

Obsah

1	Úvod	6
1.1	Základné pojmy	9
1.2	Konečné polia	14
2	Rozšírenia polí	16
2.1	Algebraické prvky	16
2.2	Korene polynómu v nadpoli	17
2.3	Separabilné polynómy	20
2.4	Rozšírenie poľa, Galoisova grupa.	22
2.5	Konečné rozšírenie	23
2.6	Symetrické polynómy	27
2.7	Hlavná veta algebry	33
3	Algebraický uzáver poľa	35
4	Jednoduché rozšírenie	37
5	Cyklotomické polynómy	39
5.1	Primitívna odmocnina z 1	40
5.2	Redukcia polynómu modulo prvočíslo	41
6	Izomorfizmy polí	44
6.1	Rozšírenia izomorfizmov	44
6.2	Rozkladové pole	46
6.3	Mohutnosť konečných polí	49
6.4	Ireducibilita nad konečnými poľami	49
6.5	Ireducibilita nad Z a Q	51
6.6	Zriedkavosť reducibility	53
6.7	Eisensteinovo kritérium ireducibility	55
6.8	Rád Galoisovej grupy	56
6.9	Galoisova grupa polynómu	58
6.10	Vnorenie do grupy permutácií	60

7	Riešiteľnosť v radikáloch	62
7.1	Riešiteľné grupy	63
7.2	Cauchyho veta	64
7.3	Centrum grupy	66
7.4	Neriešiteľnosť S_n	68
7.5	Generátory grupy S_n	68
7.6	Neriešiteľné Galoisove grupy	70
8	Riešiteľnosť v radikáloch podľa Galoisovej grupy	71
8.1	Normálne rozšírenie.	71
8.2	Odmocniny z 1	73
8.3	Charaktery grupy v poli	75
8.4	Noetherovej systémy	78
8.5	Rozklad konečnej komutatívnej grupy	82
8.6	Kummerovské polia	86
8.7	Galoisova korešpondencia.	87
9	Euklidovské geometrické konštrukcie	89
9.1	Pravidelné mnohoholníky	94
10	Konštrukcia Galoisovej grupy	97
10.1	Tranzitívnosť grupy	97
10.2	Frobeniov automorfizmus	99
10.3	Okruhy s jednoznačným rozkladom	101
10.4	Permutácie neurčitých	104
10.5	Redukcia modulo prvočíslo	106
10.6	Zriedkavosť riešiteľnosti v radikáloch	109
11	Dodatky	111
11.1	Zornova lema a jej ekvivalenty	111
11.2	Wedderburnova veta	116
11.3	Hlavná veta algebry II	118

11.4 Cardanov vzorec	121
12 Doplnky	123
12.1 Rozklad grupy podľa podgrupy	123
12.2 Rád prvku v grupe	124
12.3 Cyklická podgrupa	125
12.4 Faktorové grupy	125
12.5 Homomorfizmus grúp	127
12.6 Súčin podgrúp	128
12.7 Faktorové okruhy	130
12.8 Rozklad permutácií na cykly	131
12.9 Deliteľnosť polynómov	132