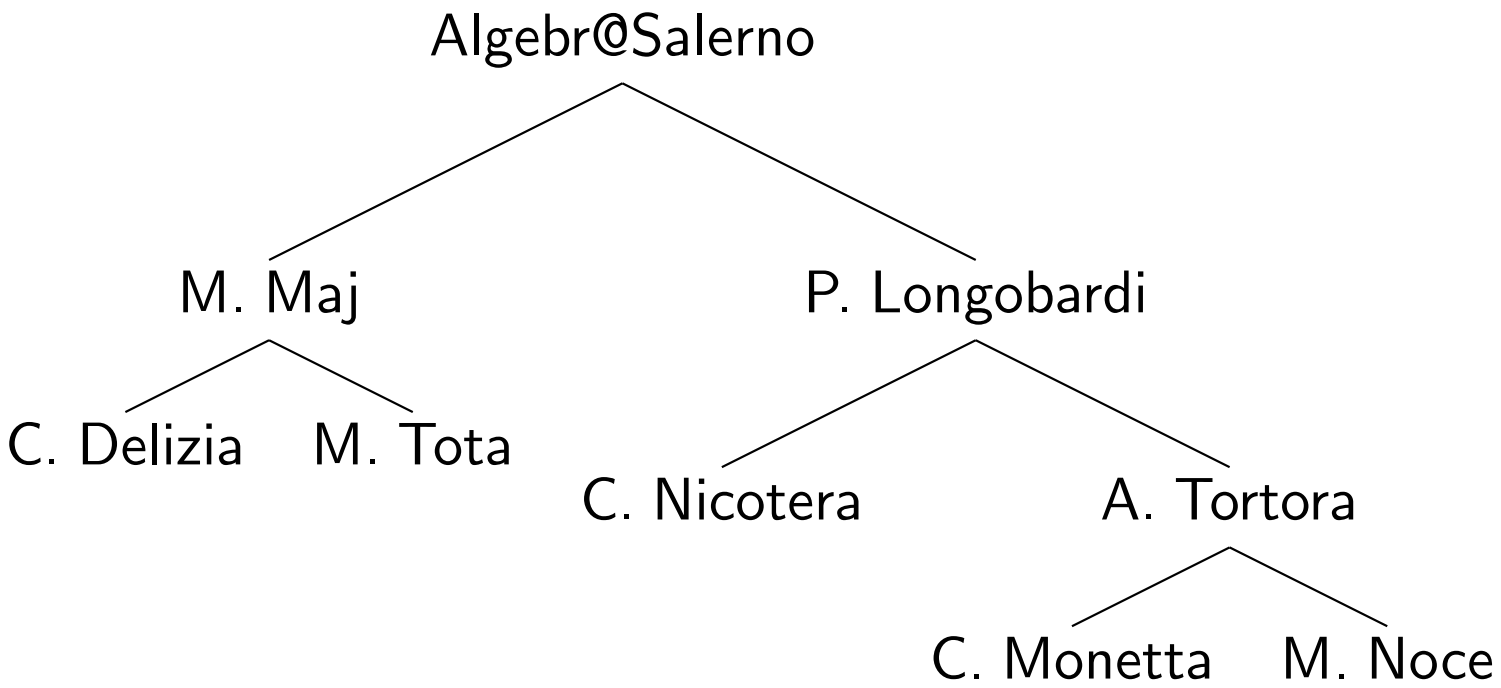
Il Gruppo di Salerno

Antonio Tortora
antortora@unisa.it

Università degli Studi di Salerno
Dipartimento di Matematica

Associazione De Componendis Cifris: evento conoscitivo
Napoli, CNR - 22 gennaio 2018

Gli elementi del Gruppo



Didattica: insegnamenti di Algebra

Laurea Triennale

- Algebra I – M. Maj, M. Tota
- Algebra II – P. Longobardi, M. Tota
- Semigruppi liberi e Teoria dei codici – C. Delizia
- Teoria di Galois – G. Vincenzi

Didattica: insegnamenti di Algebra

Laurea Triennale

- Algebra I – M. Maj, M. Tota
- Algebra II – P. Longobardi, M. Tota
- Semigruppi liberi e Teoria dei codici – C. Delizia
- Teoria di Galois – G. Vincenzi

Laurea Magistrale

- Istituzioni di Algebra Superiore – P. Longobardi
- Teoria dei Gruppi – M. Maj, A. Tortora
- Teoria dei Moduli – M. Maj
- Teoria dei Numeri e Crittografia – P. Longobardi

Didattica: insegnamenti di Algebra

Laurea Triennale

- Algebra I – M. Maj, M. Tota
- Algebra II – P. Longobardi, M. Tota
- Semigruppi liberi e Teoria dei codici – C. Delizia
- Teoria di Galois – G. Vincenzi

