.ustavinformatiky.cz/`

Offered topics

The topics can be found in SIS at the address `http://mff.cuni.cz/phd/temata/p4m1`.

Provided teaching

Code	Subject	Winter	Summer
NAIL056	**Seminar on Logic I**	0/2 C	—
NAIL080	**Seminar on Logic II**	—	0/2 C
NDMI045	**Analytic and Combinatorial Number Theory**	—	2/0 Ex
NMAG265	**Students' Seminar on Set Theory**	0/2 C	—
NMAG405	**Universal Algebra 1**	2/2 C+Ex	—
NMAG407	**Model Theory**	2/0 Ex	—
NMAG446	**Logic and Complexity**	—	2/0 Ex
NMAG450	**Universal Algebra 2**	—	2/1 C+Ex
NMAG455	**Quadratic forms and class fields I**	2/0 Ex	—
NMAG456	**Quadratic forms and class fields II**	—	2/0 Ex
NMAG462	**Modular forms and L-functions I**	2/0 Ex	—
NMAG466	**Lattice Theory 2**	—	2/0 Ex
NMAG470	**Number Theory Seminar**	0/2 C	0/2 C
NMAG473	**Modular forms and L-functions II**	—	2/0 Ex
NMAG475	**MSTR Elective Seminar**	0/2 C	0/2 C
NMAG498	**MSTR Elective 1**	2/0 Ex	—
NMAG499	**MSTR Elective 2**	—	2/0 Ex
NMAG531	**Approximations of Modules**	—	2/0 Ex
NMAG536	**Proof Complexity and the P vs. NP Problem**	—	2/0 Ex
NMAG562	**Homological and Homotopic Algebra**	2/0 Ex	—
NMAG563	**Introduction to complexity of CSP**	2/0 Ex	—
NMAG565	**Algebra and Infinite Combinatorics**	2/0 Ex	—
NMAG567	**Group Representations 2**	2/2 C+Ex	—
NMAG571	**Algebra Seminar**	0/2 C	0/2 C
NMAG573	**Seminar on CSP**	0/2 C	0/2 C
NMIN160	**Set Theory**	2/0 Ex	—
NMMB451	**Applications of Mathematics in Computer Science**	—	0/2 C
NMMB452	**Seminar on Mathematics Inspired by Cryptography**	0/2 C	0/2 C
NMMB453	**Students' Seminar on Logic**	0/2 C	0/2 C
NMMB471	**MIT Elective Seminar**	—	0/2 C
NMMB498	**MIT Elective 1**	2/0 Ex	—
NMMB499	**MIT Elective 2**	—	2/0 Ex
NMMB551	**Seminar on Combinatorial, Algorithmic and Finitary Algebra**	0/2 C	0/2 C
NMMB621	**Doctoral seminar in cryptology**	0/2 C	0/2 C
NTIN071	**Automata and Grammars**	—	2/2 C+Ex
NTIN090	**Introduction to Complexity and Computability**	2/1 C+Ex	—
NMAG575	**Forcing**	2/0 Ex	—
NMAG576	**Seminar on Forcing**	—	0/2 C

NLTM014	**Nonstandard Seminar 1**	0/2 C	—
NLTM015	**Nonstandard Seminar 2**	—	0/2 C
NMAG577	**Seminar on Reckoning**	0/2 C	0/2 C
NTIN062	**Complexity I**	2/1 Z+Zk	—
NTIN064	**Computability**	—	2/0 Ex
NTIN073	**Recursion**	2/0 Ex	—
NTIN088	**Algorithmic Randomness**	—	2/0 Ex
NMAI067	**Logic in Computer Science**	2/0 Ex	—
NAIL021	**Boolean Functions and Their Applications**	2/0 Ex	—
NMAI040	**Introduction to Number Theory**	2/0 Ex	—
NDMI066	**Algebraic Number Theory and Combinatorics**	2/0 Ex	—

List of requirements for taking the state doctoral exam

Student will choose - in agreement with his or her advisor - one of three topics: „Algebra”, „Mathematical logic” or „Number theory.” The state doctoral exam is then conducted in the chosen topic according to the following list of requirements:

Algebra

I. Basics

Obligatory part.

I.1 Basic algebra

Group theory: finite groups, the Sylow theorems, the structure of finitely generated abelian groups, free groups and their subgroups.

Galois theory: Galois extensions and Galois groups, radical field extensions, unsolvability of polynomial equations by radicals.

Representation theory and algebraic geometry: Representations of finite groups, Maschke's theorem, characters. The correspondence between affine algebraic sets and ideals in polynomial rings, Hilbert's Nullstellensatz.

Universal algebra: varieties of algebras, subdirect decompositions, free algebras, the Birkhoff theorem. Lattices, complete lattices, closure operators and Galois correspondences.

II. Advanced topics

After agreement with the advisor, the student will select two different topics from the advanced topics of the specialization ”Algebra”, ”Number theory” or ”Mathematical logic”. However, at least one of them must be one of the following (II.1–II.10):

II.1. Group theory

Group action on a set. Permutation, solvable and nilpotent groups. Linear groups. Finite simple groups, simplicity of A_n and $\mathrm{PSL}_n(\mathrm{K})$. Basics of the theory of groups extensions, semidirect products of groups. Induced representations of groups and the Frobenius reciprocity, Mackey's theorem and its consequences.

II.2 Binary systems

Left distributive groupoids (free, monogenerated, the word problem), relation to braid groups. Medial and two–sided distributive groupoids, the equational theory of medial idempotent groupoids. Normal subquasigroups and congruences of loops and quasigroups, nuclei, the center, nilpotence. Relations to the multiplication group. LCC, CC, extra, Bol and Moufang loops. Inverse properties, diassociativity. Isotopy, central and medial quasigroups. Toyoda's theorem.

II.3 Commutative algebra

Commutative noetherian rings: the spectrum, localization, primary decomposition. Integral extensions, Dedekind domains, factorization of ideals. Localization and completion of modules. Krull's Principal ideal theorem. Regular sequences, depth, the Auslander–Buchsbaum theorem.

II.4 Algebraic geometry

Affine and projective algebraic sets, the Zarisky topology, decomposition into irreducible components. Function fields, rational maps, birational equivalence. Homomorphisms of algebraic sets, projective elimination, closedness of homomorphisms from projective algebraic sets. Bézout's theorem. Krull dimension and its properties.

II.5 Module theory and homological algebra

Projective and injective modules. Chain conditions on ideals, the Hopkins–Levitzki theorem, Faith's characterization of noetherian rings. The Morita equivalence. Categories of modules, the tensor product, functors Ext and Tor, long exact sequences. Direct limits, pure embeddings, pure–injective modules and relation to model theory. Derived categories.

II.6 Approximations of modules and infinite combinatorics

Cotorsion pairs, filtrations, the Eklof and Hill lemmas. Deconstructibility for regular and singular cardinals (dependence on the set theory, Shelah's Singular compactness theorem). The structure of Whitehead and Baer modules.

II.7 Representations of finite dimensional algebras

Finite dimensional algebras as factors of path algebras. The Krull–Schmidt theorem. Finite, tame and wild representation types. Hereditary algebras and Gabriel's characterisation of the finite representation type. Tilting modules and tilted algebras. Almost split maps, the AR–sequences, the AR–quiver of a finite dimensional algebra.

II.8 Universal algebra and lattice theory

Malcevské podmínky. Commutators for general algebras and Abelian algebra. Equational theories, term rewriting systems and the Knuth–Bendix algorithm, finitely based varieties. Distirbutive, modular, semimodular and geometric lattices, lattice congruences, free lattices and the word problem. Jónsson's lemma and varieties of lattices.

II.9 Universal algebraic methods in the CSP

Relational and algebraic clones, homomorphisms of clones and primitive positive interpretation of relational structures. Complexity of the CSP and clones of polymorphisms, Taylor clones, Maltsev CSP's and finite width problems, Schaefer's theorem classifying CSP's on a two–element set.

II.10 Combinatorics on words

Dickson's lemma. F–semigroups (the minimal generating set, codes, the stability condition, rank of semigroup). The Chomsky hierarchy (formal grammars and the corresponding automata, Kleene's theorem, pumping lemmas, Parikh's theorem). Equations in free monoids (the Compactness theorem, the Graph lemma, properties of the defect, equaivalence and test sets). The Post correspondence problem.

