桑木文庫
洋書
0449

DAVID HILBERT
GESAMMELTE ABHANDLUNGEN

ERSTER BAND

ZAHLENTHEORIE

BERLIN
VERLAG VON JULIUS SPRINGER
1932

桑木文庫
洋書
0449

物理
08
H
12.1

九州帝國大學理學部
8347
物理學教室

九州帝國大學工學部
810441
1932年7月15日
數學物理學教室

DAVID HILBERT
GESAMMELTE ABHANDLUNGEN

ERSTER BAND

ZAHLENTHEORIE

理学部 洋 遡及
022232002006815
九州大学蔵書

数学・物理学図書室

BERLIN
VERLAG VON JULIUS SPRINGER
1932

物理
08
H
12.1

九州帝國大學理學部
8347
物理學教室

九州帝國大學工學部
810441
1932年7月15日
數學物理學教室

DAVID HILBERT
GESAMMELTE ABHANDLUNGEN

ERSTER BAND

ZAHLENTHEORIE

理学部 洋 遡及
022232002006815
九州大学蔵書

九州帝國大學圖書之印

BERLIN
VERLAG VON JULIUS SPRINGER
1932

ALLE RECHTE, INSBESONDERE DAS DER ÜBERSETZU
IN FREMDE SPRACHEN, VORBEHALTEN.
COPYRIGHT 1932 BY JULIUS SPRINGER IN BERLIN
PRINTED IN GERMANY.

19. 4. 25
130641

Vorwort.

Der Plan einer Herausgabe meiner Abhandlungen ist durch die Großzügigkeit von FERDINAND SPRINGER verwirklicht worden. Ihm und meinem Freunde RICHARD COURANT bin ich wegen ihrer stets bereiten, durch Rat und Tat wirksamen Hilfe zu größtem Dank verpflichtet.

Die wissenschaftliche Arbeit bei der Herausgabe hat nicht nur äußerste Sorgfalt, sondern auch feinstes Verständnis erfordert und konnte daher nur geleistet werden von Gelehrten, die durch gründliche Studien in den dabei behandelten Fächern dazu vorbereitet sind. Diese Aufgabe ist für den vorliegenden ersten Band, der insbesondere meinen großen zahlentheoretischen Bericht enthält, in vollkommener Weise von den Mathematikern WILHELM MAGNUS, OLGA TAUSSKY, HELMUT ULM gelöst worden. Die Entwicklung der Theorie der algebraischen Zahlen bis in die neueste Zeit wird in dem Nachwort von H. HASSE dargestellt.

Für die drei weiteren Bände ist die Verteilung des Stoffes in folgender Weise beabsichtigt:

Band II: Geometrie, Algebra und Invariantentheorie,
Band III: Analysis,
Band IV: Verschiedenes.

Außer den hier genannten Mathematikern spreche ich noch allen denen, die an diesen Arbeiten Anteil genommen haben, meinen wärmsten Dank aus und hoffe, daß die Veranstaltung dieser Gesamtausgabe wegen der mannigfachen Fragen, die darin berührt werden, insbesondere der jungen Generation Anregung bieten und damit am besten unserer geliebten mathematischen Wissenschaft zur Förderung dienen wird.

Göttingen, im April 1932.

DAVID HILBERT.

ALLE RECHTE, INSBESONDERE DAS DER ÜBERSETZUNG
IN FREMDE SPRACHEN, VORBEHALTEN.
COPYRIGHT 1932 BY JULIUS SPRINGER IN BERLIN.
PRINTED IN GERMANY.

Vorwort.

Der Plan einer Herausgabe meiner Abhandlungen ist durch die Großzügigkeit von FERDINAND SPRINGER verwirklicht worden. Ihm und meinem Freunde RICHARD COURANT bin ich wegen ihrer stets bereiten, durch Rat und Tat wirksamen Hilfe zu größtem Dank verpflichtet.

Die wissenschaftliche Arbeit bei der Herausgabe hat nicht nur äußerste Sorgfalt, sondern auch feinstes Verständnis erfordert und konnte daher nur geleistet werden von Gelehrten, die durch gründliche Studien in den dabei behandelten Fächern dazu vorbereitet sind. Diese Aufgabe ist für den vorliegenden ersten Band, der insbesondere meinen großen zahlentheoretischen Bericht enthält, in vollkommener Weise von den Mathematikern WILHELM MAGNUS, OLGA TAUSSKY, HELMUT ULM gelöst worden. Die Entwicklung der Theorie der algebraischen Zahlen bis in die neueste Zeit wird in dem Nachwort von H. HASSE dargestellt.

Für die drei weiteren Bände ist die Verteilung des Stoffes in folgender Weise beabsichtigt:

Band II: Geometrie, Algebra und Invariantentheorie,
Band III: Analysis,
Band IV: Verschiedenes.

Außer den hier genannten Mathematikern spreche ich noch allen denen, die an diesen Arbeiten Anteil genommen haben, meinen wärmsten Dank aus und hoffe, daß die Veranstaltung dieser Gesamtausgabe wegen der mannigfachen Fragen, die darin berührt werden, insbesondere der jungen Generation Anregung bieten und damit am besten unserer geliebten mathematischen Wissenschaft zur Förderung dienen wird.