Laurea Magistrale

- Istituzioni di Algebra Superiore – P. Longobardi
- Teoria dei Gruppi – M. Maj, A. Tortora
- Teoria dei Moduli – M. Maj
- Teoria dei Numeri e Crittografia – P. Longobardi

Piano Lauree Scientifiche per la Matematica

- Laboratorio di Algebra e Crittografia – M. Tota, A. Tortora

Ricerca: Teoria dei Gruppi

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel
- gruppi di Grigorchuk e loro generalizzazioni

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel
- gruppi di Grigorchuk e loro generalizzazioni

Con x e y elementi di un gruppo G, definiamo il *commutatore*

$$[x, y] = x^{-1}y^{-1}xy.$$

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel
- gruppi di Grigorchuk e loro generalizzazioni

Con x e y elementi di un gruppo G, definiamo il *commutatore*

$$[x, y] = x^{-1}y^{-1}xy.$$

Il gruppo G si dice *2-Engel* se $[x, y, y] = [[x, y], y] = 1$ per ogni $x, y \in G$.

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel
- gruppi di Grigorchuk e loro generalizzazioni

Con x e y elementi di un gruppo G, definiamo il *commutatore*

$$[x, y] = x^{-1}y^{-1}xy.$$

Il gruppo G si dice *2-Engel* se $[x, y, y] = [[x, y], y] = 1$ per ogni $x, y \in G$. In tal caso si ha

(*i*) $xy^2x = yx^2y$;

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel
- gruppi di Grigorchuk e loro generalizzazioni

Con x e y elementi di un gruppo G, definiamo il *commutatore*

$$[x, y] = x^{-1}y^{-1}xy.$$

Il gruppo G si dice *2-Engel* se $[x, y, y] = [[x, y], y] = 1$ per ogni $x, y \in G$. In tal caso si ha

(*i*) $xy^2x = yx^2y$;

(*ii*) $[x^n, y] = [x, y]^n$

Ricerca: Teoria dei Gruppi

I nostri gruppi

- p-gruppi finiti
- gruppi infiniti con condizioni finitarie
- gruppi di Engel
- gruppi di Grigorchuk e loro generalizzazioni

Con x e y elementi di un gruppo G, definiamo il *commutatore*

$$[x, y] = x^{-1}y^{-1}xy.$$

Il gruppo G si dice *2-Engel* se $[x, y, y] = [[x, y], y] = 1$ per ogni $x, y \in G$. In tal caso si ha

(*i*) $xy^2x = yx^2y$;

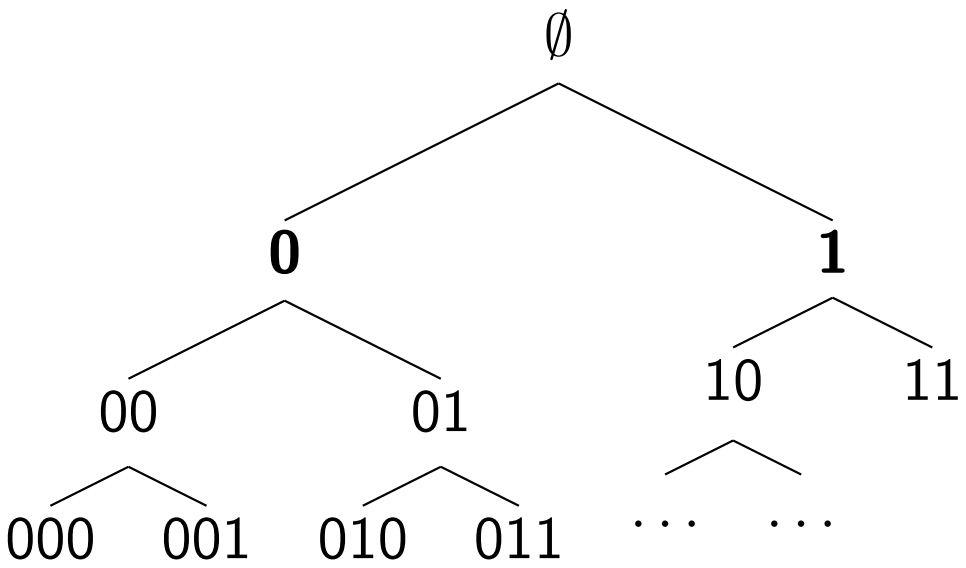
(*ii*) $[x^n, y] = [x, y]^n = [x, y^n]$, per ogni $n \in \mathbb{Z}$.

Automorfismi di un albero

I due gruppi di Grigorchuk sono sottogruppi del gruppo degli automorfismi di un albero con radice regolare di grado $d = 2$ o 4.