Recommended literature

Anderson, F. W., Fuller, K. R.: **Rings and Categories of Modules.** *GTM 13. 2nd ed. Springer, New York, 1992.*

Assem I., Simson, D., Skowronski, A.: **Elements of the Representation Theory of Associative Algebras I.** *LMSST 65. Cambridge University Press, Cambridge, 2006.*

Atiyah, M. F., Macdonald, I. G.: **Introduction to commutative algebra.** *Addison-Wesley Publishing Co., 1969.*

Auslander M., Reiten, I., Smalo. S. O.: **Representation theory of Artin algebras.** *Cambridge University Press, Cambridge, 1997.*

Barto L., Krokhin, A., Willard, R.: **Polymorphisms, and how to use them.** *Dagstuhl Follow-Ups. Vol. 7. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2017.*

Bergman C.: **Universal Algebra: Fundamentals and Selected Topics.** *Chapman and Hall/CRC, 2011.*

Berstel, J., Perrin, D.: **Theory of Codes.** *Academic Press, London, 1985.*

Bruck, R. H.: **A Survey of Binary Systems.** *Springer, Berlin, 1971.*

Bruns, W., Herzog, J.: **Cohen–Macaulay Rings.** *CSAM 39. Cambridge University Press, Cambridge, 1998.*

Bulatov, A., Krokhin, A., Larose, B.: **Dualities for constraint satisfaction problems.** *In: Complexity of Constraints, LNCS 5250. Springer, New York, 2008.*

Bulatov, A., Valeriote, M.: **Results on the algebraic approach to the CSP.** *Proc. Dagstuhl Sem., LNCS, Springer, New York, 2008.*

Burris, S., Sankappanavar, H. P.: **A Course in Universal Algebra.** *Springer, New York, 1981.*

Cox, D. A., Little, J., O'Shea, D.: **Ideals, varieties, and algorithms.** *4th edition. Springer, Cham, 2015.*

Crawley, P., Dilworth, R. P.: **Algebraic Theory of Lattices.** *Prentice Hall, 1973.*

Dehornoy, P.: **Braids and Self Distributivity. Birkhäuser.** *Basel, 2000.*

Eilenberg, S.: **Automata, languages and machines A and B.** *Academic Press, 1973, 1974.*

Eisenbud, D.: **Commutative Algebra.** *GTM 150. Springer, New York, 1995.*

Eklof, P. C., Mekler, A. H.: **Almost–Free Modules.** *2nd ed. Elsevier, Amsterdam, 2002.*

Enochs, E. E., Jenda, O. M. G.: **Relative Homological Algebra. Vol. 1,2.** *GEM 30, 54. 2nd ed. W. de Gruyter, Berlin, 2011.*

Facchini, A.: **Module Theory.** *Birkhäuser, Basel, 1998.*

Fulton, W.: **Algebraic Curves.** *Reprint of 1969 original. Addison-Wesley Publishing Company, 1989.*

Goebel, R., Trlifaj, J.: **Approximations and Endomorphism Algebras of Modules. Vol. 1,2.** *GEM 41. 2nd ed. W. de Gruyter, Berlin, 2012.*

Goertz, U., Wedhorn, T.: **Algebraic geometry I.** *Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010.*

Gratzer, G.: **General Lattice Theory.** *2nd ed. Birkhäuser, Basel, 1998.*

Hobby, D., McKenzie, R.: **The structure of finite algebras.** *Contemp. Math. 76. AMS, Providence, 1988.*

Jezek, J.: **Universal Algebra.** *Text available at* `http://www.karlin.mff.cuni.cz/~jezek`.

Lallement, G.: **Semigroups and combinatorial applications.** *Wiley, 1979.*

Lang, S.: **Algebra.** *3rd ed. Academic Press, New York, 1993.*

Lothaire, M.: **Algebraic Combinatorics on Words.** *Cambridge University Press, Cambridge, 2002.*

Lothaire, M.: **Applied Combinatorics on Words.** *Cambridge University Press, Cambridge, 2005.*

Lothaire, M.: **Combinatorics on Words.** *Cambridge University Press, Cambridge, 1997.*

Matsumura, H.: **Commutative Ring Theory.** *CSAM 8. Cambridge University Press, Cambridge, 1994.*

Pflugfelder, H. O.: **Quasigroups and Loops: Introduction.** *Heldermann Vlg, Berlin, 1990.*

Prest, M.: **Purity, spectra and localisation.** *Cambridge University Press, Cambridge, 2009.*

Prochazka, L. et al: **Algebra.** *Academia, Praha, 1990.*

Rotman, J. J.: **An introduction to the theory of groups.** *Springer, New York, 1995.*

Rotman, J. J.: **An introduction to homological algebra.** *2nd edition. Springer, New York, 2009.*

Rowen, L. H.: **Graduate Algebra: Commutative View.** *GSM 73. AMS, Providence, 2006.*

Rowen, L. H.: **Graduate Algebra: Noncommutative View.** *GSM 91. AMS, Providence, 2008.*

Rozenberg, G., Salomaa, A. (eds.): **Handbook of Formal Languages, vol. 1 – 3.** *Springer, 2004.*

Shafarevich, I. R.: **Basic algebraic geometry 1** *3rd edition. Springer, Heidelberg, 2013.*

Weibel, C.: **An Introduction to Homological Algebra. CSAM 38.** *Cambridge University Press, Cambridge, 1994.*

Weintraub, S. H.: **Representation Theory of Finite groups. GSM 59.** *AMS, Providence, 2003.*

Mathematical logic

I. Common background

Obligatory part.

I.1 Basic logic

Propositional and predicate logic. First-order structures, Tarski's definition of satisfiability. Provability, the completeness and the compactness theorems. Set theory as a first-order theory. Godel's theorems on the incompleteness and on the unprovability of consistency. Turing machines: universal machine, algorithmically undecidable problems, the halting problem. Quantifier elimination in the ordered field of real numbers.

II. Advanced topics

After agreement with the advisor, the student will select two different topics from the advanced topics of the specialization "Algebra", "Number theory" or "Mathematical logic". However, at least one of them must be one of the following (II.1–II.6):

II.1. General model theory

Basic notions: substructure and elementary substructure, diagram, homomorphism, embedding and elementary embedding, isomorphism. The Lowenheim-Skolem theorems. Model completeness. Definable sets, types, quantifier elimination. Model constructions: omitting types, Henkin's construction, Skolemization. Craig interpolation, elementary chains, Robinson's joint consistency theorem, indiscernible elements. Saturated and homogeneous models, prime models. Ultraproduct and its basic properties. Elementary classes.

II.2 Applied model theory

Real closed ordered fields and their reducts and expansions, theorems of Tarski and of Wilkie. O-minimal structures and their basic geometric and topological properties. Stable and omega-stable theories, uncountable categoricity, Morley's theorem. Minimal and strongly minimal structures, general closer operator, geometries and dimension in strongly minimal structures. Omega-stable groups, the Cherlin-Zilber hypothesis. Hrushovski's amalgamation method.

II.3. Set theory

Axioms of ZFC. Axiom of choice AC, Zorn's lemma, well-orderings. Ordinal and cardinal arithmetic, transfinite induction. Infinite combinatorics: independent and almost-disjoint set systems, Ramsey's theorem, closed and unbounded sets and stacionary sets, the diamond principle, Martin's axiom. Trees (Suslin's, Aronszajn's, Kurepa's), Suslin's hypothesis. Boolean algebras, ultrafilters, Stone duality. Constructible sets, axiom V = L. GCH and AC in L. Forcing and Boolean models, the independence of CH. Inaccessible and measurable cardinals, elementary embeddings. Descriptive set theory: Borel, analytic and projective sets, infinite games, determinacy. Uniformization theorems. Borel equivalences. Polish spaces, Polish groups and their actions.

II.4. Computability theory

Partial recursive functions, recursive and recursively enumerable sets. Universal partial recursive function, index. Recursion theorem and Rice's theorem. Creative sets, effective unseparability. Jump operator, the arithmetical hierarchy, degrees of unsolvability. Arithmetic forcing, priority method. Kolmogorov complexity, basics of algorithmic randomness.

II.5 Proof theory and formal arithmetic

Gentzen's sequent calculus, cut elimination, Herbrand's theorem. Craig's interpolation. Robinson's arithmetic Q and Peano arithmetic PA. Interpretability of theories. Undecidability of Q and PA. Provably total recursive functions. The non-existence of finite axiomatization of PA. Second order logic, simple type theory, infinitary logic. Reverse mathematics. Non-classical logics: intuitionistic, modal, many-valued.

II.6 Logic and complexity

Time and space complexity of algorithms, main complexity classes. Boolean circuits and main known circuit lower bounds. Natural proofs of Razborov and Rudich. Finite model theory, descriptive complexity. Definability in finite structures, Fagin's theorem. Logics with the least fixed-point operator. O-1 laws. The Ehrenfeucht-Fraisse method. Locality and theorems of Hanf and Gaifman. Pebbling games. The spectrum problem. Proof complexity, propositional proof systems of Cook and Reckhow. Resolution, DPLL SAT-algorithm and their connection. Frege systems and Extended Frege systems. Resolution size lower bounds. Bounded arithmetic. Definability of polynomial hierarchy. Witnessing functions and search problems. Propositional translations. The problem of finite axiomatizability of bounded arithmetic.