Göttingen, im April 1932.

DAVID HILBERT.

高等教育出版社

Inhaltsverzeichnis.

Seite

1. Über die Transzendenz der Zahlen e und π 1
[Nachrichten der Gesellschaft der Wissenschaften zu Göttingen S. 113—116 (1893). Mathem. Annalen Bd. 43, S. 216—219 (1893).]

2. Zwei neue Beweise für die Zerlegbarkeit der Zahlen eines Körpers in Primideale 5
[Jahresbericht der Deutschen Mathematikervereinigung Bd. 3, S. 59 (1894).]

3. Über die Zerlegung der Ideale eines Zahlkörpers in Primideale 6
[Mathem. Annalen Bd. 44, S. 1—8 (1894).]

4. Grundzüge einer Theorie des Galoisschen Zahlkörpers 13
[Nachrichten der Gesellschaft der Wissenschaften zu Göttingen S. 224—236 (1894).]

5. Über den Dirichletschen biquadratischen Zahlkörper 24
[Mathem. Annalen Bd. 45, S. 309—340 (1894).]

Einleitung 24
§ 1. Die ganzen Zahlen des Dirichletschen Zahlkörpers 25
§ 2. Die Primideale des Dirichletschen Körpers 26
§ 3. Die Einteilung der Idealklassen in Geschlechter 28
§ 4. Die Erzeugung der Idealklassen des Hauptgeschlechtes 32
§ 5. Die ambigen Ideale 37
§ 6. Die ambigen Klassen 38
§ 7. Die Anzahl der existierenden Geschlechter 42
§ 8. Das Reziprozitätsgesetz 43
§ 9. Der spezielle Dirichletsche Körper 47
§ 10. Die Anzahl der Idealklassen des speziellen Dirichletschen Körpers K . 48

6. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper 53
[Nachrichten der Gesellschaft der Wissenschaften zu Göttingen S. 29—39 (1896).]

7. Die Theorie der algebraischen Zahlkörper 63
[Jahresbericht der Deutschen Mathematikervereinigung Bd. 4, S. 175—546 (1897).]

Vorwort 63

Erster Teil. *Die Theorie des allgemeinen Zahlkörpers.*

1. Die algebraische Zahl und der Zahlkörper 69
§ 1. Der Zahlkörper und die konjugierten Zahlkörper 69
§ 2. Die ganze algebraische Zahl 70
§ 3. Die Norm, die Differente, die Diskriminante einer Zahl. Die Basis des Zahlkörpers 71

Seite

2. Die Ideale des Zahlkörpers 73
§ 4. Die Multiplikation der Ideale und ihre Teilbarkeit. Das Primideal . . . 73
§ 5. Die eindeutige Zerlegbarkeit eines Ideals in Primideale 75
§ 6. Die Formen des Zahlkörpers und ihre Inhalte 77

3. Die Kongruenzen nach Idealen 79
§ 7. Die Norm eines Ideals und ihre Eigenschaften 79
§ 8. Der Fermatsche Satz in der Idealtheorie und die Funktion $\varphi(a)$ . . . 82
§ 9. Die Primitivzahlen nach einem Primideal 83

4. Die Diskriminante des Körpers und ihre Teiler. 84
§ 10. Der Satz über die Teiler der Diskriminante des Körpers. Hilfssätze über ganze Funktionen 84
§ 11. Die Zerlegung der linken Seite der Fundamentalgleichung. Die Diskriminante der Fundamentalgleichung 88
§ 12. Die Elemente und die Differente des Körpers. Beweis des Satzes über die Teiler der Körperdiskriminante 90
§ 13. Die Aufstellung der Primideale. Der feste Zahlteiler der rationalen Einheitsform U 91

5. Der Relativkörper 92
§ 14. Die Relativnorm, die Relativdifferente und die Relativdiskriminante . . 92
§ 15. Eigenschaften der Relativdifferente und der Relativdiskriminante eines Körpers 95
§ 16. Die Zerlegung eines Elementes des Körpers k im Oberkörper K. Der Satz von der Differente des Oberkörpers K 97

6. Die Einheiten des Körpers 98
§ 17. Die Existenz konjugierter Zahlen, deren absolute Beträge gewissen Ungleichungen genügen 98
§ 18. Sätze über die absolute Größe der Körperdiskriminante 100
§ 19. Der Satz von der Existenz der Einheiten eines Körpers. Ein Hilfssatz über die Existenz einer Einheit von besonderer Eigenschaft 102
§ 20. Beweis des Satzes von der Existenz der Einheiten 106
§ 21. Die Grundeinheiten. Der Regulator des Körpers. Ein System von unabhängigen Einheiten 108

