

Ina Kersten

# Algebra

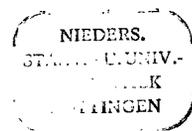
L<sup>A</sup>T<sub>E</sub>X-Bearbeitung von  
Ole Riedlin



Universitätsverlag Göttingen  
2006

# Inhaltsverzeichnis

0	Worum geht es? . . . . .	13
<b>Gruppen</b>		<b>17</b>
1	Die Isomorphiesätze der Gruppentheorie . . . . .	17
1.1	Einige Grundbegriffe . . . . .	17
1.2	Aussagen über Bild und Urbild . . . . .	19
1.3	Homomorphiesatz . . . . .	20
1.4	Ein Untergruppenkriterium . . . . .	20
1.5	Erster Noetherscher Isomorphiesatz . . . . .	21
1.6	Zweiter Noetherscher Isomorphiesatz . . . . .	22
1.7	Übungsaufgaben 5 – 10 . . . . .	22
2	Die Sylowschen Sätze . . . . .	24
2.1	Hilfssatz über Binomialkoeffizienten . . . . .	24
2.2	Abzählformel und Bahnformel . . . . .	25
2.3	Erster Sylowscher Satz . . . . .	26
2.4	Satz von Cauchy . . . . .	27
2.5	Gruppen der Ordnung 6 . . . . .	27
2.6	$p$ -Gruppen . . . . .	28
2.7	$p$ -Sylowgruppen . . . . .	28
2.8	Zweiter Sylowscher Satz . . . . .	29
2.9	Folgerungen . . . . .	29
2.10	Der Normalisator einer Untergruppe . . . . .	30
2.11	Dritter Sylowscher Satz . . . . .	31
2.12	Satz von Lagrange . . . . .	31
2.13	Gruppen der Ordnung 15 . . . . .	32
2.14	Übungsaufgaben 11 – 16 . . . . .	34
3	Strukturaussagen über einige Gruppen . . . . .	35
3.1	Die Klassengleichung . . . . .	35
3.2	Das Zentrum einer $p$ -Gruppe ist nicht-trivial . . . . .	36
3.3	Existenz von Normalteilern in $p$ -Gruppen . . . . .	36
3.4	Zyklische Gruppen . . . . .	37



3.5	Gruppen der Ordnung $p^2$	37
3.6	Gruppen der Ordnung $2p$	38
3.7	Direkte Produkte von Normalteilern	39
3.8	Endliche abelsche Gruppen	40
3.9	Übungsaufgaben 17 – 22	42
4	Auflösbare Gruppen	43
4.1	Definition einer auflösbaren Gruppe	43
4.2	Beispiele	43
4.3	Untergruppen und Bilder auflösbarer Gruppen	43
4.4	Verfeinerung von Normalreihen	44
4.5	Kommutatorgruppen	46
4.6	Beispiele	46
4.7	Iterierte Kommutatorgruppen	47
4.8	Kriterium für Auflösbarkeit mit Kommutatoren	48
4.9	Übungsaufgaben 23–26	48
5	Exkurs über Permutationsgruppen	49
5.1	Symmetrische Gruppe $S_n$	49
5.2	Zyklen	50
5.3	Kanonische Zyklenzerlegung einer Permutation	50
5.4	Das Vorzeichen einer Permutation	51
5.5	Alternierende Gruppe $A_n$	53
5.6	Einfachheit von $A_n$ für $n \geq 5$	53
5.7	$S_n$ ist für $n \geq 5$ nicht auflösbar	55
5.8	Bemerkung über Transpositionen	55
5.9	Übungsaufgaben 27 – 30	56
<b>Ringe</b>		<b>57</b>
6	Grundbegriffe der Ringtheorie	57
6.1	Definition eines Ringes	57
6.2	Einheiten und Nullteiler	58
6.3	Beispiele	58
6.4	Unterringe	59
6.5	Ideale	59
6.6	Summe, Durchschnitt und Produkt von Idealen	60
6.7	Erzeugung von Idealen	61
6.8	Hauptidealringe	61
6.9	Ringhomomorphismen	62
6.10	Quotientenringe	63
6.11	Quotientenkörper	64
6.12	Polynomringe	65
6.13	Der Grad eines Polynoms	66
6.14	Hilbertscher Basissatz	67

