CURRICULUM VITÆ ET STUDIORUM

ANDREA CARANTI

Born 2 May 1952 in Rome, Italy
Three children

Current position

Full Professor of Algebra since 9 April 1987

Academic Career

Laurea in Matematica at Università degli Studi di Roma "La Sapienza", 28 February 1975 (A. Machì)
Borsa CNR laureando, Roma, 1974–1975 (Machì)
Borsa CNR laureato, Padova, 1976 (G. Zacher)
Servizio militare, Firenze e Padova, 1976–1977
Borsa CNR laureato, Trento, 1977–1979 (Zacher)
Assistant Professor of Algebra, Trento, 1979–1985
Lecturer, Geometria II, Trento, 1979–1981
Lecturer, Algebra, Trento, 1981–1985
Borsa CNR-NATO, Würzburg (Germany), 1982 (H. Heineken)
Associate Professor of Algebra, Trento, 1985–1987
Visiting Fellow, Erlangen (Germany), Wintersemester 1985–1986
Full Professor of Algebra, Trento, 1987–...
Visiting Fellow, ANU Canberra, September 1996, CNR (Italy) mobility grant
Visiting Fellow, ANU Canberra, December 1996 (CNR–GNSAGA)
Visiting Fellow, ANU Canberra, December 1999 (INdAM–GNSAGA)

Academic Appointments

Dean of Undergraduate Studies, Trento, 1992–95
Dean of Graduate Studies, Trento, 1997–2000
Dean of Undergraduate Studies, Trento, 1998–2001
Member of the Board of Opera Universitaria, Trento, 2001–2008
Dean of Undergraduate Studies, Trento, 2008–2010
Rector's deputy for disabilities, Trento, 2010–2011
Dean of the Faculty of Science, Trento, 2011–2012
Member of the Senate, Trento, 2012–2013
Member of Nucleo di Valutazione, Trento, 2013–2015
Chair, Department of Mathematics, Trento, 2015–...

Updated: 6 April 2018.

University Courses given

Algebra B, Trento, 2016/17
Group Theory, Trento, 2015–18
Algebra A, Trento, 2015/16, 2017/18
Algebra, Trento, 2006–16
Algebra, Trento, 1999/2000 (U.D. 1), 2000/01 (U.D. 1, 2), 2001/02 (U.D. 2), 2002/03 (U.D. 1), 2003/04 (U.D. 2), 2004/05 (U.D. 1, 2), 2005/06 (U.D. 2)
Algebra, Trento, 1981–85, 1986/87, 1988/89, 1990/91, 1992–95, 1996/97
Geometria e Algebra Lineare, Trento, 2013/14
Finite Fields and Symmetric Cryptography, Trento, 2005–09
Galois Theory, Trento, 1985/86, 1987/88, 1989/90, 1991–93, 1994/95 (1° modulo), 1996–99 (1° modulo), 2002–06
Number Theory and Cryptography, Trento, 2000/01, 2004/05
Elementary Mathematics from an Advanced Standpoint, Trento, 2002–04
Introductory Mathematics for Economics, Trento, 1997–00, 2001/02
Geometria II, Trento, 1979–1981

Advanced Courses given

Algebra (Group algebras), Istituto Nazionale di Alta Matematica, Roma, March-May 1989
Analyticity and growth of pro-p groups, NATO Advanced Study Institute "Generators and Relations in Groups and Geometries", Il Ciocco, April 1990
Computing in groups of prime-power order, Summer School on Computational Group Theory, Politecnico, Budapest, August-September 1992
Algebra (Representation theory of algebras), Scuola Matematica Interuniversitaria, Perugia, August 1990
Algebra (Lie algebras), Scuola Matematica Interuniversitaria, Cortona, July/August 1996