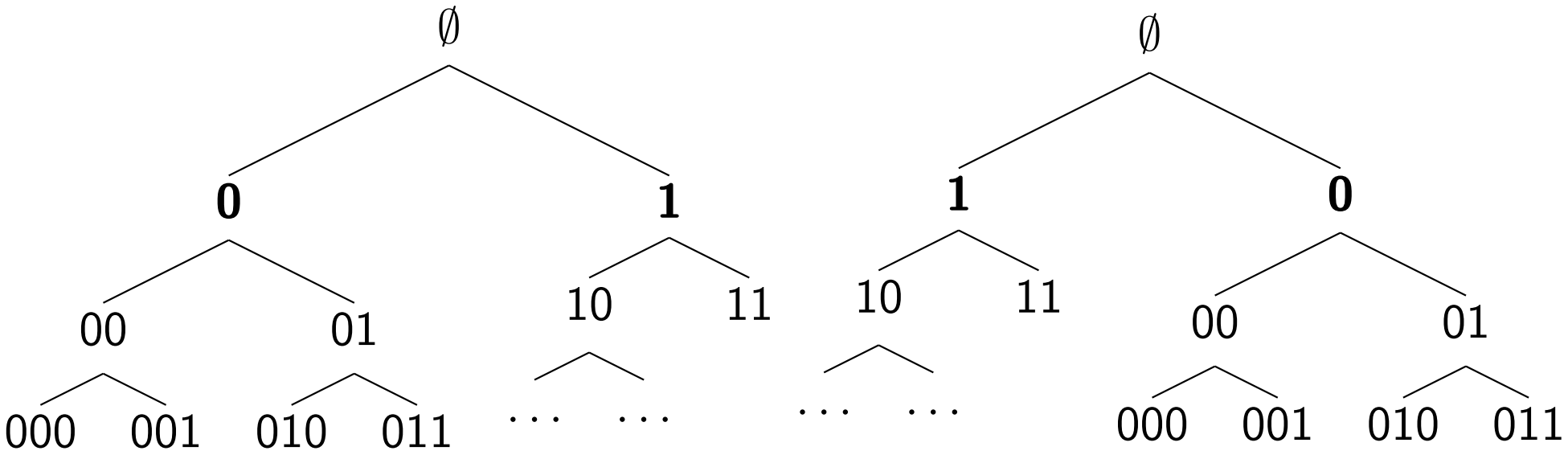
Automorfismi di un albero

I due gruppi di Grigorchuk sono sottogruppi del gruppo degli automorfismi di un albero con radice regolare di grado $d = 2$ o 4.



Automorfismi di un albero

I due gruppi di Grigorchuk sono sottogruppi del gruppo degli automorfismi di un albero con radice regolare di grado $d = 2$ o 4.



Un automorfismo è una permutazione dell'insieme dei vertici che fissa la radice e conserva l'adiacenza.

Applicazioni della teoria dei gruppi alla crittografia

Trento, 2016

Applicazioni della teoria dei gruppi alla crittografia

Trento, 2016

R. Aragona, M. Calderini, A.T., M. Tota

- *On the primitivity of PRESENT and other lightweight ciphers*

Journal of Algebra and its applications, First online: 2017
arXiv:1611.01346 [math.GR].

Applicazioni della teoria dei gruppi alla crittografia

Trento, 2016

R. Aragona, M. Calderini, A.T., M. Tota

- *On the primitivity of PRESENT and other lightweight ciphers*

Journal of Algebra and its applications, First online: 2017
`arXiv:1611.01346 [math.GR]`.

BunnyTN 2016

C. Monetta, A.T.

- *The conjugacy search problem for supersoluble groups*

in preparazione.

Applicazioni della teoria dei gruppi alla crittografia

Trento, 2016

R. Aragona, M. Calderini, A.T., M. Tota

- *On the primitivity of PRESENT and other lightweight ciphers*

Journal of Algebra and its applications, First online: 2017
arXiv:1611.01346 [math.GR].

BunnyTN 2016

C. Monetta, A.T.

- *The conjugacy search problem for supersoluble groups*

in preparazione.

B. Eick, D. Kahrobaei, Polycylic groups: a new platform for cryptology?, 2004, arXiv:math/0411077 [math.GR].

Applicazioni della teoria dei gruppi alla crittografia

D. Kahrobaei, V. Shpilrain, A.T.

- *Using 2-Engel groups in public key cryptography*

(in preparazione).

Applicazioni della teoria dei gruppi alla crittografia

D. Kahrobaei, V. Shpilrain, A.T.

- *Using 2-Engel groups in public key cryptography*

(in preparazione).

Scambio della chiave basato sull'uso dei gruppi 2-Engel:

$$xy^2x = yx^2y;$$

Applicazioni della teoria dei gruppi alla crittografia

D. Kahrobaei, V. Shpilrain, A.T.

- *Using 2-Engel groups in public key cryptography*

(in preparazione).