7. Die Idealklassen des Körpers 109
§ 22. Die Idealklasse. Die Endlichkeit der Anzahl der Idealklassen 109
§ 23. Anwendungen des Satzes von der Endlichkeit der Klassenanzahl 110
§ 24. Aufstellung des Systems der Idealklassen. Engere Fassung des Klassenbegriffes 112
§ 25. Ein Hilfssatz über den asymptotischen Wert der Anzahl aller Hauptideale, welche durch ein festes Ideal teilbar sind 112
§ 26. Die Bestimmung der Klassenanzahl durch das Residuum der Funktion $\zeta(s)$ für $s = 1$ 115
§ 27. Andere unendliche Entwicklungen der Funktion $\zeta(s)$ 117
§ 28. Die Zusammensetzung der Idealklassen eines Körpers 118
§ 29. Die Charaktere einer Idealklasse. Eine Verallgemeinerung der Funktion $\zeta(s)$ 119

8. Die zerlegbaren Formen des Körpers 119
§ 30. Die zerlegbaren Formen des Körpers. Die Formenklassen und ihre Zusammensetzung 119

Seite

9. Die Zahlringe des Körpers 121
§ 31. Der Zahlring. Das Ringideal und seine wichtigsten Eigenschaften . . . 121
§ 32. Die durch eine ganze Zahl bestimmten Ringe. Der Satz von der Differente einer ganzen Zahl des Körpers 122
§ 33. Die regulären Ringideale und ihre Teilbarkeitsgesetze 126
§ 34. Die Einheiten eines Ringes. Die Ringklassen 127
§ 35. Der Modul und die Modulklasse. 128

Zweiter Teil. *Der Galoissche Zahlkörper.*

10. Die Primideale des Galoisschen Körpers und seiner Unterkörper 129
§ 36. Die eindeutige Zerlegung der Ideale des Galoisschen Körpers in Primideale 129
§ 37. Die Elemente, die Differente und die Diskriminante des Galoisschen Körpers 131
§ 38. Die Unterkörper des Galoisschen Körpers 131
§ 39. Der Zerlegungskörper und der Trägheitskörper eines Primideals $\mathfrak{P}$ . . . 132
§ 40. Ein Satz über den Zerlegungskörper 134
§ 41. Der Verzweigungskörper eines Primideals $\mathfrak{P}$ 134
§ 42. Ein Satz über den Trägheitskörper 135
§ 43. Sätze über die Verzweigungsgruppe und den Verzweigungskörper. . . . 136
§ 44. Die überstrichenen Verzweigungskörper eines Primideals $\mathfrak{P}$. 136
§ 45. Kurze Zusammenfassung der Sätze über die Zerlegung einer rationalen Primzahl p im Galoisschen Körper 138

11. Die Differenten und Diskriminanten des Galoisschen Körpers und seiner Unterkörper 139
§ 46. Die Differenten des Trägheitskörpers und der Verzweigungskörper . . . 139
§ 47. Die Teiler der Diskriminante des Galoisschen Körpers 140

12. Die Beziehungen der arithmetischen zu algebraischen Eigenschaften des Galoisschen Körpers 141
§ 48. Der relativ-Galoissche, der relativ-Abelsche und der relativ-zyklische Körper 141
§ 49. Die algebraischen Eigenschaften des Trägheitskörpers und der Verzweigungskörper. Die Darstellung der Zahlen des Galoisschen Körpers durch Wurzeln im Bereiche des Zerlegungskörpers 142
§ 50. Die Dichtigkeit der Primideale ersten Grades und der Zusammenhang dieser Dichtigkeit mit den algebraischen Eigenschaften eines Zahlkörpers 142

13. Die Zusammensetzung der Zahlkörper 144
§ 51. Der aus einem Körper und dessen konjugierten Körpern zusammengesetzte Galoissche Körper 144
§ 52. Die Zusammensetzung zweier Körper, deren Diskriminanten zueinander prim sind 145

14. Die Primideale ersten Grades und der Klassenbegriff 146
§ 53. Die Erzeugung der Idealklassen durch Primideale ersten Grades 146

15. Der relativ-zyklische Körper vom Primzahlgrade 149
§ 54. Die symbolische Potenz. Der Satz von den Zahlen mit der Relativnorm 1 149
§ 55. Das System von relativen Grundeinheiten und der Nachweis ihrer Existenz 150
§ 56. Die Existenz einer Einheit in K, welche die Relativnorm 1 besitzt und doch nicht dem Quotienten zweier relativ-konjugierten Einheiten gleich wird 152
§ 57. Die ambigen Ideale und die Relativdifferente des relativ-zyklischen Körpers K 154
§ 58. Der Fundamentalsatz von den relativ-zyklischen Körpern mit der Relativdifferente 1. Die Bezeichnung dieser Körper als Klassenkörper 155

