

Alessio Russo

Numeri, Gruppi, Polinomi

Un'introduzione all'Algebra

II Edizione



Copyright © MMVIII
ARACNE editrice S.r.l.

www.aracneeditrice.it
info@aracneeditrice.it

via Raffaele Garofalo, 133 A/B
00173 Roma
(06) 93781065

ISBN 978-88-548-2058-6

*I diritti di traduzione, di memorizzazione elettronica,
di riproduzione e di adattamento anche parziale,
con qualsiasi mezzo, sono riservati per tutti i Paesi.*

*Non sono assolutamente consentite le fotocopie
senza il permesso scritto dell'Editore.*

I edizione: novembre 2007
II edizione: settembre 2008

Indice

Premessa	5
1 Principio di Induzione e sue Applicazioni	7
1.1 Insiemi, relazioni ed applicazioni	7
1.2 Numeri Naturali	10
1.3 Coefficienti Binomiali	19
1.4 Osservazioni finali sul Principio di induzione	21
2 Aritmetica sui Numeri Interi	23
2.1 Numeri Interi	23
2.2 Divisibilità	25
2.3 Massimo Comune Divisore e Minimo Comune Multiplo	27
2.4 Numeri Primi e Teorema Fondamentale dell'Aritmetica	31
3 Aritmetica Modulare	36
3.1 Congruenza modulo un intero	36
3.2 Anello degli interi modulo m	37
3.3 Funzione di Eulero ed Equazioni Congruenziali	39
3.4 Aritmetica modulare e grandi numeri	42
3.5 Piccolo Teorema di Fermat e applicazioni (Crittosistema RSA)	43
4 Introduzione alla Teoria dei Gruppi	46
4.1 Operazioni in un insieme - Semigrupperi, Monoidi e Gruppi	47
4.2 Sottogruppi	53
4.3 Teorema di Lagrange e applicazioni	57
4.4 Sottogruppi Normali e Gruppi Quoziente	62
4.5 Omomorfismi di Gruppi	67
4.6 Gruppi di Permutazioni	74
4.7 Azioni di un gruppo e Teorema di Sylow	82
5 Polinomi	89
5.1 Elementi Algebrici e Trascendenti	89
5.2 Polinomi in una indeterminata	91
5.3 Divisibilità nell'anello dei polinomi su un campo	94
5.4 Fattorizzazione nell'anello dei polinomi su un campo	98
5.5 Radici di un polinomio	102
5.6 Molteplicità di una radice	105
5.7 Fattorizzazione in $\mathbb{C}[x]$ e in $\mathbb{R}[x]$	106
5.8 Divisibilità e Fattorizzazione in $\mathbb{Z}[x]$	107

6 Ricerca delle radici	111
6.1 Campo dei Quozienti e Caratteristica	111
6.2 Polinomio minimo ed Estensioni algebriche	112
6.3 Campo di spezzamento	115
6.4 Risolubilità per radicali e Gruppo di Galois	120
Bibliografia	131
Indice Analitico	132