6.15	Übungsaufgaben 31 – 35 . . . . .	68
7	Restklassenringe . . . . .	69
7.1	Kongruenzen . . . . .	69
7.2	Rechnen mit Restklassen . . . . .	70
7.3	Ideale im Restklassenring . . . . .	71
7.4	Primideale und maximale Ideale . . . . .	71
7.5	Das Zornsche Lemma . . . . .	72
7.6	Existenz maximaler Ideale . . . . .	73
7.7	Der Homomorphiesatz für Ringe . . . . .	73
7.8	Chinesischer Restsatz . . . . .	73
7.9	Übungsaufgaben 36 – 40 . . . . .	76
8	Teilbarkeit in kommutativen Ringen . . . . .	77
8.1	Division mit Rest im Polynomring . . . . .	77
8.2	Nullstellen und Linearfaktoren . . . . .	77
8.3	Euklidische Ringe . . . . .	78
8.4	ggT und kgV . . . . .	79
8.5	Irreduzible Elemente und Primelemente . . . . .	80
8.6	Assoziierte Elemente . . . . .	81
8.7	Eindeutigkeit von Primfaktorzerlegungen . . . . .	81
8.8	Primfaktorzerlegung in Hauptidealringen . . . . .	82
8.9	Faktorielle Ringe . . . . .	82
8.10	Existenz von ggT und kgV in faktoriellen Ringen . . . . .	83
8.11	Spezielle Version des Chinesischen Restsatzes . . . . .	84
8.12	Beispiele für Körper . . . . .	84
8.13	Übungsaufgaben 41 – 44 . . . . .	85
9	Primfaktorzerlegung in Polynomringen . . . . .	86
9.1	Hilfssatz über Primelemente . . . . .	86
9.2	Primitive Polynome . . . . .	86
9.3	Übergang zum Quotientenkörper von $R$ . . . . .	87
9.4	Satz von Gauß . . . . .	88
9.5	Umkehrung des Satzes von Gauß . . . . .	88
9.6	Wann ist ein Polynomring ein Hauptidealring? . . . . .	88
9.7	Eisensteinsches Irreduzibilitätskriterium . . . . .	89
9.8	Eisensteinpolynome . . . . .	90
9.9	Irreduzibilitätsnachweis durch Substitution . . . . .	90
9.10	Das $p$ -te Kreisteilungspolynom . . . . .	90
9.11	Reduktionssatz . . . . .	91
9.12	Beispiel zum Reduktionssatz . . . . .	92
9.13	Übungsaufgaben 45 – 48 . . . . .	92
10	$R$ -Moduln . . . . .	93
10.1	Links- und Rechtsmoduln . . . . .	93
10.2	Beispiele für $R$ -Moduln . . . . .	93

10.3	<i>R</i> -Modulhomomorphismen . . . . .	94
10.4	Untermodul . . . . .	94
10.5	Erzeugendensysteme . . . . .	94
10.6	Beispiele für freie Moduln . . . . .	95
10.7	Definition des Tensorprodukts . . . . .	95
10.8	Universelle Eigenschaft des Tensorproduktes . . . . .	96
10.9	Folgerungen . . . . .	96
10.10	Das Tensorprodukt von direkten Summen . . . . .	97
10.11	Tensorprodukt mit einem freien Modul . . . . .	97
10.12	Hauptsatz über endlich erzeugte abelsche Gruppen . . . . .	98
10.13	Übungsaufgaben 49–50 . . . . .	103
<b>Körper</b>		<b>105</b>
11	Grundbegriffe der Körpertheorie . . . . .	105
11.1	Wiederholung der Definition eines Körpers . . . . .	105
11.2	Teilkörper und Körpererweiterungen . . . . .	105
11.3	Erzeugung und Adjunktion . . . . .	106
11.4	Isomorphismen und <i>K</i> -Isomorphismen . . . . .	106
11.5	Die Charakteristik eines Integritätsrings . . . . .	107
11.6	Primkörper . . . . .	107
11.7	Der Grad einer Körpererweiterung . . . . .	108
11.8	Algebraische und transzendente Elemente . . . . .	109
11.9	Das Minimalpolynom . . . . .	109
11.10	Satz über den Grad des Minimalpolynoms . . . . .	109
11.11	Beispiele . . . . .	110
11.12	Charakterisierung algebraischer Elemente . . . . .	111
11.13	Einfache Körpererweiterungen . . . . .	111
11.14	Übungsaufgaben 51 – 54 . . . . .	112
12	Algebraische Körpererweiterungen . . . . .	113
12.1	Endliche und algebraische Körpererweiterungen . . . . .	113
12.2	Der algebraische Abschluss von <i>K</i> in <i>L</i> . . . . .	114
12.3	Die Eigenschaft „algebraisch“ ist transitiv . . . . .	114
12.4	Existenz von Nullstellen in Körpererweiterungen . . . . .	114
12.5	Existenz eines Zerfällungskörpers . . . . .	115
12.6	Differenziation und mehrfache Nullstellen . . . . .	116
12.7	Übungsaufgaben 55 – 59 . . . . .	117
13	Normale Körpererweiterungen . . . . .	118
13.1	Ein Fortsetzungslemma . . . . .	118
13.2	Eindeutigkeit des Zerfällungskörpers . . . . .	119
13.3	Endliche normale Körpererweiterungen . . . . .	119
13.4	Einbettung in eine normale Erweiterung . . . . .	120
13.5	Der Satz vom primitiven Element . . . . .	120