Seite

Dritter Teil. *Der quadratische Zahlkörper.*

16. Die Zerlegung der Zahlen im quadratischen Körper 157
§ 59. Die Basis und die Diskriminante des quadratischen Körpers 157
§ 60. Die Primideale des quadratischen Körpers 158
§ 61. Das Symbol $\left(\frac{a}{w}\right)$ 160
§ 62. Die Einheiten des quadratischen Körpers 160
§ 63. Die Aufstellung des Systems der Idealklassen 161
17. Die Geschlechter im quadratischen Körper und ihre Charakterensysteme . . 161
§ 64. Das Symbol $\left(\frac{n,m}{w}\right)$ 161
§ 65. Das Charakterensystem eines Ideals 166
§ 66. Das Charakterensystem einer Idealklasse und der Begriff des Geschlechts 167
§ 67. Der Fundamentalsatz über die Geschlechter des quadratischen Körpers . 168
§ 68. Ein Hilfssatz über diejenigen quadratischen Körper, deren Diskriminanten nur durch eine einzige Primzahl teilbar sind 168
§ 69. Das Reziprozitätsgesetz für quadratische Reste. Ein Hilfssatz über das Symbol $\left(\frac{n,m}{w}\right)$ 169
§ 70. Beweis der im Fundamentalsatz 100 ausgesprochenen Beziehung zwischen den sämtlichen Charakteren eines Geschlechts 172
18. Die Existenz der Geschlechter im quadratischen Körper 173
§ 71. Der Satz von den Normen der Zahlen eines quadratischen Körpers . . . 173
§ 72. Die Klassen des Hauptgeschlechtes 175
§ 73. Die ambigen Ideale 176
§ 74. Die ambigen Idealklassen 176
§ 75. Die durch ambige Ideale bestimmten ambigen Idealklassen 177
§ 76. Die ambigen Idealklassen, welche kein ambiges Ideal enthalten 178
§ 77. Die Anzahl aller ambigen Klassen 179
§ 78. Der arithmetische Beweis für die Existenz der Geschlechter 180
§ 79. Die transzendente Darstellung der Klassenanzahl und eine Anwendung darauf, daß der Grenzwert eines gewissen unendlichen Produktes positiv ist 181
§ 80. Das Vorhandensein unendlich vieler rationaler Primzahlen, nach denen gegebene Zahlen vorgeschriebene quadratische Restcharaktere erlangen . 182
§ 81. Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Charakteren in einem quadratischen Körper 184
§ 82. Der transzendente Beweis für die Existenz der Geschlechter und für die übrigen in § 71 bis § 77 erlangten Resultate 186
§ 83. Die engere Fassung des Äquivalenz- und Klassenbegriffes 186
§ 84. Der Fundamentalsatz für den neuen Klassen- und Geschlechtsbegriff . 187
19. Die Bestimmung der Anzahl der Idealklassen des quadratischen Körpers . . 188
§ 85. Das Symbol $\left(\frac{a}{n}\right)$ für eine zusammengesetzte Zahl n 188
§ 86. Der geschlossene Ausdruck für die Anzahl der Idealklassen 188
§ 87. Der Dirichletsche biquadratische Zahlkörper 191
20. Die Zahlringe und Moduln des quadratischen Körpers 192
§ 88. Die Zahlringe des quadratischen Körpers 192
§ 89. Ein Satz von den Modulklassen des quadratischen Körpers. Die binären quadratischen Formen 192
§ 90. Die niedere und die höhere Theorie des quadratischen Zahlkörpers . . . 194

Seite

Vierter Teil. *Der Kreiskörper.*

21. Die Einheitswurzeln mit Primzahlexponent l und der durch sie bestimmte Kreiskörper. 195
§ 91. Der Grad des Kreiskörpers der l-ten Einheitswurzeln und die Zerlegung der Primzahl l in diesem Körper 195
§ 92. Die Basis und die Diskriminante des Kreiskörpers der l-ten Einheitswurzeln 196
§ 93. Die Zerlegung der von l verschiedenen rationalen Primzahlen im Kreiskörper der l-ten Einheitswurzeln 197
22. Die Einheitswurzeln für einen zusammengesetzten Wurzelexponenten m und der durch sie bestimmte Kreiskörper 198
§ 94. Der Kreiskörper der m-ten Einheitswurzeln 198
§ 95. Der Grad des Kreiskörpers der l^h-ten Einheitswurzeln und die Zerlegung der Primzahl l in diesem Körper 199
§ 96. Die Basis und die Diskriminante des Kreiskörpers der l^h-ten Einheitswurzeln 200
§ 97. Der Kreiskörper der m-ten Einheitswurzeln. Der Grad, die Diskriminante und die Primideale dieses Körpers 200
§ 98. Die Einheiten des Kreiskörpers $k\left(e^{\frac{2i\pi}{m}}\right)$. Die Definition der Kreiseinheiten 203
23. Der Kreiskörper in seiner Eigenschaft als Abelscher Körper 205
§ 99. Die Gruppe des Kreiskörpers der m-ten Einheitswurzeln 205
§ 100. Der allgemeine Begriff des Kreiskörpers. Der Fundamentalsatz über die Abelschen Körper 206
§ 101. Ein allgemeiner Hilfssatz über zyklische Körper 207
§ 102. Von gewissen Primzahlen in der Diskriminante eines zyklischen Körpers vom Grade l^h 208
§ 103. Der zyklische Körper vom Grade u, dessen Diskriminante nur u enthält, und die zyklischen Körper vom Grade u^h und 2^h, in denen U_1 bzw. Π_1 als Unterkörper enthalten ist. 212
§ 104. Beweis des Fundamentalsatzes über Abelsche Körper 215
24. Die Wurzelzahlen des Kreiskörpers der l-ten Einheitswurzeln 216
§ 105. Die Definition und Existenz der Normalbasis 216
§ 106. Der Abelsche Körper vom Primzahlgrade l und von der Diskriminante p^{l-1}. Die Wurzelzahlen dieses Körpers 218
§ 107. Die charakteristischen Eigenschaften der Wurzelzahlen 218
§ 108. Die Zerlegung der l-ten Potenz einer Wurzelzahl im Körper der l-ten Einheitswurzeln 222
§ 109. Eine Äquivalenz für die Primideale ersten Grades des Körpers der l-ten Einheitswurzeln 223
§ 110. Die Konstruktion sämtlicher Normalbasen und Wurzelzahlen 224
§ 111. Die Lagrangesche Normalbasis und die Lagrangesche Wurzelzahl . . . 225
§ 112. Die charakteristischen Eigenschaften der Lagrangeschen Wurzelzahl . . 225
25. Das Reziprozitätsgesetz für l-te Potenzreste zwischen einer rationalen Zahl und einer Zahl des Körpers der l-ten Einheitswurzeln 228
§ 113. Der Potenzcharakter einer Zahl und das Symbol $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$ 228
§ 114. Ein Hilfssatz über den Potenzcharakter der l-ten Potenz der Lagrangeschen Wurzelzahl 229