Scambio della chiave basato sull'uso dei gruppi 2-Engel:

$$xy^2x = yx^2y; \qquad [x^n, y] = [x, y]^n = [x, y^n].$$

Applicazioni della teoria dei gruppi alla crittografia

D. Kahrobaei, V. Shpilrain, A.T.

- *Using 2-Engel groups in public key cryptography*

(in preparazione).

Scambio della chiave basato sull'uso dei gruppi 2-Engel:

$$xy^2x = yx^2y; \quad [x^n, y] = [x, y]^n = [x, y^n].$$

AMS (Spring Eastern) Sectional Meetings

D. Kahrobaei, A.T.

- Special Session on *Algorithmic Group Theory and Applications*

Northeastern University, Boston, MA – April 21-22, 2018
`www.ams.org/meetings/sectional/2252_program_ss26.html`

Eventi: Ischia Group Theory

Convegno internazionale biennale organizzato, dal 2004, in collaborazione con l'Università dell'Aquila e l'Università di Milano

http://www.dipmat2.unisa.it/ischiagrouptheory

Ischia Group Theory 2018, 19 – 24 marzo

ISCHIA GROUP THEORY 2018

ISCHIA (NAPLES, ITALY)
MARCH, 19th - 24th

www.dipmat2.unisa.it/ischiagrouptheory

MAIN SPEAKERS:
A. Abdollahi (Iran)
E. Aljadeff (Israel)
A. Ballester-Bolinches (Spain)
A. Caranti (Italy)
F. de Giovanni (Italy)
R. Esteban-Romero (Spain)
G.A. Fernández-Alcober (Spain)
A.M.W. Glass (U.K.)
G. Glauberman (U.S.A.)
R. Grigorchuk (U.S.A.)
T. Hawkes (U.K.)
H. Heineken (Germany)
W. Herfort (Austria)
M. Herzog (Israel)
L-C. Kappe (U.S.A.)
O. Kegel (Germany)
E. Khukhro (U.K.)
B. Klopsch (Germany)
L.A. Kurdachenko (Ukraine)
M. Kuzucuoğlu (Turkey)
M.L. Lewis (U.S.A.)
A. Lubotzky (Israel)
A. Lucchini (Italy)
A. Olshanskiy (U.S.A./Russia)
C.W. Parker (U.K.)
C.E. Praeger (Australia)
D.J.S. Robinson (U.S.A.)
D. Segal (U.K.)
Y. Segev (Israel)
P. Shumyatsky (Brazil)
S.E. Stonehewer (U.K.)
A. Turull (U.S.A.)
N. Vavilov (Russia)
J.S. Wilson (U.K.)
A. Zalesski (Belarus)
E.I. Zelmanov (U.S.A.)

SCIENTIFIC COMMITTEE:
Mariagrazia BIANCHI (Milano)
Patrizia LONGOBARDI (Salerno)
Mercede MAJ (Salerno)
Carlo SCOPPOLA (L'Aquila)

ORGANIZING COMMITTEE:
Costantino DELIZIA
Carmine MONETTA
Chiara NICOTERA
Marialaura NOCE
Antonio TORTORA
Maria TOTA
(Università di Salerno)

UNIVERSITÀ DEGLI STUDI DI SALERNO

Ischia Group Theory 2018: main speakers

A. Abdollahi (Iran)
E. Aljadeff (Israel)
A. Ballester-Bolinches (Spain)
A. Caranti (**Italy**)
F. de Giovanni (**Italy**)
R. Esteban-Romero (Spain)
G.A. Fernández-Alcober (Spain)
A.M.W. Glass (U.K.)
G. Glauberman (U.S.A.)
T. Hawkes (U.K.)
H. Heineken (Germany)
W. Herfort (Austria)
M. Herzog (Israel)
L.-C. Kappe (U.S.A.)
O.H. Kegel (Germany)
E. Khukhro (U.K.)
B. Klopsch (Germany)
L.A. Kurdachenko (Ukraine)
M. Kuzucuoğlu (Turkey)
M.L. Lewis (U.S.A.)
A. Lubotzky (Israel)
A. Lucchini (**Italy**)
A. Olshanskiy (U.S.A./Russia)
C.W. Parker (U.K.)
C.E. Praeger (Australia)
D.J.S. Robinson (U.S.A.)
D. Segal (U.K.)
Y. Segev (Israel)
P. Shumyatsky (Brazil)
S.E. Stonehewer (U.K.)
A. Turull (U.S.A.)
N. Vavilov (Russia)
J.S. Wilson (U.K.)
A. Zalesski (Belarus)

Grazie per l'attenzione!

Campus di Unisa, Fisciano (SA)