Recommended literature

Balcar, B., Stěpánek, P.: **Teorie množin.** *Academia, Praha, 1986, 2001.*

Bartoszynski, T., Judah, H.: **Set Theory, On the Structure of Real Line.** *A. K. Peters, Wellesley, Massachussets, 1995.*

Barwise, J. (ed.): **Handbook of Mathematical Logic.** *NHPC, 1972 (rusky Nauka, Moskva, 1982).*

Buss, S. R. (ed.): **Handbook of Proof Theory, Studies in Logic and the Foundations of Mathematics 137.** *Elsevier, Amsterdam, 1998.*

Cook, S. A., Nguyen, P.: **Logical foundations of proof complexity.** *Cambridge University Press.*

Demuth, O., Kryl, R., Kučera, A.: **Teorie algoritmů I, II.** *SPN, Praha, 1984, 1989.*

Devlin, K. J.: **Constructibility.** *Springer–Verlag, Heidelberg, 1984.*

Dries van den, L.: **Tame Topology and O–minimal Structures.** *London Mathematical Society Lecture Note Series, no. 248, 1998.*

Ebbinghaus, H.–D., Flum, J., Thomas, W.: **Mathematical Logic.** *Springer–Verlag, Heidelberg, 1984.*

Ebbinghaus, H.–D., Flum, J.: **Finite Model Theory.** *Springer–Verlag, 2005.*

Gabbay, D., Guenthner, F. (eds.): **Handbook of Philosophical Logic I–IV.** *D. Riedel Publishing comp., 1983.*

Hájek, P., Pudlák, P.: **Metamathematics of First–Order Arithmetic.** *Springer–Verlag, Heidelberg, 1993.*

Hodges, W.: **Model Theory.** *Cambridge University Press, Cambridge, 1993.*

Chang, C. C., Keisler, H. J.: **Model–Theory.** *NHPC, New York, 1973 (rusky Mir, Moskva, 1977).*

Jech, T.: **Set Theory.** *Springer–Verlag, 2002.*

Kechris, A.: **Classical descriptive set theory.** *Springer–Verlag, New York, 1994.*

Krajíček, J.: **Bounded arithmetic, propositional logic, and complexity theory.** *Cambridge University Press, Cambridge, 1995.*

Kunen, K.: **Set Theory, An Introduction to Independence Proofs.** *NHPC, New York, 1980.*

Laxembourgh, W. A. J., Stroyan, K. D.: **Introduction to the Theory of Infinitesimals.** *Academic Press, London, 1976.*

Li, M., Vitanyi, P.: **An Introduction to Kolmogorov Complexity and Its Applications.** *Springer, 1997.*

Marker, D.: **Model Theory — An Introduction.** *Springer, 2002.*

Moschovakis, Y.: **Descriptive Set Theory.** *North–Holland, 1980.*

Odifreddi, P.: **Classical Recursion Theory. The Theory of Functions and Sets of Natural Numbers.** *NHPC, New York, 1989.*

Papadimitriou, C. H.: **Computational Complexity.** *Addison Wesley, 1994.*

Pillay, A.: **Geometric Stability Theory.** *Clarendon Press, Oxford, 1996.*

Priest, G.: **An Introduction to Non–Classical Logic** *Cambridge University Press, 2001.*

Rogers, H., Jr.: **Theory of Recursive Functions and Effective Computability.** *Mc Graw–Hill, New York, 1967.*

Shelah, S.: **Classification Theory.** *NHPC, New York, 1990.*

Shelah, S.: **Proper and Unproper Forcing.** *Springer–Verlag, Heidelberg, 1998.*

Shoenfield, J. R.: **Mathematical Logic.** *Addison Wesley Publishing Company, Reading, 1967 (rusky Nauka, Moskva, 1975).*

Simpson, S.: **Subsystems of second order arithmetic.** *Springer–Verlag, New York, 1999.*

Soare, R. I.: **Recursively Enumerable Dets and Degrees, A Study of Computable Functions and Computably Generated Sets.** *Springer–Verlag, Heidelberg, 1987.*

Takeuti, G.: **Proof Theory.** *Elsevier, Amsterdam, 1987.*

Number Theory

I. Basics

Obligatory part.

Basic number theory: Density of primes, Legendre and Jacobi symbol, quadratic reciprocity, continued fractions, quadratic number fields, Rabin–Miller algorithm, RSA.

Algebraic number theory: number fields, existence of integral basis, Dedekind domains. Prime splitting and ramification. Geometry of numbers, class number, Dirichlet unit theorem. Cyclotomic fields, solving diophantine equations, p–adic numbers.

Computer algebra: Berlekamp algorithm for polynomial factorization. Groebner bases and Buchberger algorithm. Factorization of polynomials with integral coefficients.

II. Advanced topics

After agreement with the advisor, the student will select two different topics from the advanced topics of the specialization "Algebra", "Number theory" or "Mathematical logic". However, at least one of them must be one of the following (II.1–II.6):

II.1 Cryptology and factorization

Pseudo-random number generators, symmetric and stream ciphers, hash functions, provable security, cryptographic protocols, zero-knowledge proofs. Number field sieve and its constituent algorithms (finding the root, choice of polynomial, etc.). Further factorization algorithms (p-1, p+1, rho, use of elliptic curves) and their importance for number field sieve. Primality tests and proofs (quadratic Frobenius, N-1 test, ECPP, polynomial-time algorithms).

II.2 Advanced cryptoanalysis methods

Theory of boolean functions, S-boxes, their cryptographic properties, linear and differential cryptoanalysis, LLL–algorithm and its cryptoanalytic applications.

II.3 Self-correcting codes

Classical theory of cyclic codes. Self-dual codes and invariant theory. Convolution codes. Turbo codes. Decoding algorithms, esp. Viterbi's and various algorithms for Reed–Solomon codes. Quaternary codes. Covering radius and steganography applications. Detailed knowledge of BCH, alternating, Kerdock, Preparata, Justensen, Reed–Muller, and QR codes. Asymptotic estimates and constructions of asymptotically optimal codes. LDPC codes. MDS codes. Basic estimates (Plotkin, Hamming, Griesmer, Singleton, Johnson, Gilbert–Varshamov, linear programming).

II.4 Elliptic curves

Varieties over finite fields (Frobenius morphism, Hasse–Weil theorem for Jacobian, Tate's theorem). Arithmetic of elliptic curves (group law, rational points, torsion points, isomorphisms and isogenies). Montgomery scalar multiplication. Pairing and its implementation. Computations of the number of points (elementary methods, Schoof's and Satoh's algorithm, complex multiplication). Computations of the discrete logarithm (chinese remainder theorem, baby–step giant–step, Pollard's methods). Cryptography based on pairing. Applications of elliptic curves for factorization and prime-testing.

II.5 Algebraic number theory II

Quadratic forms: class group of binary forms, genus theory, primes represented by a binary form, universal forms, Hasse–Minkowski theorem, Hilbert symbol. Adeles and ideles, locally compact groups. Global and local class field theory.

II.6 Analytic number theory

L-functions: Riemann zeta-function, Dirichlet L-functions, Euler product, meromorphic continuation, functional equation, Dirichlet theorem on primes in arithmetic progressions. Modular forms: Basic properties, dimensions of spaces of modular forms. Fourier expansion, Eisenstein series. Hecke operators, applications.

Recommended literature

Cassels, J. W. S.: **Local Fields.** *Cambridge University Press, Cambridge, 1986.*

Cohen H.: **A course in computational algebraic number theory.** *Springer, Berlin, 1993.*

Cohen, H., Frey, G. et al. (eds.): **Handbook of Elliptic and Hyperelliptic Curve Cryptography.** *Chapman & Hall–CRC, Boca Raton, 2005.*

Cox, D. A., **Primes of the Form x2+ny2: Fermat, Class Field Theory, and Complex Multiplication.** *Wiley, 1989.*

Crandall, R., Pomerance, C.: **Prime Numbers — A Computational Perspective.** *2nd ed. Springer, New York, 2005.*

Goldreich, O.: **Foundations of Cryptography, Basic Tools.** *Cambridge University Press, Cambridge, 2001.*

Gôuvea, F. Q.: **P–adic Numbers: An Introduction.** *Springer, New York, 1997.*

Hardy, G. H., Wright, E. M.: **An Introduction to the Theory of Numbers.** *Clarendon Press, Oxford, 1945.*

Irelan, K., Rosen, M.: **A classical introduction to modern number theory.** *Springer, Berlin, 1990.*

Koblitz, N.: **Introduction to Elliptic Curves and Modular Forms.** *Springer, 1993.*

Koblitz, N.: **P–adic Numbers, P–adic Analysis and Zeta–Functions.** *Springer, 1984.*

Lang, S.: **Algebra.** *Springer, New York, 2003.*

Lang, S.: **Algebraic Number Theory.** *Springer, New York, 1994.*

Marcus, D. A.: **Number Fields.** *Springer, 1977.*

Menezes, A.J. et al. (eds.): **Handbook of Applied Cryptography.** *Chapman & Hall–CRC, Boca Raton, 2006.*

Milne, J. S.: **Algebraic Number Theory.** *Online* http://www.jmilne.org/math/.

Milne, J. S.: **Class Field Theory.** *Online* http://www.jmilne.org/math/.

Milne, J. S.: **Elliptic Curves.** *Online* http://www.jmilne.org/math/.

Pless, V. S., Brualdi, R. A., Huffman, W. C. (eds.): **Handbook of Coding Theory.** *North Holland, 1998.*

Serre, J.-P. **A Course in Arithmetic.** *Graduate Texts in Mathematics 7, 1973.*

Silverman, J. H.: **The Arithmetic of Elliptic Curves.** *Springer, 1986.*

Steuding, J.: **Diophantine Analysis.** *Chapman & Hall, 2005.*

Stinson, D. R.: **Cryptography: Theory and Practice.** *CRC Press, Boca Raton, 2006.*

Sudan, M.: **Algorithmic Introduction to Coding Theory.** *Online* http://theory.lcs.mit.edu/~madhu/FT01/course.html.

Study programme P4M2 Geometry, topology, and global analysis

Subject-area board

Current composition of the board is at the address http://mff.cuni.cz/phd/or/p4m2.

Cooperating institutes

- Institute of Mathematics of the CAS, v.v.i.
  Žitná 25, 115 67 Praha 1
  http://www.math.cas.cz

Offered topics

The topics can be found in SIS at the address http://mff.cuni.cz/phd/temata/p4m2.