Seite

§ 115. Beweis des Reziprozitätsgesetzes im Körper $k(\zeta)$ zwischen einer rationalen und einer beliebigen Zahl 230

26. Die Bestimmung der Anzahl der Idealklassen im Kreiskörper der m-ten Einheitswurzeln 234

§ 116. Das Symbol $\left[\frac{a}{L}\right]$ 234

§ 117. Die Ausdrücke für die Klassenanzahl im Kreiskörper der m-ten Einheitswurzeln 235

§ 118. Die Ableitung der aufgestellten Ausdrücke für die Klassenanzahl des Kreiskörpers $k\left(e^{\frac{2i\pi}{m}}\right)$ 238

§ 119. Das Vorhandensein von unendlich vielen rationalen Primzahlen, welche nach einer gegebenen Zahl einen vorgeschriebenen, zu ihr primen Rest lassen 240

§ 120. Die Darstellung sämtlicher Einheiten des Kreiskörpers durch die Kreiseinheiten 242

27. Anwendungen der Theorie des Kreiskörpers auf den quadratischen Körper . 243

§ 121. Die Erzeugung der Einheiten des reellen quadratischen Körpers aus Kreiseinheiten 243

§ 122. Das Reziprozitätsgesetz für quadratische Reste. 243

§ 123. Der imaginäre quadratische Körper mit einer Primzahldiskriminante . 245

§ 124. Die Bestimmung des Vorzeichens der Gaußschen Summe 246

Fünfter Teil. *Der Kummersche Zahlkörper.*

28. Die Zerlegung der Zahlen des Kreiskörpers im Kummerschen Körper . . . 249

§ 125. Die Definition des Kummerschen Körpers. 249

§ 126. Die Relativdiskriminante des Kummerschen Körpers 250

§ 127. Das Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ 253

§ 128. Die Primideale des Kummerschen Körpers. 254

29. Die Normenreste und Normennichtreste des Kummerschen Körpers 257

§ 129. Die Definition der Normenreste und Normennichtreste 257

§ 130. Der Satz von der Anzahl der Normenreste. Die Verzweigungsideale . 257

§ 131. Das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ 264

§ 132. Einige Hilfssätze über das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ und über Normenreste nach dem Primideal $\mathfrak{l}$ 267

§ 133. Das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ zur Unterscheidung zwischen Normenresten und Normennichtresten 272

30. Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Potenzcharakteren im Kummerschen Körper 275

§ 134. Der Grenzwert eines gewissen unendlichen Produktes 275

§ 135. Primideale des Kreiskörpers $k(\zeta)$ mit vorgeschriebenen Potenzcharakteren 276

31. Der reguläre Kreiskörper 278

§ 136. Die Definition des regulären Kreiskörpers, der regulären Primzahl und des regulären Kummerschen Körpers 278

Seite

§ 137. Ein Hilfssatz über die Teilbarkeit des ersten Faktors der Klassenanzahl von $k\left(e^{\frac{2i\pi}{l}}\right)$ durch l 279

§ 138. Ein Hilfssatz über die Einheiten des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$ für den Fall, daß l in den Zählern der ersten $\frac{l-3}{2}$ Bernoullischen Zahlen nicht aufgeht 281

§ 139. Ein Kriterium für die regulären Primzahlen 283

§ 140. Ein besonderes System von unabhängigen Einheiten im regulären Kreiskörper 286

§ 141. Eine charakteristische Eigenschaft für die Einheiten eines regulären Kreiskörpers 287