Italian Projects

PRIN 1994, "Teoria dei gruppi ed algebra non commutativa", local unit head
PRIN 1995, "Teoria dei gruppi, algebra non commutativa e logica matematica", local unit head
PRIN 1996, "Teoria dei gruppi, algebra non commutativa e teoria dei modelli", local unit head
PRIN 1999–2000, "Algebre di Lie graduate e pro-p-gruppi di ampiezza finita", head
PRIN 2001–2002, "Algebre di Lie graduate e pro-p-gruppi di ampiezza finita, algebre loop, e derivazioni", head
PRIN 2003–2005, "Algebre di Lie graduate e pro-p-gruppi: rappresentazioni, periodicità e derivazioni", head
PRIN 2006–2008, "Anelli e algebre di Lie. Gruppi. Crittografia", local unit head

PRIN 2008 (2010–2012), "Algebre di Lie, gruppi, metodi computazionali, identità combinatorie, derivazioni", local unit head

PRIN 2015 (2017–2020), "Group theory and applications"

Project "Dipartimenti di Eccellenza", MIUR–Italy, proponent as Head of Department, 6 635 000 EUR

European Projects

Tempus Project "Using Computer Algebra", 1993–1996

Human Capital and Mobility Project "Computational Group Theory", 1993–1996

Invited Talks

Linz (Austria), Gastvortrag, March 1985
Aachen (Germany), Gastvortrag, December 1985
Würzburg (Germany), Oberseminar, January 1986
Erlangen (Germany), Kolloquium, February 1986
Napoli, April 1986
Padova, November 1986
Genova, June 1987
Padova, February 1988
Bialystok (Poland), June 1988
Trieste, GNSAGA Workshop, October 1988
Lecce, May 1990
Padova, January 1991
p-groups, Oberwolfach, 1992
Padova, November 1993
Milano, Seminario Matematico e Fisico, aprile 1994
Eindhoven (The Netherlands), October 1994
Aachen (Germany), Colloquium, January 1995
ANU Canberra, Colloquium, September 1996
Miniconference, ANU Canberra, September 1996
DAG-DAY, Eindhoven (The Netherlands), October 1996
Group Theory Workshop, Napoli, March 1997
London Mathematical Society Symposium on Pro-p-groups and Related Topics, Durham, July 1997
One Hour Invited Talk, Groups St Andrews in Bath, July-August 1997
Firenze, Group Theory Workshop, February 1998
Freiburg, Colloquium, June 1998
EICMA, Milano, September 1998
SunCAGE '98, Caserta, November 1998
Padova, January 1999
Group Theory Workshop, Padova, February 1999
Minicourse at the Research Seminar on Groups, Combinatorics and Computer Science, Oulu, Finlandia, August 1999
Group Theory and Computation, Sydney, November 1999

Group Theory Workshop, Milano Bicocca, January 2000
Asymptotic Group Theory Conference, Jerusalem, May 2000
Group Theory Workshop, Lecce, December 2000
One Hour Invited Talk, Groups St Andrews in Oxford, July-August 2001
Accepted Poster, Coding and Cryptography, Milan Research centre for Industrial and Applied Mathematics (MIRIAM) Workshop, Milano, December 2003
Proseminar, Würzburg, November 2004
Workshop on Coding and Cryptography, Cork, May 2005
Incontro di Algebra Commutativa e Computazionale, Genova, November 2005
Science Festival, Genova, November 2006
Galway, January 2007
Group Theory Conference, Ischia, April 2008
Edinburgh Mathematical Society Meeting, St Andrews, 22 May 2009
Workshop on block ciphers and their security, Trento, 4 December 2009
Groups, Algebras and Algorithms, 18 March 2010, Eindhoven University of Technology
Universität Basel, 19 May 2010
Advances in Group Theory and Applications, Porto Cesareo, 7–10 June 2011
Bergwinter der Universität Innsbruck, Obergurgl, Austria, 16 April 2014
Scriver veloce. Sistemi tachigrafici dall'antichità a Twitter, Rovereto, 23 May 2014
UMI Conference, Siena, 2015
Gruppen und topologische Gruppen Wüzburg, Germany, 13–14 May 2016
Groups, Rings, and Their Automorphisms, a Conference in Honour of Evgeny Khukhro, Lincoln, UK, 31 August–2 September 2016
Ischia Group Theory 2018, 19–24 March 2018