Provided teaching

Code	Subject	Winter	Summer
NMAG569	**Mathematical Methods of Quantum Field Theory**	0/2 C	—
NMAG575	**Forcing**	2/0 Ex	—
NMAG471	**Fundamentals of Category Theory**	2/2 C+Ex	—
NMAG461	**Hypercomplex Analysis**	2/0 Ex	—
NMAG566	**Riemannian Geometry 2**	—	2/0 Ex

NMAG451	**Fractals**	0/2 C	—
NMAG498	**MSTR Elective 1**	2/0 Ex	—
NMAG561	**Commutative Algebra 2**	—	2/0 Ex
NMAG437	**Seminar on Differential Geometry**	—	0/2 C
NMAG452	**Introduction to Differential Topology**	—	2/0 Ex
NMAG454	**Fibre Spaces and Gauge Fields**	—	3/1 C+Ex
NMAG532	**Algebraic Topology 2**	—	2/2 C+Ex
NMAG448	**Classical groups and their invariants**	—	2/2 C+Ex

List of requirements for taking the state doctoral exam

I. Common background

At lest three of the following subjects:

I.1. General Topology

Basic notions. Uryson lemma, Tietze thorem. Connectedness and local connectedness. Compactness and local compactness. Tichonov theorem. Stone-Weierstrass theorem, Cech-Stone compactification. Paracompactness. Stone's theorem about paracompactness of metric spaces. Metrizable spaces, metrizability theorems, completeness of metric spaces. Topological groups, basic properties. Uniform spaces and uniformly continuous maps, metrizability, completeness.

I.2. Set theory

Axiomatic set theory. Ordinal and cardinal numbers and their basic arithmetics. Axiom of choice and its equivalents, transfinite recursion. Infinite combinatorics, stationary sets. Ramsey theorem, Erdos-Rado theorem, lemma about delta system, independent systems. Partial orderings.

I.3. Category theory

Categories and functors, examples. Natural transformations and equivalences, examples. Limits a colimits, completeness, their forms in concerte categories. Adjunction, reflectivity and coreflectivity. Closed and Cartesian closed categories. Small categories, Mac Lane representation.

I.4. Sectected topics from algebra

Tensor algebra, in particular multilinear algebra. Selected topics from ring and module theory (extensions, resolvents, gradings, filtrations). Basics of homological algebra (homology of complexes, cohomology of groups and other algebraic systems).

I.5. Riemannian manifolds

Theory of connections. Parallel transport. Riemann metric, Riemann connections, curvature tensors and their meaning. Sectional curvature and its meaning. Geodesics. Homogeneous Riemannian manifolds. Hermitian metrics. Submanifolds of Euclidean space. Holonomy groups.

I.6. Analysis on manifolds

Vector bundles and their classification. Differential operators, invariant differencial operators on homogeneous manifolds. Integration on manifolds. Basics of integral geometry on manifolds. Fourier and Radon transform. Complex manifolds, holomorphic and meromorphic functions.

I.7. Lie groups and algebras

Classification of simple Lie groups and their finite dimensional representations. Decomposition of tensor product into irreducible components. Klimyk formula. Characters of representations and character formulas (Weyl, Freudenthal, etc.).

I.8. Algebraic topology

Homology and cohomology groups (either simplicial or singular) and their computation. Borsuk theorems, theorems concerning invariance of domains and dimensions, fundamental theorem of algebra. Euler theorem. Map degree. Lefschetz fixed point theorem. De Rham cohomology. Basics of homotopy theory.

II. Advanced topics

One of the following:

II.1. General topology

Pointless approaches to topology. Variants of Stone duality. Boolean algebras, Heyting algebras, continuous lattices, and related dualities. Strengthening the structure of pointless topology. Spaces of continuos functions, possible topologies on these, Arzel-Ascoli theorem, Cp(X). Cardinal invariants of topological spaces, their mutual relations. Ultrafilter spaces, cardinal characteristics. Computer topology. Topological dynamics, almost periodic points, classification of dynamical systems, Ellis enveloping, recurence in dynamical systems, applications in combinatorics. Properties of topological spaces related to combinatorial principles of set theory. Continuity structures, theory of miform and proximite systems.

II.2. Set theory

Boolean algebras, partial orderings. Stone duality, structural properties. Combinatorial principles, Martin axiom, Fodor-Solovay theorem, Silver theorem, Suslin a Aronszajn trees. Kurep hypothesis, Hausdorf gap. Basics of forcing. PFA. Elementary substructures, ultraproduct, basics of pcf theory.

II.3. Category theory

Monads and monadic categories. Categories and logic. Basics of topos theory. Concrete categorical questions of special structures. Theory of concrete categories and structures. Initial and terminal construction of an object. Algebraic and topological categories. Complete and almost complete embeddings. Rigid objects, rigid graphs, algebras and spaces. Universality and almost universality, almost universality of category of paracompact spaces.

II.4. Geometry of homogeneous and symmetric spaces.

Homogeneous spaces, reductive spaces, canonical connections. Invariant metrics and differential operators on homogeneous spaces, especially Riemannian ones, examples, classification. Some generalizations of symmetric spaces, Einstein spaces.

II.5. Parabolic structures on manifolds

Graded Lie algebras, their real forms. Principal fibre bundles, connections, covariant derivatives and their curvatures. Homogeneous differential operators. Cartan and parabolic geometries, Cartan connection and its curvature. Conformal, projective, quaternionic geometry and further examples of parabolic geometries.

II.6. Integral geometry and complex analysis

Functions of several complex variables. Complex manifolds, Hermitian and Kaehler manifolds. Sheaves and subsheaves. Differential forms on complex manifolds and Dolbeaut cohomology. Radon and Penrose transformation.

II.7. Invariant differential operators

Spin structures on Riemannian manifolds. Dirac operator and its properties, Laplace operators. Spectral properties of differential operators. Theory of differential operators of Dirac type. Conformal invariance of operators on a conformal manifold. Bochner and Weitzenbock formula. Invariant operators for other geometric structures.

II.8. Algebraic topology

Derived functors. Spectral sequences an their applications. Fibrations, homological and homotopical theory of fibrations. Topology of Lie groups and classifyng spaces. Characteristic classes of vector bundles, Chern-Weil homomorphism. Basics of K-theory. Cohomological operations. Obstruction theory. Index theorems. Operads, algebras over operads.

Recommended literature

Adámek, J., Herrlich H., Strecker G.: **Abstract and Concrete Categories.** *Wiley, New York, 1990.*

Borceaux, F., Bosche van den, G.: **Algebra in a Localic Topos with Applications to Ring Theory.** *Springer, 1983.*

Čap, A., Slovák, J.: **Parabolic geometries, I: Background and general theory.** *AMS Publishing House, 2009.*

Ellis, R.: **Lectures in Topological Dynamics.** *Benjamin, New York, 1967.*

Engelking, R.: **General Topology.** *PWN, Warsawa, 1977.*

Friedrich, Th.: **Dirac Operatoren in der Riemannschen Geometrie.** *Wiesbaden, 1997.*

Fulton, W., Harris, J.: **Representation Theory.** *A first course, GTM 129. Springer New York, 1991.*

Fustenberg, H.: **Reccurence in Ergodic Theory and Combinatorial Number Theory.** *Princeton University Press, Princeton, 1981.*

Gillmann, L., Jerison, M.: **Rings of continuous functions.** *D. van Nostrand, New York, 1960.*

Harris, J.: **Algebraic geometry.** *A first course, GTM 133. Springer, New York, 1992.*

Hatcher A.: **Algebraic Topology.** *Text available at* `http://www.math.cornell.edu/~hatcher/AT/ATpage.html`.

Helgason, S.: **Differential geometry, Lie groups and Symmetric spaces.** *Pure and Appl. Math. 80, Ac. Press, 1978.*

Isbell J. R.: **Uniform spaces.** *Amer. Math. Soc., Providence, 1964.*

Jech, T.: **Set Theory.** *Springer–Verlag, Berlin, 2003.*

Johnstone, P. T.: **Stone Spaces.** *Cambridge University Press, Cambridge, 1982.*

Johnstone, P. T.: **Topos Theory.** *Academic Press, London, 1972.*

Juhásy, I.: **Cardinal functions in topology — Ten Years Later.** *Math Centre Tracts 125, Amsterdam, 1980.*

Juhásy, I.: **Cardinal Functions in Topology.** *Math. Centre Tracts 34, Amsterdam, 1975.*

Kelley, J. L.: **General Topology.** *Van Nostrand, New York, 1955.*

Kunen, K.: **Set Theory — An Introduction to Independence Proofs.** *North–Holland, Amsterdam, 1980.*

Lawson, B. L., Michelsohn, M. L.: **Spin Geometry.** *Princeton Math. Series, Princeton, 1989.*

Leinster, T.: **Basic Category Theory.** *Cambridge University Press, Cambridge, 2014.*

MacLane, S.: **Categories for the Working Mathematician.** *GTM5. Springer–Verlag, New York, 1970.*

MacLane, S.: **Homology.** *Academic Press, New York, 1963.*

Massey, W.: **Singular Homology theory.** *GTM 70. Springer, New York, 1976.*

Monk, J. D., Bonnet, R.: **Handbook of Boolean Algebras, vol 1.** *North–Holland, Amsterdam, 1989.*

Pultr, A.: **Podprostory euklidovských prostorů.** *SNTL, Praha, 1986.*

Pultr, A., Trnková, V.: **Combinatorial, Algebraic and Topological Representations of Groups, Semigroups and Categories.** *Academia, Praha, 1980.*

Rudin, M. E.: **Lectures on Set Theoretic Topology.** *Amer. Math. Soc., Providence, 1975.*

Samelson, H.: **Notes on Lie algebras.** *Van Nostrand, New York, 1969.*

Sharpe, R. W.: **Differential geometry.** *GTM 166. Cartans Generalization of Kleins Erlangen Program, Springer, 1997.*

Wells, R. O. jr.: **Differential analysis on complex manifolds.** *GTM65. Springer New York, 1979.*

Study programme P4M3 Mathematical analysis

Subject-area board

Current composition of the board is at the address `http://mff.cuni.cz/phd/or/p4m3`.

