

# Table des matières

<b>1</b>	<b>Anneaux, morphismes et idéaux</b>	<b>1</b>
1.1	Définition . . . . .	1
1.2	Idéaux . . . . .	5
1.3	Anneaux quotients . . . . .	7
1.4	Somme et produit d'idéaux . . . . .	15
<b>2</b>	<b>Séries formelles, anneaux des polynômes</b>	<b>19</b>
2.1	Séries formelles, polynômes . . . . .	19
2.2	Division avec reste dans l'anneau des polynômes . . . . .	22
2.3	Polynômes à plusieurs variables . . . . .	25
2.4	Polynômes symétriques . . . . .	26
<b>3</b>	<b>Localisation, corps des fractions</b>	<b>31</b>
3.1	Idéaux premiers, idéaux maximaux . . . . .	31
3.2	Localisation . . . . .	33
<b>4</b>	<b>Anneaux principaux</b>	<b>39</b>
4.1	Divisibilité . . . . .	39
4.2	Anneaux principaux . . . . .	42
4.3	Anneaux euclidiens . . . . .	43
4.4	Éléments irréductibles, éléments premiers . . . . .	45
4.5	Polynômes sur un corps . . . . .	47
4.6	Corps finis . . . . .	49
<b>5</b>	<b>Théorème chinois</b>	<b>55</b>
5.1	Théorème chinois . . . . .	55
5.2	Algorithme de Garner . . . . .	56
5.3	Partage de secret . . . . .	60
<b>6</b>	<b>Anneaux factoriels</b>	<b>63</b>
6.1	Anneaux factoriels . . . . .	63
6.2	Les anneaux principaux sont factoriels . . . . .	66

6.3	Théorème des deux carrés . . . . .	67
<b>7</b>	<b>Polynômes sur un anneau factoriel</b>	<b>73</b>
7.1	$A$ factoriel implique $A[X]$ factoriel . . . . .	73
7.2	Tests d'irréductibilité . . . . .	77
7.3	Pgcd de polynômes . . . . .	80
<b>8</b>	<b>Factorisation et racines de polynômes</b>	<b>83</b>
8.1	Partie sans facteur carré . . . . .	83
8.2	Algorithme de Kronecker . . . . .	86
8.3	Algorithme de Berlekamp . . . . .	88
8.4	Racines réelles . . . . .	91
<b>9</b>	<b>Extensions de corps</b>	<b>95</b>
9.1	Degré d'une extension . . . . .	95
9.2	Extensions algébriques . . . . .	99
9.3	Constructions à la règle et au compas . . . . .	102
<b>10</b>	<b>Clôture algébrique, extensions séparables</b>	<b>107</b>
10.1	Corps de décomposition . . . . .	107
10.2	Clôture algébrique . . . . .	110
10.3	Extensions séparables, élément primitif . . . . .	112
<b>11</b>	<b>Racines de l'unité, corps finis</b>	<b>117</b>
11.1	Racines de l'unité . . . . .	117
11.2	Corps finis . . . . .	120
<b>12</b>	<b>Codes correcteurs d'erreurs</b>	<b>127</b>
<b>13</b>	<b>Résultants</b>	<b>135</b>
13.1	Élimination et matrice de Sylvester . . . . .	135
13.2	Formule de Héron . . . . .	139
13.3	Théorème d'extension . . . . .	140
13.4	Calcul via l'algorithme d'Euclide . . . . .	143
13.5	Résultant et racines . . . . .	144
13.6	Factorisation sur une extension algébrique . . . . .	147
<b>14</b>	<b>Corrigés de certains exercices</b>	<b>155</b>
	<b>Bibliographie</b>	<b>181</b>