Alessio Russo

Numeri, gruppi, polinomi

Un'introduzione all'Algebra
Nuova edizione

www.aracneeditrice.it
info@aracneeditrice.it

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

ISBN 978-88-548-5837-4

III edizione: febbraio 2013

Indice

Premessa 9

1 Principio di induzione e sue applicazioni **11**
- 1.1 Insiemi, relazioni ed applicazioni 11
- 1.2 Numeri naturali 16
- 1.3 Coefficienti binomiali 28
- 1.4 Un'osservazione finale 31

2 Aritmetica sui numeri interi **33**
- 2.1 Numeri interi 33
- 2.2 Divisibilità 36
- 2.3 Massimo comune divisore e minimo comune multiplo . . . 39
- 2.4 Numeri primi e teorema fondamentale dell'aritmetica . . . 45

3 Aritmetica modulare **51**
- 3.1 Congruenza modulo un intero 51
- 3.2 Anello degli interi modulo m 53
- 3.3 Funzione di Eulero ed equazioni congruenziali 56
- 3.4 Aritmetica modulare e grandi numeri 59
- 3.5 Piccolo teorema di Fermat e applicazioni (crittosistema RSA) 61

4 Teoria dei gruppi **65**
- 4.1 Operazioni in un insieme - semigruppi, monoidi e gruppi . 66
- 4.2 Sottogruppi 74
- 4.3 Teorema di Lagrange e applicazioni 80
- 4.4 Sottogruppi normali e gruppi quoziente 87
- 4.5 Omomorfismi di gruppi 94

4.6 Gruppi di permutazioni 103
4.7 Azioni di un gruppo e teorema di Sylow 114

5 Polinomi **125**
5.1 Elementi algebrici e trascendenti 125
5.2 Polinomi in una indeterminata 127
5.3 Divisibilità nell'anello dei polinomi su un campo 131
5.4 Fattorizzazione nell'anello dei polinomi su un campo . . . 137
5.5 Radici di un polinomio 143
5.6 Molteplicità di una radice 147
5.7 Fattorizzazione in $\mathbb{C}[x]$ e in $\mathbb{R}[x]$ 148
5.8 Divisibilità e fattorizzazione in $\mathbb{Z}[x]$ 150

6 Ricerca delle radici **155**
6.1 Campo dei quozienti e caratteristica 155
6.2 Polinomio minimo ed estensioni algebriche 157
6.3 Campo di spezzamento 162
6.4 Risolubilità per radicali e gruppo di Galois 168

Bibliografia **183**

Indice analitico **185**