Cooperating institutes

- Institute of Mathematics of the CAS, v.v.i.
  Žitná 25, 115 67 Praha 1
  `http://www.math.cas.cz`

Homepage of the study programme

`http://karlin.mff.cuni.cz/studium/phd/4m3/`.

Offered topics

The topics can be found in SIS at the address `http://mff.cuni.cz/phd/temata/p4m3`.

Provided teaching

Code	Subject	Winter	Summer
NMMA437	**Advanced Differentiation and Integration 1**	2/0 Ex	—

NMMA438	**Advanced Differentiation and Integration 2**	—	2/0 Ex
NMMA433	**Descriptive Set Theory 1**	2/0 Ex	—
NMMA434	**Descriptive Set Theory 2**	—	2/0 Ex
NMMA440	**Differential Equations in Banach Spaces**	—	2/0 Ex
NMMA583	**Qualitative Properties of Weak Solutions to Partial Differential Equations**	2/0 Ex	—
NMMA577	**Quasi-Conformal Mappings 1**	2/0 Ex	—
NMMA578	**Quasi-Conformal Mappings 2**	—	2/0 Ex
NMMA561	**Operator Algebras 1**	2/0 Ex	—
NMMA562	**Operator Algebras 2**	—	2/0 Ex
NMMA403	**Theory of Real Functions 1**	2/0 Ex	—
NMMA404	**Theory of Real Functions 2**	—	2/0 Ex
NMMA461	**Regularity of Navier — Stokes Equations**	0/2 C	0/2 C
NMMA584	**Regularity of Weak Solutions to Partial Differential Equations**	—	0/2 C
NMAA009	**Seminar on Mathematical Analysis**	0/2 C	0/2 C
NMMA454	**Seminar on Function Spaces**	0/2 C	0/2 C
NMMA457	**Seminar on Basic Properties of Function Spaces**	0/2 C	0/2 C
NMMA575	**Topological and Geometric Properties of Convex Sets 1**	2/0 Ex	—
NMMA576	**Topological and Geometric Properties of Convex Sets 2**	—	2/0 Ex
NMMA435	**Topological Methods in Functional Analysis 1**	2/0 Ex	—
NMMA436	**Topological Methods in Functional Analysis 2**	—	2/0 Ex
NMMA565	**Introduction to Approximation Theory 1**	2/0 Ex	—
NMMA566	**Introduction to Approximation Theory 2**	—	2/0 Ex
NMMA533	**Introduction to Interpolation Theory 1**	2/0 Ex	—
NMMA534	**Introduction to Interpolation Theory 2**	—	2/0 Ex
NMMA481	**Selected topics in harmonic analysis 1**	2/0 Ex	—
NMMA482	**Selected topics in harmonic analysis 2**	—	2/0 Ex
NMAG533	**Principles of Harmonic Analysis**	3/1 C+Ex	—
NMAG534	**Non-commutative harmonic analysis**	—	3/1 C+Ex
NMMO623	**Mathematical Methods in Solid State Continuum Mechanics for Ph.D. Students 1**	2/0 Ex	—
NMMO624	**Mathematical Methods in Solid State Continuum Mechanics for Ph.D. Students 2**	—	2/0 Ex
NMMO539	**Mathematical Methods in Mechanics of Non-Newtonian Fluids**	2/0 Ex	—
NMMO535	**Mathematical Methods in Mechanics of Solids**	2/0 Ex	—

NMMO536	**Mathematical Methods in Mechanics of Compressible Fluids**	—	2/0 Ex
NMMO621	**Nonlinear Differential Equations and Inequalities for Ph.D. Students I**	2/0 Ex	—
NMMO622	**Nonlinear Differential Equations and Inequalities for Ph.D. Students II**	—	2/0 Ex
NMMO561	**Regularity of solutions of Navier-Stokes equations**	2/0 Ex	—
NMAG437	**Seminar on Differential Geometry**	0/2 C	0/2 C
NMAG569	**Mathematical Methods of Quantum Field Theory**	0/2 C	0/2 C
NMMO461	**Seminar in Continuum Mechanics**	0/2 C	0/2 C
NMMA452	**Seminar on Partial Differential Equations**	0/2 C	0/2 C
NMMA458	**Seminar on Topology**	0/2 C	0/2 C

List of requirements for taking the state doctoral exam

For the purpose of the state doctoral exam please visit the webpage of the subject-area board `http://karlin.mff.cuni.cz/studium/phd/4m3/` where two lists of topics, denoted List A and List B, can be found.

List A

1. Distribution theory

2. Advanced spectral theory

3. Complex analysis

4. Introduction to abstract harmonic analysis

5. Introduction to the approximation theory

6. Classial harmonic analysis

7. Hausdorff measure and change of variables in an integral

8. Spaces of functions of bounded variation and approximation by smooth functions

9. Qualitative theory of ordinary differential equations

10. Classical potential theory

11. Introduction to the hyperbolic conservation laws

12. Introduction to optimalization theory

13. Sturm-Liouville theory of second-order linear equations

14. Integral equations and the eigenvalue problem

15. Laplace transform

List B

1. Introduction to interpolation theory

2. Topological degree

3. Integral representation on compacts

4. Theory of C-algebras*

5. Descriptive set theory

6. Function spaces

7. Singular integrals

8. Littewood-Payley theory

9. Riesz and Bessel potentials

10. Hardy spaces

11. Finite distortion mappings

12. Isoperimetric inequality

13. Diferentiability of convex functions

14. Introduction to the homogeneization theory

15. Introduction to the theory of stochastic parabolic equations

16. Existence theory for the Navier-Stokes-Fourier system

17. Attractor: structure and dimensional estimates

18. Volterra integral equations

19. Regularity of Navier-Stokes equations

Topics on both lists are of unified extent corresponding approximately to 70-100 pages in a monograph. The supervisor of each student who intends to take the exam will choose one topic from the list A and one topic from the list B. These two topics will be complemented by a third one (of the same extent) according to the supervisor's choice. This third topic might be chosen from one of the lists, or it can be a new topic which (so far) has not been included to the lists. The third topic should be close to the topic of the student's dissertation or his/her field of research.

The supervisor will then apply to the subject-area board for approval of the list of three chosen topics before applying for fixing of the exam date. The subject-area board will assess the appropriateness of the suggested list and decide by acclamation whether or not it gives its approval. When the application was approved, the three topics are considered to be established. The exam then consists of three parts each of those corresponding to one of the topics. If the third topic had not been included to one of the lists before the exam, could be included to one of those on the decision of the subject-area board. More details concerning the lists can be found at `http://karlin.mff.cuni.cz/studium/phd/p4m3/phdzkouska.php`.

Recommended literature

Adams, R.A.: **Sobolev spaces.** *Pure and Applied Mathematics, Vol. 65. Academic Press, 1975.*

Alfsen, E.M.: **Compact convex sets and boundary integrals.** *Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 57. Springer-Verlag, New York-Heidelberg, 1971.*

Amann, H.: **Ordinary differential equations : an introduction to nonlinear analysis.** *De Gruyter, Berlin, 1990.*

Ambrosio, L., Fusco, N., Pallara, D.: **Functions of bounded variation and free discontinuity problems.** *Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 2000.*

Armitage, D.H., Gardiner, S.J.: **Classical potential theory.** *Springer, London, 2001.*

Bennett, C., Sharpley, R.: **Interpolation of Operators.** *Pure and Applied Mathematics, 129. Academic Press, Inc., Boston, MA, 1988.*

Benyamini, Y., Lindenstrauss, J.: **Geometric Nonlinear Functional Analysis, Vol. 1.** *Colloquium Publications Vol 48, Amer. Math. Soc., 2000.*

Bergh, J., Löfström, J.: **Interpolation spaces. An introduction.** *Grundlehren der Mathematischen Wissenschaften, No. 223. Springer-Verlag, Berlin-New York, 1976.*

Bressan, A., Piccoli, B.: **Introduction to the mathematical theory of control.** *AIMS Series on Applied Mathematics Vol 2, AIMS, 2007.*

Chavel, I.: **Isoperimetric inequalities. Differential geometric and analytic perspectives.** *Cambridge Tracts in Mathematics, 145. Cambridge University Press, Cambridge, 2001.*

Cheney, E.W.: **Introduction to approximation theory.** *McGraw-Hill Book Co., New York-Toronto, Ont.-London 1966.*

Deimling, K.: **Nonlinear functional analysis.** *Springer-Verlag, Berlin, 1985.*

DeVore, R.A., Lorentz, G.G.: **Constructive approximation.** *Grundlehren der Mathematischen Wissenschaften 303, Springer-Verlag, Berlin, 1993.*

DiBenedetto, E.: **Partial differential equations.** *Birkhäuser Boston Inc., 1995.*

Evans, L.C.: **Partial differential equations.** *American Mathematical Society, Providence, 2010.*

Evans, L.C., Gariepy, R.F.: **Measure theory and fine properties of functions.** *Studies in Advanced Mathematics. CRC Press, Boca Raton, FL, 1992.*