Other Talks

GNSAGA Workshop, L'Aquila, 1976
GNSAGA Workshop, Ferrara, 1978
GNSAGA Workshop, Modena, 1981
CIRM Workshop Trento, 1982
UMI Conference, Perugia 1983
Group Theory Workshop, Padova, 1984
GNSAGA Workshop, Torino 1984
Groups '85, St Andrews, 1985
Groups '89, St Andrews, 1989
Mal'cev Conference, Novosibirsk, 1989
CIRM Workshop Trento, 1993
Arbeitstagung "Gruppen und topologische Gruppen", Krems, Austria, June 1994
CIRM Workshop "Linear Groups", Levico, September 1995
GNSAGA Workshop "Computation in Algebra and Geometry", L'Aquila, October 1996
Group Theory Workshop, Udine, November 2003

Advances in Group Theory and Applications, Lecce, 5–8 September 2017

Organizer of Conferences and Workshops

Algebra Minicourse, Trento, 1980
Group Theory Workshop, Trento, 1984
Arbeitstagung "Gruppen und topologische Gruppen", Trento, June 1986
A short course in computational group theory, Trento, May 1988
Arbeitstagung "Gruppen und topologische Gruppen", Trento, June 1990
Profinite groups, INdAM, Cortona, September/October 1991
Nilpotent and Soluble Quotient Methods (with M.F. Newman), Trento, June 1998
Finitely-presented groups: questions and algorithms (with E.A. O'Brien, M.F. Newman), Trento, July 2001
Lie Algebras, their Classification and Applications (with Bettina Eick, Jörg Feldvoss, Marco Costantini), Braunschweig, May 2004
Lie Algebras, their Classification and Applications (with Bettina Eick, Willem de Graaf, Carlo Scoppola, Csaba Schneider) Trento, July 2005
The 11th Rhine Workshop on Computer Algebra, Levico Terme, June 2008
Group Theory in Trento, 7–8 June 2012
Gruppen und topologische Gruppen, Trento, 16–17 June 2017

Conferences and Workshops attended

Group theory, CIRM, Trento, 1979
Arbeitstagung "Gruppen und topologische Gruppen", Innsbruck 1982, München 1982, Freiburg 1983, Erlangen 1983, München 1984, Freiburg 1985, Erlangen 1985, München 1986, Erlangen 1987, Erlangen 1989, Würzburg 1991, Freiburg 1992, München 1993, Würzburg 1995, Würzburg 1996
Combinatorial Geometry, La Mendola, 1983
Eurocal '85, Linz (Austria), April 1985
International Colloquium on Group Theory, Debrecen, 1985
Gruppentheorie, Oberwolfach, September 1985
International Conference in Group Theory, Brixen/Bressanone, 1986
CAMASA '86, Pavia, 1986
Computational Group Theory, Oberwolfach, May 1988
First International Symposium in Algebra and Number Theory, Hong Kong, August 1988
Groups - Korea 1988, Pusan, August 1988
International Conference in Group Theory, Brixen/Bressanone, June 1989
Algebra Workshop, Warwick, March 1991
Computational Group Theory, Oberwolfach, 1992
Groups '93, Galway, August 1993
Computational Group Theory, Oberwolfach, 1997
Computational Group Theory, Columbus, OH, June 1999
Group Theory Workshop, Brescia, October 2001
Group Theory Workshop, Salerno, October 2002

