

OBSAH

Úvod	7
1. Historie a motivace moderní algebry	8
2. Ekvivalence a uspořádané množiny	9
I. Dělitelnost v oborech integrity	13
3. Elementární teorie čísel	14
3.1. Přirozená čísla	14
3.2. Základní věta aritmetiky	15
3.3. Kongruence	18
3.4. Eulerova věta	19
3.5. Čínská věta o zbytcích	21
4. Obory integrity	23
4.1. Definice oboru integrity	23
4.2. Příklady oborů integrity	25
4.3. Podílová tělesa	29
5. Základní pojmy teorie dělitelnosti	30
5.1. Invertibilní prvky	30
5.2. Dělitelnost jako uspořádání	31
5.3. Největší společný dělitel	32
5.4. Ireducibilní prvky	33
6. Gaussovské obory	33
7. Eukleidovské obory	37
7.1. Eukleidův algoritmus	37
7.2. Hlavní ideály	39
Shrnutí	41
8. * Rozšíření celých čísel	42
8.1. Obory $\mathbb{Z}[\sqrt{s}]$	42
8.2. Gaussova celá čísla	43
9. * Obory polynomů	45
9.1. Gaussovo lemma	45
9.2. Eisensteinovo kritérium	48
10. Kořeny polynomů	48
10.1. Počet kořenů	48
10.2. Algebraická a transcendentní čísla	49
10.3. Racionální kořeny	51
10.4. * Cardanovy vzorce	51
10.5. * Newtonova metoda	54
10.6. Věta o interpolaci	54
11. * Vícenásobné kořeny a lineární diferenční rovnice	55
11.1. Vícenásobné kořeny	55
11.2. Lineární diferenční rovnice	58
II. Obecné algebry	63
12. Algebry	64
12.1. Algebry	64
12.2. Podalgebry	65
12.3. Direktní součiny	68

12.4.	Homomorfismy	68
12.5.	Izomorfní algebry	71
13.	* Algebry v obecném jazyce	73
III.	Grupy	75
14.	Základní vlastnosti	76
14.1.	Abelovské grupy	76
14.2.	Obecné grupy	78
14.3.	Podgrupy, homomorfismy, direktní součiny	80
14.4.	Reprezentace grup	82
15.	Cyklické grupy	83
15.1.	Řád prvku	83
15.2.	Klasifikace a vlastnosti	84
15.3.	Grupy \mathbb{Z}_p^* jsou cyklické	87
15.4.	* Diskrétní logaritmus	89
15.5.	* Kryptografické aplikace	89
16.	* Klasifikace konečných abelovských grup	92
17.	Permutační grupy	95
17.1.	Permutace, znaménko, generátory	95
17.2.	Konjugace	96
17.3.	Grupy automorfismů	97
18.	Rozklady podle podgrupy	98
18.1.	Rozklady a Lagrangeova věta	98
18.2.	Normální podgrupy	101
19.	* Působení grupy na množině	102
IV.	Okruhy	109
20.	Základní vlastnosti	110
20.1.	Definice a příklady	110
20.2.	Podokruhy	112
20.3.	Ideály	113
20.4.	Homomorfismy	114
20.5.	Charakteristika okruhu	115
21.	* Moduly	116
V.	Faktoralgebry	119
22.	Faktorgrupy	120
23.	Faktorokruhy	123
23.1.	Konstrukce faktorokruhu	123
23.2.	Maximální ideály a konstrukce těles	125
23.3.	* Zobecněná Čínská věta o zbytcích	126
24.	* Faktoralgebry	128
24.1.	Konstrukce faktoralgebry	129
24.2.	Kongruence grup a okruhů	130
24.3.	Faktoralgebry v obecném jazyce	131
VI.	Tělesa	133
25.	Rozšíření konečného stupně	134
26.	* Konstrukce pravítkem a kružítkem	138
27.	Kořenová a rozkladová nadtělesa, algebraický uzávěr	141

27.1. Kořenová a rozkladová nadtělesa	141
27.2. Algebraický uzávěr	143
28. * Konečná tělesa	145
Literatura	148
Rejstřík	149
Obsah	151