Folland, B.B.: **A course in abstract harmonic analysis.** *Studies in Advanced Mathematics. CRC Press, Boca Raton, FL, 1995.*

Grafakos, L.: **Classical Fourier Analysis.** *Graduate Texts in Mathematics, 250. Springer, New York, 2009.*

Grafakos, L.: **Modern Fourier Analysis.** *Graduate Texts in Mathematics, 249. Springer, New York, 2008.*

Hartman, Ph.: **Ordinary differential equations.** *S. M. Hartman, Baltimore, Md., 1973.*

Iwaniec, T., Martin, G.: **Geometric Function Theory and Non-linear Analysis.** *Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 2001.*

Kechris, A.S.: **Classical descriptive set theory.** *Graduate Texts in Mathematics, 156. Springer-Verlag, New York, 1995.*

Kufner, A., John, O., Fučík, S.: **Function Spaces.** *Monographs and Textbooks on Mechanics of Solids and Fluids; Noordhoff International Publishing, Leyden; Academia, Praha, 1977.*

Pick, L., Kufner, A., John, O., Fučík, S.: **Function spaces. Vol. 1.** Second revised and extended edition. *De Gruyter Series in Nonlinear Analysis and Applications, 14. Walter de Gruyter & Co., Berlin, 2013.*

Robinson, J.C.: **Infinite-dimensional dynamical systems : an introduction to dissipative parabolic PDEs and the theory of global attractors.** *Cambridge University Press, 2001.*

Rudin, W.: **Functional analysis. Second edition.** *International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., New York, 1991.*

Rudin, W.: **Analýza v reálném a komplexním oboru.** *Academia, Praha, 2003.*

Srivastava, S.M.: **A course on Borel sets.** *Graduate Texts in Mathematics, 180. Springer-Verlag, New York, 1998.*

Stein, E.M.: **Singular Integrals and Differentiability Properties of Functions.** *Princeton Mathematical Series, No. 30 Princeton University Press, Princeton, N.J. 1970.*

Stein, E.M.: **Harmonic Analysis: Real-Variable Methods, Orthogonality, and Oscillatory Integrals.** *Princeton Mathematical Series 43. Princeton University Press, Princeton, NJ, 1993.*

Takesaki, M.: **Theory of operator algebras. I.** *Springer-Verlag, New York-Heidelberg, 1979.*

Widder, D.V.: **The Laplace Transform** *Princeton Mathematical Series Vol 6, Princeton, 1941.*

Ziemer, W.P.: **Weakly differentiable functions. Sobolev spaces and functions of bounded variation.** *Graduate Texts in Mathematics, 120. Springer-Verlag, New York, 1989.*

Study programme P4M6 Computational mathematics

Subject-area board

Current composition of the board is at the address http://mff.cuni.cz/phd/or/p4m6.

Cooperating institutes

- Institute of Computer Science of the CAS, v.v.i.
  Pod Vodárenskou věží 2, 182 07 Praha 8
  http://www.ustavinformatiky.cz/

- Institute of Mathematics of the CAS, v.v.i.
  Žitná 25, 115 67 Praha 1
  http://www.math.cas.cz/

- Institute of Thermomechanics of the CAS, v.v.i.
  Dolejškova 1402/5, 182 00 Praha 8
  http://www.it.cas.cz/

- Institute of Information Theory and Automation of the CAS, v.v.i.
  Pod Vodárenskou věží 4/1143, 182 08 Praha 8
  http://www.utia.cas.cz/

Offered topics

The topics can be found in SIS at the address http://mff.cuni.cz/phd/temata/p4m6.

Provided teaching

Code	Subject	Winter	Summer
NMMO461	**Seminar in Continuum Mechanics**	0/2 C	0/2 C
NMMO533	**Nonlinear Differential Equations and Inequalities 1**	3/1 C+Ex	—
NMMO535	**Mathematical Methods in Mechanics of Solids**	2/0 Ex	—
NMMO536	**Mathematical Methods in Mechanics of Compressible Fluids**	—	2/0 Ex
NMMO537	**Saddle Point Problems and Their Solution**	—	2/2 C+Ex
NMMO539	**Mathematical Methods in Mechanics of Non-Newtonian Fluids**	2/0 Ex	—
NMNV451	**Seminar in Numerical Mathematics**	0/2 C	0/2 C
NMNV461	**Techniques for a posteriori error estimation**	2/0 Ex	—

NMNV462	**Numerical Modelling of Electrical Engineering Problems**	—	2/0 Ex
NMNV463	**Modelling of materials — theory, model reduction and efficient numerical methods**	0/2 C	0/2 C
NMNV464	**A Posteriori Numerical Analysis Based on the Method of Equilibrated Fluxes**	—	2/0 Ex
NMNV468	**Numerical Linear Algebra for Data Science and Informatics**	—	2/2 C+Ex
NMNV561	**Bifurcation Analysis of Dynamical Systems 1**	2/0 Ex	—
NMNV562	**Bifurcation Analysis of Dynamical Systems 2**	—	2/0 Ex
NMNV565	**High-Performance Computing for Computational Science**	2/2 C+Ex	—
NMNV623	**Contemporary Problems in Numerical Mathematics**	0/3 C	0/3 C
NMST442	**Matrix Computations in Statistics**	—	2/2 C+Ex

List of requirements for taking the state doctoral exam

1. Mathematical and functional analysis

Ordinary and partial differential equations, classical and weak solutions. Integral equations. Fourier transformation. Spectral theory of linear operators. Special types of operators, properties. Distributions, Sobolev spaces. Monotone, potential operators. Nonlinear differential equations.

2. Numerical methods

Methods for the solution of systems of linear algebraic equations. Methods for the computation of eigenvalues and eigenvectors of matrices. Methods for the solution of systems of nonlinear algebraic equations. Approximation, interpolation and extrapolation. Minimization and optimization methods. Numerical methods for ordinary differential equations. Numerical integration. Finite difference method for the solution of differential equations. Finite element and finite volume methods. Numerical solution of nonlinear partial differential equations. Multigrid methods.

3. Elective subjects related to the topic of the PhD thesis

Recommended literature

Axelsson, O., Barker, V. A.: **Finite Element Solution of Boundary Value Problems, Theory and Computation.** *Academic Press, New York, 1984.*

Ciarlet, P. G.: **The Finite Element Method for Elliptic Problems.** *North–Holland, Amsterdam, 1978.*

Ciarlet, P. G.: **Linear and Nonlinear Functional Analysis with Applications.** *SIAM, 2013.*

Demmel, J. W.: **Applied Numerical Linear Algebra.** *PA, SIAM, Philadelphia, 1997.*

Dolejší, V., Feistauer, M.: **Discontinuous Galerkin Method - Analysis and Applications to Compressible Flow.** *Springer, 2015.*

Feistauer, M., Felcman, J., Straškraba, I.: **Mathematical and Computational Methods for Compressible Flow.** *Clarendon Press, Oxford, 2003.*

Feistauer, M.: **Mathematical Methods in Fluid Dynamics.** *Longmann Scientific & Technical, Harlow, 1993.*

Fučík, S., Kufner, A.: **Nonlinear Differential Equations.** *Elsevier, Amsterdam, 1980.*

Golub, G. H., Loan van, C. F.: **Matrix Computations.** *4rd ed., Johns Hopkins University Press, Baltimore, 2013.*

Greenbaum, A., Chartier, T. P.: **Numerical Methods: Design, Analysis, and Computer Implementation of Algorithms.** *Princeton University Press, 2012.*

Johnson, C.: **Numerical Solution of Partial Differential Equations by the Finite Element Method.** *Cambridge University Press, Cambridge, 1988.*

Křížek, M., Neittaanmaki, P.: **Mathematical and Numerical Modelling in Electrical Engineering, Theory and Applications.** *Kluwer, Dordrecht, 1996.*

Liesen, J., Strakoš, Z.: **Krylov Subspace Methods, Principles and Analysis.** *Oxford University Press, 2013.*

Málek, J., Strakoš, Z.: **Preconditioning and the Conjugate Gradient Method in the Context of Solving PDEs.** *SIAM Spotlight Series, SIAM, Philadelphia, 2015.*

Meurant, G.: **Computer Solution of Large Linear Systems.** *North-Holland, 1999.*

Nečas, J.: **Introduction to the Theory of Nonlinear Elliptic Equations.** *Teubner, Band 52, 1983.*

Ortega, J. M., Rheinboldt, W. C.: **Iterative Solution of Nonlinear Equations in Several Variables.** *Academic Press, New York, London, 1970.*

Rudin, W.: **Real and Complex Analysis, 3rd Edition.** *McGraw-Hill, New York, 1987.*

Saad, Y.: **Iterative Methods for Sparse Linear Systems.** *PWS Publishing Company, 1996.*

Trefethen, L. N., Bau, D.: **Numerical Linear Algebra.** *SIAM, Philadelphia, 1997.*

Ueberhuber, C. W.: **Numerical Computation 2.** *Springer, Berlin, 1995.*

Yosida, K.: **Functional Analysis.** *Springer Verlag, Berlin, 1980.*

Study programme P4M8 General questions of mathematics and computer science

Subject-area board

Current composition of the board is at the address http://mff.cuni.cz/phd/or/p4m8.

Cooperating institutes

- Institute of Mathematics of the CAS, v.v.i.
  Žitná 25, 115 67 Praha 1
  http://www.math.cas.cz

Offered topics

The topics can be found in SIS at the address http://mff.cuni.cz/phd/temata/p4m8.