§ 142. Der Begriff der primären Zahl im regulären Kreiskörper 288

32. Die ambigen Idealklassen und die Geschlechter im regulären Kummerschen Körper 289

§ 143. Der Begriff der Einheitenschar im regulären Kreiskörper 289

§ 144. Die ambigen Ideale und die ambigen Idealklassen eines regulären Kummerschen Körpers 291

§ 145. Der Begriff der Klassenschar im regulären Kummerschen Körper . . . 292

§ 146. Zwei allgemeine Hilfssätze über die relativen Grundeinheiten eines relativzyklischen Körpers von ungeradem Primzahlgrade 292

§ 147. Die durch ambige Ideale bestimmten Idealklassen 294

§ 148. Die sämtlichen ambigen Idealklassen 302

§ 149. Das Charakterensystem einer Zahl und eines Ideals im regulären Kummerschen Körper 305

§ 150. Das Charakterensystem einer Idealklasse und der Begriff des Geschlechtes 307

§ 151. Obere Grenze für den Grad der aus sämtlichen ambigen Klassen bestehenden Klassenschar 308

§ 152. Die Komplexe des regulären Kummerschen Körpers 309

§ 153. Obere Grenze für die Anzahl der Geschlechter in einem regulären Kummerschen Körper 310

33. Das Reziprozitätsgesetz für l-te Potenzreste im regulären Kreiskörper 312

§ 154. Das Reziprozitätsgesetz für l-te Potenzreste und die Ergänzungssätze . 312

§ 155. Die Primideale erster und zweiter Art im regulären Kreiskörper . . . 313

§ 156. Hilfssätze über Primideale erster Art im regulären Kreiskörper 316

§ 157. Ein besonderer Fall des Reziprozitätsgesetzes für zwei Primideale . . 319

§ 158. Das Vorhandensein gewisser Hilfsprimideale, für welche das Reziprozitätsgesetz gilt 321

§ 159. Beweis des ersten Ergänzungssatzes zum Reziprozitätsgesetz 323

§ 160. Beweis des Reziprozitätsgesetzes zwischen zwei beliebigen Primidealen 324

§ 161. Beweis des zweiten Ergänzungssatzes zum Reziprozitätsgesetz 326

34. Die Anzahl der vorhandenen Geschlechter im regulären Kummerschen Körper 328

§ 162. Ein Satz über das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ 328

§ 163. Der Fundamentalsatz über die Geschlechter eines regulären Kummerschen Körpers 329

§ 164. Die Klassen des Hauptgeschlechtes in einem regulären Kummerschen Körper. 331

§ 165. Der Satz von den Relativnormen der Zahlen eines regulären Kummerschen Körpers 332

Seite

35. Neue Begründung der Theorie des regulären Kummerschen Körpers 335
§ 166. Die wesentlichen Eigenschaften der Einheiten des regulären Kreiskörpers 335
§ 167. Beweis einer Eigenschaft für die Primärzahlen von Primidealen der zweiten Art 337
§ 168. Beweis des Reziprozitätsgesetzes für die Fälle, daß eines der beiden Primideale von der zweiten Art ist 340
§ 169. Ein Hilfssatz über das Produkt $\prod'\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$, worin $\mathfrak{w}$ alle von $\mathfrak{l}$ verschiedenen Primideale durchläuft 343
§ 170. Das Symbol $\{\nu,\mu\}$ und das Reziprozitätsgesetz zwischen zwei beliebigen Primidealen 346
§ 171. Übereinstimmung des Symbols $\{\nu,\mu\}$ mit dem Symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ 347
36. Die Diophantische Gleichung $\alpha^m+\beta^m+\gamma^m=0$ 349
§ 172. Die Unmöglichkeit der Diophantischen Gleichung $\alpha^l+\beta^l+\gamma^l=0$ für reguläre Primzahlexponenten l 349
§ 173. Weitere Untersuchungen über die Unmöglichkeit der Diophantischen Gleichung $\alpha^m+\beta^m+\gamma^m=0$ 354
Literaturverzeichnis 356
Verzeichnis der Sätze und Hilfssätze 362

8. Über die Theorie der relativquadratischen Zahlkörper 364
[Jahresbericht der Deutschen Mathematikervereinigung Bd. 6, S. 88—94 (1899).]

9. Über die Theorie des relativquadratischen Zahlkörpers 370
[Mathem. Annalen Bd. 51, S. 1—127 (1899).]
Einleitung 370
I. *Allgemeine Definitionen und vorbereitende Sätze* 371
§ 1. Quadratische Reste und Nichtreste im Grundkörper k und das Symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$ 371
§ 2. Die Begriffe Relativnorm, Relativdifferente und Relativdiskriminante . 372
§ 3. Das ambige Ideal 374
§ 4. Die Primfaktoren der Relativdiskriminante 374
§ 5. Die Zerlegung der Primideale des Grundkörpers k im relativquadratischen Körper K 376
§ 6. Das Symbol $\left(\frac{\mu}{\mathfrak{a}}\right)$ 379
§ 7. Normenreste und Normennichtreste des Körpers K und das Symbol $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ 380
§ 8. Eigenschaften des Symbols $\left(\frac{\nu,\mu}{\mathfrak{p}}\right)$ 380
§ 9. Die allgemeinen Grundformeln für das Symbol $\left(\frac{\nu,\mu}{\mathfrak{p}}\right)$ 385
§ 10. Die Anzahl der Normenreste nach einem nicht in 2 aufgehenden Primideal 388
§ 11. Die Einheitenverbände des Körpers k 388
§ 12. Die Komplexe des relativquadratischen Körpers K 389
§ 13. Primideale des Körpers k mit vorgeschriebenen quadratischen Charakteren 390
II. *Die Theorie der relativquadratischen Körper für einen Grundkörper mit lauter imaginären Konjugierten und von ungerader Klassenanzahl* 393
§ 14. Die relativen Grundeinheiten des Körpers K 393
§ 15. Die Anzahl der aus ambigen Idealen entspringenden ambigen Komplexe in K 397