13.6	Übungsaufgaben 60–64	122
<b>14</b>	<b>Endliche Körper</b>	<b>123</b>
14.1	Satz über die Ordnung von Gruppenelementen	123
14.2	Endliche Untergruppen von $K^*$ sind zyklisch	124
14.3	Anzahl der Elemente eines endlichen Körpers	124
14.4	Der Körper mit $p^n$ Elementen	125
14.5	Kleiner Satz von Fermat	125
14.6	Satz von Wilson	126
14.7	Übungsaufgaben 65 – 69	126
<b>Galoisttheorie</b>		<b>127</b>
<b>15</b>	<b>Galoiserweiterungen</b>	<b>127</b>
15.1	Fixkörper	127
15.2	Wirkung einer endlichen Untergruppe von $\text{Aut}(L)$	128
15.3	Beispiel	129
15.4	Der Grad über dem Fixkörper	129
15.5	Die Galoisgruppe einer Körpererweiterung	130
15.6	Satz über die Ordnung der Galoisgruppe	130
15.7	Definition einer Galoiserweiterung	131
15.8	Charakterisierung von Galoiserweiterungen	131
15.9	Einbettung in eine Galoiserweiterung	132
15.10	Übungsaufgaben 70 – 71	132
<b>16</b>	<b>Hauptsatz der Galoistheorie</b>	<b>133</b>
16.1	Hauptsatz	133
16.2	Beispiel	134
16.3	Wann ist ein Zwischenkörper galoissch über $K$ ?	134
16.4	Beispiel	135
16.5	Abelsche und zyklische Erweiterungen	136
16.6	Zwischenkörper einer zyklischen Erweiterung	136
16.7	Der Frobenius-Homomorphismus	137
16.8	Vollkommene Körper	137
16.9	Bemerkung über Zwischenkörper	138
16.10	Übungsaufgaben 72 – 74	138
<b>Anwendungen und Ergänzungen</b>		<b>139</b>
<b>17</b>	<b>Einheitswurzelkörper</b>	<b>139</b>
17.1	Einheitswurzeln	139
17.2	Die Eulersche $\varphi$ -Funktion	140
17.3	Primitive $n$ -te Einheitswurzeln	141
17.4	Der $n$ -te Einheitswurzelkörper ist abelsch	141
17.5	Das $n$ -te Kreisteilungspolynom	141
17.6	Irreduzibilität in $\mathbb{Q}[X]$	143

17.7	Übungsaufgaben 75–76 . . . . .	144
<b>18</b>	<b>Auflösbarkeit von Gleichungen . . . . .</b>	<b>145</b>
18.1	Galoisgruppe eines Polynoms . . . . .	145
18.2	Radikalerweiterung . . . . .	145
18.3	Galoisgruppe einer reinen Gleichung . . . . .	145
18.4	Lineare Unabhängigkeit von Charakteren . . . . .	146
18.5	Kompositum von Zwischenkörpern . . . . .	147
18.6	Gleichungen mit auflösbarer Galoisgruppe . . . . .	148
18.7	Durch Radikale auflösbare Gleichungen . . . . .	148
18.8	Nicht auflösbare Gleichungen vom Grad $p$ . . . . .	149
18.9	Rationaler Funktionenkörper . . . . .	150
18.10	Symmetrische Funktionen . . . . .	151
18.11	Die allgemeine Gleichung $n$ -ten Grades . . . . .	152
18.12	Übungsaufgaben 77–80 . . . . .	153
<b>19</b>	<b>Konstruierbarkeit mit Zirkel und Lineal . . . . .</b>	<b>154</b>
19.1	Konstruktion von Senkrechten und Parallelen . . . . .	154
19.2	Lemma über konstruierbare Punkte . . . . .	155
19.3	Wurzeln konstruierbarer Punkte . . . . .	157
19.4	Algebraische Formulierung der Konstruierbarkeit . . . . .	157
19.5	Konstruierbare Punkte haben 2-Potenzgrad . . . . .	159
19.6	Delisches Problem der Würfelverdoppelung . . . . .	160
19.7	Problem der Quadratur des Kreises . . . . .	160
19.8	Problem der Winkeldreiteilung . . . . .	160
19.9	Regelmäßige $n$ -Ecke . . . . .	161
<b>20</b>	<b>Algebraischer Abschluss eines Körpers . . . . .</b>	<b>162</b>
20.1	Algebraisch abgeschlossene Körper . . . . .	162
20.2	Definition des algebraischen Abschlusses . . . . .	163
20.3	Polynomringe in beliebig vielen Unbestimmten . . . . .	163
20.4	Existenz des algebraischen Abschlusses . . . . .	164
20.5	Eindeutigkeit des algebraischen Abschlusses . . . . .	165
20.6	Universelle Eigenschaft des Polynomrings . . . . .	166
	<b>Literaturverzeichnis</b>	<b>168</b>
	<b>Index</b>	<b>169</b>