Provided teaching

Code	Subject	Winter	Summer
NMUM603	**Mathematics in the ancient times I**	2/0 Ex	—
NMUM604	**Mathematics in the ancient times II**	—	2/0 Ex
NMUM602	**Didactics of Mathematics for Ph.D. Students**	—	2/2 C+Ex
NUMV084	**ICT in Mathematics Teaching I**	0/2 C	—
NUMV085	**ICT in Mathematics Teaching II**	—	0/2 C
NMIN203	**Beginners' course in Mathematica**	0/2 C	—
NMIN264	**Advanced course in Mathematica**	—	0/2 C
NMUM461	**Applications of Mathematics for Teachers**	—	0/2 colloquium
NUMV058	**Greek Mathematical Texts I**	0/2 C	—
NUMV059	**Greek Mathematical Texts II**	—	0/2 C
NUMV101	**Advanced probability for mathematicians**	—	2/0 Ex
NAIL102	**Philosophical problems of Informatics**	0/1 C	0/1 C
NPOZ007	**Philosophical Problems of Physics**	0/1 C	—
NPGR020	**Geometry for Computer Graphics**	—	2/0 Ex
NPGR021	**Geometric Modelling**	2/2 C+Ex	—
NMUM365	**Seminar in combinatorics and graph theory**	—	0/2 C

Programme description

The programme is intended mainly for graduates of education-oriented study programmes involving mathematics or computer science for high-school teachers, and for university teachers of mathematics, computer science, and didactics of these subjects.

A necessary condition for admission into this programme is an excellent knowledge of high-school mathematics, as well as basic university courses of mathematics.

The programme has three branches:

1. Elementary mathematics
2. History of mathematics/computer science
3. Teaching of mathematics/computer science

The branch *Elementary mathematics* offers a number of ways for increasing the level of mathematical culture of high-school teachers, and provides better qualification for teaching in general, especially for working with gifted students. Elementary mathematics encompasses classical mathematical disciplines related to high-school mathematics and education-oriented study programmes at universities, and provides a suitable extension of these subjects. Its goals include keeping the historical continuity of mathematics, and strengthening the respect towards traditional mathematical values.

In the branch *History of mathematics/computer science*, attention is paid mainly to the 19th and 20th century, and Czech mathematics/computer science, including various biographical and bibliographic aspects. History of mathematics is closely related to the problems of teaching, because the development of mathematics has been influenced by textbooks and teachers.

The branch *Teaching of mathematics/computer science* is primarily intended for those who already have a teaching experience. A dissertation thesis might include educational texts, collections of problems etc., including methodical guidelines and analysis of difficult parts; resulting materials should be tested in class.

List of requirements for taking the state doctoral exam

The nature of the state doctoral exam stems from the fact that the goal of this programme is to educate a mathematician/computer scientist with a general broad insight, who is not being purposely prepared for the scientific work in a certain narrow area, but his/her erudition will allow him/her to create high-quality educational texts, who is aware of modern teaching methods, possesses good orientation in the scholarly literature related to his/her field of interest, and regularly publishes his/her own findings.

The doctoral exam consists of three parts, mathematics/computer science, history of mathematics/computer science, and teaching of mathematics/computer science. Since the topics studied in this programme are quite diverse and cover various branches of mathematics/computer science, it is impossible to have a unified list of requirements for all students. Only a general framework is provided, and the requirements will be made precise by each student's supervisor and the doctoral exam committee.

Requirements

1. Mathematics/computer science

It is assumed that the student has mastered all material required for the master's state exam in education-oriented study programmes at Charles University, Faculty of Mathematics and Physics. Student must be able to show a good understanding of the connections between high-school and university topics, possess orientation in basic textbook literature, and be able to prepare and teach basic courses in mathematics/computer science.

Additional requirements will be specified by student's supervisor and the doctoral exam committee (at least several chapters of a scholarly text, whose content is not part of standard university courses). These requirements must go significantly beyond the level specified in the previous paragraph.

2. History of mathematics/computer science

It is assumed that the student understands the essence of historical topics, and possesses orientation in the development of various disciplines. Deeper knowledge of history is required for topics related to student's research.

Student's supervisor and the doctoral exam committee will specify at least 200 pages of scholarly literature.

3. Teaching of mathematics/computer science

Assumed is a good orientation in methodics, didactics, and problem solving methods in mathematics/computer science.

Student's supervisor and the doctoral exam committee will specify at least 100 pages of scholarly literature.

4. Broadening horizons

It is expected that the student shows interest in his/her field of study, follows scholarly journals and literature dealing with mathematics/computer science and their teaching, knows how to cite relevant works and search for bibliographic data, is familiar with databases of scientific works, digital repositories, etc.

Recommended literature

Alten, H.-W., Naini, A. D., Folkerts, M., Schlosser, H., Schlote, K.-H., Wußing, H.: **4000 Jahre Algebra.** *Springer–Verlag, Berlin–Heidelberg, 2008.*

Anglin, W. S., Lambek, J.: **The Heritage of Thales.** *Springer, New York, 1995.*

Anglin, W. S.: **Mathematics – A Concise History and Philosophy.** *Springer, New York, 1994.*

Boyer, C. B., Merzbach, U. C: **A History of Mathematics.** *3rd ed., John Wiley & Sons, Hoboken, New Jersey, 2011.*

Chabert, J.-L.: **A History of Algorithms – From the Pebble to the Microchip.** *Springer–Verlag, Berlin–Heidelberg, 1999.*

Cooke, R.: **The History of Mathematics, A Brief Course.** *2nd ed., John Wiley & Sons, Hoboken, New Jersey, 2005.*

Dieudonné, J. (ed.): **Abrégé d'histoire des mathématiques 1700–1900.** *Paris 1978;* German version: **Geschichte der Mathematik 1700–1900.** *Vieweg, Braunschweig, 1985.*

Edwards, C. H.: **The Historical Development of the Calculus.** *Springer–Verlag, New York, 1979.*

Eves, H. W: **An Introduction to the History of Mathematics.** *6th ed., Saunders College Publishing, Philadelphia, 1990.*

Gericke, H.: **Mathematik in Antike, Orient und Abendland.** *Fourier Verlag, Wiesbaden, 2003.*

Herman, J., Kučera, R., Šimša, J.: **Equations and Inequalities. Elementary Problems and Theorems in Algebra and Number Theory.** *Springer, 2000.*

Herman, J., Kučera, R., Šimša, J.: **Counting and Configurations. Problems in Combinatorics, Arithmetic, and Geometry.** *Springer, 2003.*

Katz, V. J.: **A History of Mathematics. An Introduction.** *3rd ed., Pearson, 2008.*

Kline, M.: **Mathematical Thought from Ancient to Modern Times.** *Oxford University Press, New York, 1990.*

Larson, L. C.: **Problem-Solving Through Problems.** *Springer, 1983.*

Metropolis, N., Howlett, J., Rota, G.-C.: **A History of Computing in the Twentieth Century.** *Academic Press, New York, 1980.*

Naumann, F.: **Vom Abakus zum Internet: Die Geschichte der Informatik.** *Primus Verlag, 2001.*

Priestley, W. M.: **Calculus: An Historical Approach.** *Springer–Verlag, New York, 1979.*

Scriba, C. J., Schreiber, P.: **5000 Jahre Geometrie.** *Springer–Verlag, Berlin–Heidelberg, 2005;* English version: **5000 Years of Geometry.***Birkhäuser, Basel, 2015.*

Scholz, E. (Hrsg.): **Geschichte der Algebra, Eine Einführung.** *Wissenschaftsverlag, Mannheim–Wien–Zürich, 1990.*

Sonar, T.: **3000 Jahre Analysis.** *Springer–Verlag, Berlin–Heidelberg, 2011;* English version: **3000 Years of Analysis.***Springer Nature Switzerland AG, 2021.*

Stillwell, J.: **Mathematics and Its History.** *3rd ed., Springer-Verlag, New York–Dordrecht–Heidelberg–London, 2010.*

van der Waerden, B. L.: **A History of Algebra, From al-Khwárizmí to Emmy Noether.** *Springer–Verlag, Berlin, 1985.*

Williams, M. R.: **A History of Computing Technology.** *2nd ed., IEEE Computer Society Press, Los Alamitos, California, 1997.*

Wußing, H.: **6000 Jahre Mathematik I, II.** *Springer–Verlag, Berlin–Heidelberg, 2008, 2009.*

Yushkevich, A. P.: **History of Mathematics in the Middle Ages** (Russian). *Moscow, 1961.*

Study programme P4M9 Probability and statistics, econometrics and financial mathematics

Subject-area board

Current composition of the board is at the address `http://mff.cuni.cz/phd/or/p4m9`.

Cooperating institutes

- Institute of Information Theory and Automation of the CAS, v.v.i.
  Pod Vodárenskou věží 4/1143, 182 08 Praha 8
  `http://www.utia.cas.cz/`

Offered topics

The topics can be found in SIS at the address `http://mff.cuni.cz/phd/temata/p4m9`.