Computational Group Theory, Columbus, OH, March 2003
Group theory meeting, Padova, September 2008
Lie Methods in Group Theory, Trento, November 2008
Topics in Algebra, Milano Bicocca, 13–15 May 2009
Group Theory Conference, Ischia, April 2010
Group Theory Conference, Ischia, March 2012
Advances in Group Theory and Applications, Porto Cesareo, 10–14 June 2013
Group Theory Conference, Ischia, April 2014
Advances in Group Theory and Applications, Porto Cesareo, 16–19 June 2015
Francesco de Giovanni Day, Napoli, 8 October 2015
Mario Curzio Day, Napoli, 25 January 2016
Group Theory Conference, Ischia, 30 March– 2 April 2016
Group Theory in Florence: a Meeting in Honour of Guido Zappa, Florence, 16–17 June 2016
The 20th Midrasha Mathematicae — 60 Faces to Groups, Jerusalem, 6–11 November 2016

Schools and Advanced Courses attended

Scuola Matematica Interuniversitaria, Perugia, 1975, 1976
Scuola Matematica Interuniversitaria, Cortona, 1977, 1978, 1979, 1980
CIME, Como, 1984
School of noncommutative algebra, Trento, September 1987
Group representation theory I, Trento, September 1987
Chevalley groups, Trento, September 1988
Group representation theory II, Trento, September 1990
School of noncommutative algebra, Parma, June 1991
Group representation theory III, Trento, September 1991

Graduate Students

Norberto Gavioli (1994), Claretta Carrara (1997), Giuseppe Jurman (1998), Marina Avitabile (1999), Erika Damian (2003), Velitchko Todorov (2005), Silvia Rensi (2005), Simone Ugolini (2010)

General talks

- Cappelli rossi, cappelli blu e codici a correzione d'errore
- Sette domande, una menzogna
- Pirati e monete d'oro (Bonus: occhi azzurri)

Languages

Italian (mother language), English (fluent), German (Kleines Deutsches Sprachdiplom des Goethe-Instituts), some French

Odds

Lauree Scientifiche project, 2006–...

On January 12, 2012, I have been interviewed by Radio3 Scienza, a daily magazine of Radio RAI, on the science of Sudoku.

On February 20, 2012, my colleague Massimiliano Sala and I have been interviewed by Radio3 Scienza on a paper by Lenstra et al. on the security of the SSL protocol.

On February 27–28, 2013, I contributed to a stand on Cryptography and Error-Correcting Codes at the *Notte dei Ricercatori* in Trento

Several talks at various schools

Ends

Member of Unione Matematica Italiana, American Mathematical Society, Accademia Roveretana degli Agiati

Member of Gruppo Nazionale per le Strutture Algebriche e Geometriche e loro Applicazioni (Istituto Nazionale di Alta Matematica)

Referee for various journals and institutions (CIVR — Italy, NSA — USA, FWF — Austria, NWO — The Netherlands)

Reviewer for Mathematical Reviews, Zentralblatt für Mathematik

Research papers

1. A. Caranti, *The multiple holomorphs of finite p-groups of class two*, arXiv:1801.10410, January 2018.
2. A. Caranti and F. Dalla Volta, *Groups that have the same holomorph as a finite perfect group*, arXiv:1612.03573, 2018, accepted for publication, Journal of Algebra.
3. ———, *The multiple holomorph of a finitely generated abelian group*, J. Algebra **481** (2017), 327–347, arXiv:1611.05662.
4. R. Aragona, A. Caranti, and M. Sala, *The group generated by the round functions of a GOST-like cipher*, Ann. Mat. Pura Appl. (4) **196** (2017), no. 1, 1–17.
5. A. Caranti, *A simple construction for a class of p-groups with all of their automorphisms central*, Rend. Semin. Mat. Univ. Padova **135** (2016), 251–258. MR 3506071
6. A. Caranti and C. M. Scoppola, *Finite morphic p-groups*, J. Pure Appl. Algebra **219** (2015), 4635–4641.
7. A. Caranti, *Erratum to "A module-theoretic approach to abelian automorphism groups" [MR3314589]*, Israel J. Math. **215** (2016), no. 2, 1025–1026. MR 3552302
8. ———, *A module-theoretic approach to abelian automorphism groups*, Israel J. Math. **205** (2015), no. 1, 235–246. MR 3314589
9. R. Aragona, A. Caranti, F. Dalla Volta, and M. Sala, *On the group generated by the round functions of translation based ciphers over arbitrary finite fields*, Finite Fields Appl. **25C** (2014), 293–305.
10. A. Caranti, *Quasi-inverse endomorphisms*, J. Group Theory **16** (2013), no. 5, 779–792. MR 3101012
11. S. C. Featherstonhaugh, A. Caranti, and L. N. Childs, *Abelian Hopf Galois structures on prime-power Galois field extensions*, Trans. Amer. Math. Soc. **364** (2012), 3675–3684.
12. A. Caranti, Francesca Dalla Volta, and M. Sala, *On some block ciphers and imprimitive groups*, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5–6, 339–350.