Seite

§ 16. Die Anzahl aller ambigen Komplexe in K 403
§ 17. Das Charakterensystem einer Zahl und eines Ideals im Körper K . . 406
§ 18. Der Begriff des Geschlechtes 408
§ 19. Obere Grenze für die Anzahl der Geschlechter in K 409
§ 20. Das primäre Primideal $\mathfrak{p}$ und das Symbol $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$ 412
§ 21. Ein System von $\frac{m}{2}$ nichtprimären Primidealen des Körpers k 412
§ 22. Die unendliche Reihe $\sum_{(\mathfrak{w})}'\left(\frac{\mathfrak{w}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{w})^s}$ 416
§ 23. Eine Eigenschaft primärer Primideale 423
§ 24. Zwei besondere Fälle des Reziprozitätsgesetzes für quadratische Reste im Körper k 427
§ 25. Das Produkt $\prod_{(\mathfrak{w})}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ für ein zu 2 primes ν und bei gewissen Annahmen über μ 428
§ 26. Das primäre Ideal und seine Eigenschaften 434
§ 27. Beispiele für die Sätze 32, 33, 38, 39 436
§ 28. Das Produkt $\prod_{(\mathfrak{w})}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ für ein beliebiges ν und bei gewissen Annahmen über μ 445
§ 29. Der Fundamentalsatz über die Anzahl der Geschlechter in einem relativquadratischen Körper 446
§ 30. Ein gewisses System von $\frac{m}{2}+z$ zu 2 primen Primidealen des Körpers k 447
§ 31. Eine Eigenschaft gewisser besonderer Ideale des Körpers k 451
§ 32. Das Symbol $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ für irgendwelche zu 2 primen Zahlen ν,μ 453
§ 33. Die Übereinstimmung der beiden Symbole $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ und $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ für irgendwelche zu 2 prime Zahlen ν,μ 454
§ 34. Die Eigenschaften des Symbols $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ für irgendwelche zu 2 prime ganze Zahlen ν,μ 464
§ 35. Das Produkt $\prod_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ für irgendwelche zu 2 prime Zahlen ν,μ 465
§ 36. Der erste Ergänzungssatz und das allgemeine Reziprozitätsgesetz für quadratische Reste 466
§ 37. Das Symbol $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ für beliebige ganze Zahlen ν,μ 467
§ 38. Die Übereinstimmung der beiden Symbole $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ und $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ für beliebige ganze Zahlen ν,μ 467
§ 39. Das Produkt $\prod_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ für beliebige ganze Zahlen ν,μ 473
§ 40. Die Anzahl der Normenreste nach einem in 2 aufgehenden Primideal . . 474
§ 41. Beweis des Fundamentalsatzes über die Geschlechter in einem beliebigen relativquadratischen Körper 476
§ 42. Die Klassen des Hauptgeschlechtes 478

Seite

§ 43. Der Satz von den Relativnormen eines relativquadratischen Körpers. . 479
§ 44. Die ternäre quadratische Diophantische Gleichung im Körper k . . . 481
Verzeichnis der Sätze und Definitionen 482

10. Über die Theorie der relativ-Abelschen Zahlkörper 483
[Acta Mathematica Bd. 26, S. 99—132 (1902) und Nachrichten der Gesellschaft der Wissenschaften zu Göttingen S. 370—399 (1898).]

11. Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem) 510
Dem Andenken an HERMANN MINKOWSKI gewidmet
[Nachrichten der Gesellschaft der Wissenschaften zu Göttingen S. 17—36 (1909) und Mathem. Annalen Bd. 67, S. 281—300 (1909).]

Zu Hilberts algebraisch-zahlentheoretischen Arbeiten. Von HELMUT HASSE 528

Verzeichnis der Begriffsnamen 536

1. Über die Transzendenz der Zahlen e und π.

[Nachrichten der Gesellschaft der Wissenschaften zu Göttingen S. 113—116 (1893). Mathem. Annalen Bd. 43, S. 216—219 (1893).]

Man nehme an, die Zahl e genüge der Gleichung n-ten Grades

$$a + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0\,,$$

deren Koeffizienten a, $a_1, \ldots, a_n$ ganze rationale Zahlen sind.