Provided teaching

Code	Subject	Winter	Summer
NMSA600	**Colloquium of the Department of Probability and Mathematical Statistics**	0/1 C	0/1 C
NMSA601	**Specialized seminar in probability and mathematical statistics**	0/2 C	0/2 C
NMEK613	**Stochastic Modelling in Economics and Finance**	0/2 C	0/2 C
NMTP613	**Seminar on Probability for Ph.D. Students I**	0/2 C	—
NMTP614	**Seminar on Probability for Ph.D. Students II**	—	0/2 C
NMST611	**Advanced Statistical Seminar**	0/1 C	0/1 C
NMTP611	**Seminar on Stochastic Evolution Equations**	0/2 C	0/2 C
NMAG467	**Seminar on Stochastic Geometry**	0/1 C	0/1 C
NMEK615	**Stochastic Programming and Approximation**	0/2 C	0/2 C
NMSA602	**Advanced topics of the field**	2/0 Ex	—
NMSA603	**Advanced topics of the field**	—	2/0 Ex
NMST603	**Modern methods of mathematical statistics**	2/0 Ex	—
NMEK603	**Optimization and variational analysis**	2/0 Ex	2/0 Ex
NMFM601	**Some topics on insurance and financial mathematics**	2/0 Ex	—
NMTP602	**Selected topics in spatial modeling**	—	2/0 Ex
NMFM612	**Advanced Topics on Risk Theory**	—	2/0 Ex
NMST605	**Advanced Course in Time Series**	2/0 Ex	—
NMST535	**Simulation Methods**	—	2/2 C+Ex
NMFM614	**Advanced Topics on Financial Mathematics**	—	2/0 Ex
NMTP604	**Advanced Theory of Stochastic Differential Equations**	—	2/0 Ex
NMTP432	**Stochastic Analysis**	—	4/2 C+Ex
NMEK605	**Chapters on modern optimization and equilibria**	2/0 Ex	—
NMEK606	**Chapters on modern optimization and equilibria**	—	2/0 Ex
NMFM611	**Advanced Topics on Non-life Actuarial Mathematics**	2/0 Ex	—
NMFM602	**Mathematical methods in the solvency management and in the financial reporting of insurance companies**	—	2/0 Ex

NMST604	**Robust statistics and econometrics – regression analysis in a bit alternative perspective**	—	2/0 Ex
NMTP612	**Interacting Particle Systems**	—	2/0 Ex
NMEK617	**Prospect Theory**	—	2/0 Ex

List of requirements for taking the state doctoral exam

The exam consists of three parts, the first part is taken from topics I. or II. below. The second part is chosen from I., II., III. or IV., but this choice cannot coincide with the choice in the first part. The third part is related to the topic of dissertation.

I. Probability and stochastic processes.

Extreme value theory, large deviation theory, reliability theory. Invariance principles, ergodic theory. Markov processes, martingales, stationary processes. Spatial modelling, stochastic geometry, complex systems. Stochastic analysis, stochastic differential equations.

II. Mathematical statistics.

Estimation theory and hypotheses testing, loss and risk functions, multivariate analysis, regression, sampling theory, robust and non-parametric methods, bayesian and sequential analysis, spatial statistics, computational statistics, simulation methods, survival analysis.

III. Econometrics and operational research.

Econometric models, time series. Optimization in finite-dimensional spaces. Convex and variational analysis. Integer, nonlinear, parametric, dynamic and stochastic programming. Stability, analysis of results. Game and oligopol theory. Operational research. Utility theory, micro- and macroeconomic models.

IV. Financial and insurance mathematics.

Stochastic financial models, application to securities and derivatives. Risk management, portfolio, hedging instruments, yield curves. Life tables and their construction. Credibility theory, Bayesian methods, insurance tariffs, estimation of structural parameters. Risk modeling, ruin theory, economic capital, insurance companies accounting.

Recommended literature

I. Probability and stochastic processes

Applebaum, D.: **Lévy Processes and Stochastic Calculus, 2nd Edition.** *Cambridge University Press, Cambridge, 2009.*

Billingsley, P.: **Convergence of Probability Measures.** *Wiley, New York, 1999.*

Den Hollander, F.: **Large deviations.** *Fields Institute Monographs 14. Providence, RI: AMS, 2000.*

Friedli, S., Velenik, Y.: **Statistical mechanics of lattice systems. A concrete mathematical introduction.** *Cambridge University Press, Cambridge, 2018.*

van der Hofstad, R.: **Random graphs and complex networks. Vol. 1.** *Cambridge Series in Statistical and Probabilistic Mathematics 43. Cambridge University Press, Cambridge, 2017.*

Liggett, T.M.: **Stochastic interacting systems: contact, voter and exclusion processes.** *Grundlehren der Mathematischen Wissenschaften 324. Springer, Berlin, 1999.*

Møller J., Waagepetersen R.: **Statistical Inference and Simulation for Spatial Point Processes.** *Chapman & Hall/CRC, Boca Raton, 2004.*

Nualart D.: **The Malliavin Calculus and Related Topics.** *Springer-Verlag, 2006.*

Oksendal B.: **Stochastic Differential Equations.** *Springer, Heidelberg, 2003.*

Rachev, S., Klebanov, L.B., Stoyanov S.V., Fabozzi, F.J.: **The Methods of Distances in the Theory of Probability and Statistics.** *Springer, New York, 2013.*

Schneider R., Weil, W.: **Stochastic and Integral Geometry.** *Springer, Berlin, 2008.*

II. Mathematical statistics

Bickel, P., Doksum, K.: **Mathematical Statistics: Basic Ideas and Selected Topics.** *Chapman & Hall/CRC, Boca Raton, 2015.*

Bühlmann, H., Gisler, A.: **A Course in Credibility Theory and its Applications.** *Springer-Verlag, Berlin–Heidelberg, 2005.*

Embrechts, P., Klüppelberg, C., Mikosch, T.: **Modelling Extremal Events. For Insurance and Finance.** *Springer-Verlag, Berlin–Heidelberg, 1997.*

Hájek, J., Šidák, Z., Sen, P.K.: **Theory of Rank Tests.** *Academic Press, Orlando, 1999.*

Jurečková, J., Sen, P.K., Picek, J.: **Methodology in Robust and Nonparametric Statistics.** *Chapman & Hall/CRC, Boca Raton, 2013.*

Lehmann, E.L.: **Testing Statistical Hypothesis.** *Chapman & Hall, New York, 1993.*

Lehmann, E.L.: **Theory of Point Estimation.** *Wadsworth & Brook/Cole, Pacific Grove, 1991.*

Sen, P.K., Singer, J.M., Pedroso de Lima: **From Finite Sample to Asymptotic Methods in Statistics.** *Cambridge University Press, Cambridge, 2009.*

Serfling, R.J.: **Approximation Theorems of Mathematical Statistics.** *Wiley, New York, 2002.*

Shorack, G.R.: **Probability for Statisticians.** *Springer–Verlag, New York, 2000.*

Vaart, A.: **Weak Convergence and Empirical Processes: With Applications to Statistics.** *Springer, Heidelberg, 1996.*

III. Econometrics and operational research

Bazaraa, M.S., Sherali, H.D., Shetty, C.M.: **Nonlinear Programming: Theory and Algorithms.** *Wiley, New York, 2006.*

Bertsekas, D.P.: **Dynamic Programming and Optimal Control, 3rd Edition.** *Athena Scientific, Massachusetts, 2005.*

Dupačová, J.: **Portfolio Optimization and Risk Management.** *Osaka University Press, Osaka, 2009.*

Davidson, J.: **Stochastic Limit Theory.** *Advanced Texts in Econometrics. Oxford University Press, Oxford, 1994.*

Fan, J., Yao, Q.: **Nonlinear Time Series.** *Springer, New York, 2003.*

Hamilton, J.D.: **Time Series Analysis.** *Princeton University Press, Princeton, 1994.*

Mendelson, E.: **Introducing Game Theory and Its Applications.** *Chapman & Hall/CRC, Boca Raton, 2004.*

McNeil, A.J., Frey, R., Embrechts, P.: **Quantitative Risk Management.** *Princeton University Press, Princeton, 2005.*

Rockafellar, R.T., Wets, R.J.: **Variational Analysis.** *Springer-Verlag, Berlin, 1998.*

Shapiro, A., Dentcheva, D., Ruszczyński, A.: **Lectures on Stochastic Programming, Modeling and Theory.** *MPS-SIAM Series on Optimization, 2009.*

Wolsey, L.A., Nemhauser, G.L.: **Integer and Combinatorial Optimization.** *Wiley, New York, 1999.*

IV. Financial and insurance mathematics

Booth, P. et al.: **Modern Actuarial Theory and Practice.** *Chapman & Hall/CRC, London, 2005.*

Cipra, T.: **Finanční ekonometrie.** (in Czech) *Ekopress, Praha, 2013.*

Cipra, T.: **Financial and Insurance Formulas.** *Springer, Berlin, 2010.*

Cipra, T.: **Time Series in Finance and Economics.** *Springer, Cham, 2020.*

Denuit, M. et al.: **Actuarial Theory for Dependent Risks.** *Wiley, Chichester, 2005.*

Föllmer, H., Schied, A: **Stochastic Finance. An Introduction in Discrete Time.** *de Gruyter, Berlin, 2002.*

Shreve, S.: **Stochastic Calculus for Finance I: The Binomial Asset Pricing Model.** *Springer Science & Business Media, 2005.*

Shreve, S.: **Stochastic Calculus for Finance II: Continuous-Time Models.** *Springer Science & Business Media, 2004.*

Witzany, J.: **Credit Risk Management: Pricing, Measurement, and Modeling.** *Springer, Cham, 2017.*

Witzany, J.: **Derivatives.** *Springer International Publishing, 2020.*

Wüthrich, M.V., Merz, M.: **Financial Modeling, Actuarial Valuation and Solvency in Insurance.** *Springer, Heidelberg, 2013.*