

Spis treści

Wstęp	11
1. Arytmetyka liczb całkowitych	13
1.1. Liczby pierwsze	13
1.2. Algorytm Euklidesa	18
1.3. Zadania	21
2. Grupy	23
2.1. Funkcja φ Eulera	27
2.2. Podgrupy	31
2.3. Homomorfizmy grup, grupy izomorficzne	32
2.4. Grupy cykliczne	34
2.5. Twierdzenie Cayleya	38
2.6. Twierdzenie Lagrange’a	39
2.7. Wnioski z twierdzenia Lagrange’a	41
2.8. Grupa dihedralna	43
2.9. Podgrupy normalne	44
2.10. Podstawowe twierdzenie o izomorfizmie grup	47
2.11. Grupy alternujące	49
2.12. Zadania	50
3. Arytmetyka modularna	53
3.1. Twierdzenie Eulera i małe twierdzenie Fermata	53
3.2. Chińskie twierdzenie o resztach	54
3.3. Residua kwadratowe	56
3.4. Zasady kryptografii z kluczem publicznym	58
3.4.1. Metoda Rabina	60
3.4.2. Metoda RSA	61
3.5. Zadania	63
4. Działanie grupy na zbiorze	65
4.1. Lemat Burnside’a	69
4.2. Grupa obrotów sześcianu	73
4.3. Grupy i kolorowania – metoda Pólyi	74
4.4. Indeksy cyklowe i twierdzenia Pólyi	77
4.5. Obliczanie liczby grafów	83
4.6. Zadania	86

5. Pierścienie	89
5.1. Przykłady pierścieni	90
5.2. Podpierścienie	91
5.3. Ideały i pierścienie ilorazowe	91
5.4. Ideały i pierścienie główne	93
5.5. Homomorfizmy pierścieni	94
5.6. Podzielność w pierścieniach	96
5.7. Charakterystyka pierścienia	99
5.8. Zadania	100
6. Pierścienie Gaussa	103
6.1. Pierścienie wielomianów	105
6.2. Pierścienie główne	108
6.3. Pierścienie euklidesowe	110
6.4. Algorytm Euklidesa w pierścieniu euklidesowym	112
6.5. Zasadnicze twierdzenie arytmetyki	112
6.6. Ciało ułamków pierścienia całkowitego	114
6.7. Wielomiany nad pierścieniami Gaussa	116
6.8. Twierdzenie Gaussa	119
6.9. Wielomiany nierozkładalne	120
6.10. Zadania	122
7. Wielomiany wielu zmiennych	123
7.1. Wielomiany symetryczne	123
7.2. Twierdzenie Wilsona	125
7.3. Podstawowe twierdzenie o wielomianach symetrycznych	126
7.4. Zadania	130
8. Rozszerzenia ciał	131
8.1. Ciało rozkładu wielomianu	134
8.2. Zasadnicze twierdzenie algebry	136
8.3. Rozszerzenia o skończoną liczbę elementów	139
8.4. Rozszerzenia skończone i algebraiczne	140
8.5. Rozszerzenia przestępne	147
8.6. Rozszerzenia izomorfizmów pierścieni i ciał	150
8.7. Rząd ciała skończonego	154
8.8. Pochodne wielomianów i krotności pierwiastków	155
8.9. Ciało Galois rzędu p^n	156
8.10. Liczby konstruowalne	160
8.11. Zadania	165
9. Skończone grupy abelowe	169
9.1. Twierdzenie Cauchy'ego dla skończonych grup abelowych	171
9.2. Twierdzenie o skończonych grupach abelowych	171
9.3. Zadania	178
10. Twierdzenia Sylowa	181
10.1. Pierwsze twierdzenie Sylowa	181
10.2. Wnioski z pierwszego twierdzenia Sylowa	183
10.3. Sprzężenie podgrupy	185
10.4. Twierdzenie o rozkładzie na orbity	188

10.5. Drugie twierdzenie Sylowa	191
10.6. Wnioski z drugiego twierdzenia Sylowa	192
10.7. Trzecie twierdzenie Sylowa	192
10.8. Wnioski z trzeciego twierdzenia Sylowa	193
10.9. Zadania	194
11. Grupy rozwiązalne	199
11.1. Komutatory i komutanty	201
11.2. Twierdzenia o izomorfizmie grup	204
11.3. Warunek konieczny i wystarczający rozwiązalności grupy	206
11.4. Zadania	208
12. Teoria Galois	209
12.1. Grupa Galois rozszerzenia ciała	209
12.2. Wielomiany i ciała rozdzielcze	217
12.3. Twierdzenie o elemencie prymitywnym	222
12.4. Twierdzenie Dedekinda–Artina	224
12.5. Rozszerzenia Galois	230
12.5.1. Wnioski z twierdzenia 12.25	233
12.5.2. Zasadnicze twierdzenie teorii Galois	236
12.6. Rozwiązalność równań algebraicznych	241
12.7. Zadania	249
13. Évariste Galois	251
14. Wskazówki do wybranych zadań	261
14.1. Rozdział 4	261
14.2. Rozdział 5	261
14.3. Rozdział 8	262
14.4. Rozdział 9	262
14.5. Rozdział 10	264
14.6. Rozdział 11	265
14.7. Rozdział 12	266
15. Oznaczenia	269
Bibliografia	271
Skorowidz¹	273