

GRUPPO DI RICERCA

Strutture algebriche: aspetti di teoria dei gruppi e di teoria dei modelli, e interazioni con la crittografia e la didattica della matematica

1. DATI IDENTIFICATIVI DEL GRUPPO DI RICERCA

Categorie ERC	PE1
Settore Scientifico Disciplinare	MATH-01/A MATH-01/B MATH-02/A
Parole Chiave (Keywords)	Model Theory, Group Theory, Group-based Cryptography, Students' logical-deductive skills

2. COMPOSIZIONE E COORDINAMENTO

Responsabile Scientifico / Coordinatore:

- **Nome e Cognome:** Paola D'Aquino
- **Qualifica:** Professore Ordinario
- **Email:** paola.daquino@unicampania.it
- **Link Orcid Personale** 0000-0003-4607-3689

Componenti del Gruppo:

1. **Alessio Russo** – Professore ordinario/Link Orcid Personal: 000-0001-6109-2680
2. **Antonio Tortora** – Professore associato/ Link Orcid Personale 0000-0002-4825-1672
3. **Umberto Dello Iacono** – Professore Associato / Link Orcid Personale: 0000-0003-0224-1046
4. **Massimiliano Di Matteo** – Dottorando
5. **Bernardo Giuseppe Di Siena** - Dottorando
6. **Davide Pantaleoni** – Dottorando
7. **Carmine Mirra** – Dottorando

3. ATTIVITÀ SCIENTIFICA E NETWORK

Breve Descrizione delle linee di ricerca:

- **Finiteness conditions in generalized solvable groups, automorphisms groups, subgroup embedding properties.**
- **On algebraic variants of the Learning With Errors Problem and their applications to Cryptography:** It is well-known that there are several efficient algorithms for solving a system of linear equations. However, if we add a small *error* to the constant terms of the system, finding the set of solutions of the original system might become a very hard problem: this is the so-called Learning With Errors problem introduced by Oded Regev in 2009. The problem can be reformulated in terms of different algebraic structures. Some generalizations of LWE were recently published, in order to extend the problem to non-abelian groups. We plan to examine the properties of various groups in order to determine the most suitable one for this problem and to investigate its potential applications.
- **Teoria dei modelli:** Analisi model-teoretica di strutture algebriche. Vengono utilizzati strumenti di logica matematica, ed in particolare di teoria dei modelli, per lo studio di strutture algebriche come anelli esponenziali, campi con valutazioni e numeri p-adici. Risultati di teoria della valutazione sono di supporto per analizzare anelli quozienti di modelli dell'Aritmetica di Peano
- **Interactions between logic and mathematics education.** The aim of this research is to explore the relationship between the manipulation of language objects and the development of logic-deductive skills, through didactic experiments, concerning the assertive aspects of language and the construction of axiomatic systems and deductive chains. A crucial point is the use of digital artifacts, specifically designed and implemented for these activities.

Collaborazioni Nazionali ed Internazionali:

- **Nazionali:** Università di Firenze, Università di Napoli Federico II, Università di Salerno
- **Internazionali:** University of Edinburgh, University of Konstanz, City University of New York

4. PROGETTI, BREVETTI E PUBBLICAZIONI

Principali Progetti di Ricerca e Brevetti:

- Models, sets and classifications – PRIN 2022 – responsabile unità: **P. D'Aquino**

- Functional Encryption per cifrature per cloud – 2023/2025 - responsabili unità: **A. Tortora, F. Zullo**

Principali Pubblicazioni Recenti:

1. **P. D'Aquino**, J. Derakhshan and A. Macintyre *Truncations of ordered abelian groups*, **Algebra Universalis**, 2021.
DOI: <https://link.springer.com/article/10.1007/s00012-021-00717-6>
2. **P. D'Aquino**, A. Fornasiero and G. Terzo, *A weak version of the strong exponential closure*, **Israel Journal of Mathematics**, 2021.
DOI: <https://doi.org/10.1007/s11856-021-2141-1>
3. **P. D'Aquino** and A. Macintyre *Commutative unital rings elementarily equivalent to prescribed product rings*, **Fundamenta Mathematicae**, 2023.
DOI: 10.4064/fm232-8-2023
4. **P. D'Aquino**, A. Fornasiero and G. Terzo, *E-ideals in exponential polynomials rings*, **Communications in Algebra**, 2025.
DOI: 10.1080/00927872.2025.2486395.
5. M. Brescia and **A. Russo**, *On cyclic automorphisms of a group*, *J. Algebra Appl.*, 20 (10) (2021).
6. M. Brescia and **A. Russo**, *On the pronorm of a group*, *Bull. Austr. Math. Soc.*, 104 (2) (2021), 287-294.
7. M. Brescia and **A. Russo**, *On groups in which many automorphisms are cyclic*, *Mathematics*, 10 (2) (2022), 262.
8. M. Brescia, M. Ferrara and **A. Russo**, *On the autocentral series of a group*, *Adv. Group Theory Appl.*, 19 (2024), 177-189.
9. F. de Giovanni, L. A. Kurdachenko and **A. Russo**, *Groups satisfying the minimal condition on subgroups which are not transitively normal*, *Rend. Circ. Mat. Palermo*, 71 (1) (2022), 397-405.
10. F. de Giovanni, L. A. Kurdachenko and **A. Russo**, *Groups with pronormal deviation*, *J. Algebra*, 613 (2023), 32-45.
11. F. de Giovanni, L. A. Kurdachenko and **A. Russo**, *Groups with subnormal deviation*, *Mathematics*, 11 (2023), 26-35.
12. **A. Russo**, *On the central kernel of a group*, *Bull. Austr. Math. Soc.*, 108 (2023), 283-289.
13. **A. Russo**, M. Viscusi, *Central endomorphisms of groups and radical rings*, *Adv. Group Theory Appl.*, 17 (2023), 129-141.
14. **A. Russo**, M. Viscusi, *Groups with many normal subgroups*, *Int. J. Group Theory*, 14 (1)

(2025), 19-23.

15. **A. Russo**, M. Viscusi, *On groups with many subgroups satisfying a transitive normality relation*, Note Mat., 44 (1) (2024), 45-51.
16. S. Marrone, **A. Tortora**, E. Bellini, A. Maione and M. Raimondo, *Development of a testbed for fully homomorphic encryption solutions*, 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 206-211.
17. C. Monetta and **A. Tortora**, *The multiple conjugacy search problem in virtually nilpotent polycyclic groups*, Adv. Group Theory Apps. 13 (2022), 61-70.
18. D. Kahrobaei, **A. Tortora** and M. Tota, *A closer look at the multilinear cryptography using nilpotent groups*, Int. J. Comput. Math - Comput. Syst. Theory, 7 no. 1 (2022), 63-67.
19. M. Ferrara, **A. Tortora** and M. Tota, *A data aggregation protocol based on TFHE*, Int. J. Comput. Math - Comput. Syst. Theory, 9 no. 4 (2024), 243-252.
20. M. Ferrara, **A. Tortora** and M. Tota, *An overview of torus fully homomorphic encryption*, Int. J. Group Theory, 14 no. 2 (2025), 59--73.
21. V. Grazian, **A. Tortora** and M. Tota, *For what algebraic systems does a useful privacy homomorphism exist?*, AIMS Mathematics, 10 no. 4 (2025), 9539-9562.
22. **U. Dello Iacono**, *From argumentation to proof in geometry within a collaborative computer-based environment*. Digital Experiences in Mathematics Education, 7(3) (2021), 395-426. <https://doi.org/10.1007/s40751-021-00090-y>