13. ———, *An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher*, Des. Codes Cryptogr. **52** (2009), no. 3, 293–301, arXiv:0812.1629.
14. ———, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308.
15. A. Caranti and S. Mattarei, *Automorphisms of p-groups of maximal class*, Rend. Sem. Mat. Univ. Padova **115** (2006), 189–198. MR MR2245595
16. A. Caranti and F. Dalla Volta, *The round functions of cryptosystem PGM generate the full symmetric group*, Des. Codes Cryptogr. **38** (2006), no. 1, 147–155.
17. A. Caranti and S. Mattarei, *Gradings of nongraded Hamiltonian Lie algebras*, J. Aust. Math. Soc. **79** (2005), no. 3, 1–42.
18. ———, *Nottingham Lie algebras with diamonds of finite type*, Internat. J. Algebra Comput. **14** (2004), no. 1, 35–67.
19. A. Caranti and M. R. Vaughan-Lee, *Graded Lie algebras of maximal class. V*, Israel J. Math. **133** (2003), 157–175.
20. ———, *Graded Lie algebras of maximal class. IV*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), no. 2, 269–312. MR 2002c:17044
21. A. Caranti and M. F. Newman, *Graded Lie algebras of maximal class. II*, J. Algebra **229** (2000), no. 2, 750–784. MR 2001g:17041
22. A. Caranti and S. Mattarei, *Some thin Lie algebras related to Albert-Frank algebras and algebras of maximal class*, J. Austral. Math. Soc. (Series A) **67** (1999), 157–184.
23. A. Caranti and G. Jurman, *Quotients of maximal class of thin Lie algebras. The odd characteristic case*, Comm. Algebra **27** (1999), no. 12, 5741–5748.
24. A. Caranti, *Loop algebras of Zassenhaus algebras in characteristic three*, Israel J. Math. **110** (1999), 61–73.
25. A. Caranti, *Thin groups of prime-power order and thin Lie algebras: an addendum*, Quart. J. Math. Oxford (2) **49** (1998), 445–450.
26. A. Caranti, *Presenting the graded Lie algebra associated to the Nottingham group*, J. Algebra **198** (1997), no. 1, 266–289.
27. A. Caranti, S. Mattarei, and M. F. Newman, *Graded Lie algebras of maximal class*, Trans. Amer. Math. Soc. **349** (1997), no. 10, 4021–4051.
28. A. Caranti, S. Mattarei, M. F. Newman, and C. M. Scoppola, *Thin groups of prime-power order and thin Lie algebras*, Quart. J. Math. Oxford Ser. (2) **47** (1996), no. 187, 279–296.
29. A. Caranti, N. Gavioli, and S. Mattarei, *Subgroups of finite p-groups inducing the same permutation character*, Comm. Algebra **22** (1994), no. 3, 877–895.
30. R. Brandl, A. Caranti, and C. M. Scoppola, *Metabelian thin p-groups*, Quart. J. Math. Oxford Ser. (2) **43** (1992), no. 170, 157–173.
31. A. Caranti and C. M. Scoppola, *Endomorphisms of two-generated metabelian groups that induce the identity modulo the derived subgroup*, Arch. Math. (Basel) **56** (1991), no. 3, 218–227.
32. A. Caranti and C. M. Scoppola, *A remark on the orders of p-groups that are automorphism groups*, Boll. Un. Mat. Ital. A (7) **4** (1990), no. 2, 201–207.
33. C. Bagiński and A. Caranti, *The modular group algebras of p-groups of maximal class*, Canad. J. Math. **40** (1988), no. 6, 1422–1435.
34. A. Caranti, S. Franciosi, and F. de Giovanni, *Some examples of infinite groups in which each element commutes with its endomorphic images*, Group theory (Bressanone, 1986) (Berlin), Lecture Notes in Math., vol. 1281, Springer, Berlin, 1987, pp. 9–17.
35. A. Caranti, *Finite p-groups of exponent p^2 in which each element commutes with its endomorphic images*, J. Algebra **97** (1985), no. 1, 1–13.
36. A. Caranti and C. M. Scoppola, *Central commutators*, Bull. Austral. Math. Soc. **30** (1984), no. 1, 67–71.

37. Andrea Caranti, *Automorphism groups of p-groups of class* 2 *and exponent* p^2*: a classification on* 4 *generators*, Ann. Mat. Pura Appl. (4) **134** (1983), 93–146.
38. Andrea Caranti, *On the automorphism groups of certain p-groups of class* 4, Boll. Un. Mat. Ital. B (6) **2** (1983), no. 2, 605–615.
39. Andrea Caranti and Pierantonio Legovini, *On finite groups whose endomorphic images are characteristic subgroups*, Arch. Math. (Basel) **38** (1982), no. 5, 388–390.
40. Andrea Caranti, *Gruppi finiti che soddisfano a una condizione sui normalizzanti*, Ricerche Mat. **29** (1980), no. 1, 3–16.
41. Andrea Caranti, *Proiettività dei p-gruppi di classe massimale*, Rend. Sem. Mat. Univ. Padova **61** (1979), 393–404 (1980).

Other Publications

1. A. Caranti and C. Giberti, *Tra* brevitas *e* secretum*, note sui linguaggi cifrati*, Scriver veloce. Sistemi tachigrafici dall'antichità a Twitter (Alessandro Tedesco, ed.), Accademia Roveretana degli Agiati, Leo S. Olschki, 2017, pp. 213–223.
2. A. Caranti, *Regular groups, radical rings, and abelian Hopf Galois structures on prime-power Galois field extensions*, Note Mat. **33** (2013), no. 1, 95–101. MR 3071313
3. ———, *Come stabilizzare un tavolo traballante, o il Teorema di Bolzano*, Manifesta 7: Index: Catalogo della mostra (Trentino, 19 luglio-2 novembre 2008) (Cinisello Balsamo (MI)) (A. Budak, A. Franke, and H. Peleg, eds.), Silvana Editoriale, 2008, p. 113.
4. ———, *Computing in groups of prime-power order*, Notes of a course given at the Summer School of Computer Algebra, Budapest Technical University, August–September 1992.
5. ———, *Analyticity and growth of pro-p-groups*, Generators and relations in groups and geometries (Lucca, 1990) (Dordrecht), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 333, Kluwer Acad. Publ., Dordrecht, 1991, pp. 321–341.
6. ———, *Alcune riflessioni sullo stato della divulgazione della Matematica in Italia*, Torricelliana (Bollettino della Società Torricelliana di Scienze e Lettere) **40** (1989), 93–106.

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38123 Trento, Italia

E-mail address: andrea.caranti@unitn.it

URL: http://science.unitn.it/∼caranti/