Wird die linke Seite dieser Gleichung mit dem Integral

$$\int_0^\infty = \int_0^\infty z^\varrho [(z-1)(z-2)\cdots(z-n)]^{\varrho+1} e^{-z}\, dz$$

multipliziert, wo ϱ eine ganze positive Zahl bedeutet, so entsteht der Ausdruck

$$a\int_0^\infty + a_1 e\int_0^\infty + a_2 e^2\int_0^\infty + \cdots + a_n e^n \int_0^\infty$$

und dieser Ausdruck zerlegt sich in die Summe der beiden folgenden Ausdrücke:

$$P_1 = a\int_0^\infty + a_1 e\int_1^\infty + a_2 e^2\int_2^\infty + \cdots + a_n e^n \int_n^\infty,$$

$$P_2 = \qquad a_1 e\int_0^1 + a_2 e^2\int_0^2 + \cdots + a_n e^n \int_0^n.$$

Die Formel

$$\int_0^\infty z^\varrho e^{-z}\, dz = \varrho!$$

zeigt, daß das Integral $\int_0^\infty$ eine ganze rationale durch $\varrho!$ teilbare Zahl ist und ebenso leicht folgt, wenn man bezüglich die Substitutionen $z = z' + 1$, $z = z' + 2, \ldots, z = z' + n$ anwendet, daß $e\int_1^\infty$, $e^2\int_2^\infty, \ldots, e^n\int_n^\infty$ ganze rationale durch $(\varrho+1)!$ teilbare Zahlen sind. Daher ist auch P_1 eine durch $\varrho!$ teilbare ganze Zahl, und zwar gilt, wie man sieht, nach dem Modul $\varrho+1$ die Kongruenz

$$\frac{P_1}{\varrho!} \equiv \pm a\,(n!)^{\varrho+1}, \qquad (\varrho+1). \tag{1}$$

Andrerseits ist, wenn mit K bezüglich k die absolut größten Werte bezeichnet werden, welche die Funktionen

$$z(z-1)(z-2)\cdots(z-n)$$

bezüglich

$$(z-1)(z-2)\cdots(z-n)e^{-z}$$

in dem Intervalle $z=0$ bis $z=n$ annehmen:

$$\left|\int_0^1\right| < kK^e, \quad \left|\int_0^2\right| < 2kK^e, \ldots, \quad \left|\int_0^n\right| < nkK^e$$

und hieraus folgt, wenn zur Abkürzung

$$\varkappa = \{|a_1 e| + 2|a_2 e^2| + \cdots + n|a_n e^n|\}k$$

gesetzt wird, die Ungleichung

$$|P_2| < \varkappa K^e. \tag{2}$$

Nun bestimme man eine ganze positive Zahl ϱ, welche erstens durch die ganze Zahl $a\cdot n!$ teilbar ist und für welche zweitens $\varkappa\frac{K^e}{\varrho!}<1$ wird. Es ist dann $\frac{P_1}{\varrho!}$ infolge der Kongruenz (1) eine nicht durch $\varrho+1$ teilbare und daher notwendig von 0 verschiedene ganze Zahl, und da überdies $\frac{P_2}{\varrho!}$ infolge der Ungleichung (2) absolut genommen kleiner als 1 wird, so ist die Gleichung

$$\frac{P_1}{\varrho!}+\frac{P_2}{\varrho!}=0$$

unmöglich.

Man nehme an, es sei π eine algebraische Zahl und es genüge die Zahl $\alpha_1=i\pi$ einer Gleichung n-ten Grades mit ganzzahligen Koeffizienten. Bezeichnen wir dann mit $\alpha_2,\ldots,\alpha_n$ die übrigen Wurzeln dieser Gleichung, so muß, da $1+e^{i\pi}$ den Wert 0 hat, auch der Ausdruck

$$(1+e^{\alpha_1})(1+e^{\alpha_2})\cdots(1+e^{\alpha_n}) = 1+e^{\beta_1}+e^{\beta_2}+\cdots+e^{\beta_N}$$

den Wert 0 haben und hierin sind, wie man leicht sieht, die N Exponenten $\beta_1,\ldots,\beta_N$ die Wurzeln einer Gleichung N-ten Grades mit ganzzahligen Koeffizienten. Sind überdies etwa die M Exponenten $\beta_1,\ldots,\beta_M$ von 0 verschieden, während die übrigen verschwinden, so sind diese M Exponenten $\beta_1,\ldots,\beta_M$ die Wurzeln einer Gleichung M-ten Grades von der Gestalt

$$f(z) = bz^M + b_1 z^{M-1} + \cdots + b_M = 0,$$

deren Koeffizienten ebenfalls ganze rationale Zahlen sind und in welcher insbesondere der letzte Koeffizient b_M von 0 verschieden ist. Der obige Ausdruck erhält dann die Gestalt

$$a + e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_M},$$

wo a eine ganze positive Zahl ist.

Man multipliziere diesen Ausdruck mit dem Integral

$$\int_0^\infty = \int_0^\infty z^\varrho [g(z)]^{\varrho+1} e^{-z}\,dz,$$

wo ϱ wiederum eine ganze positive Zahl bedeutet und wo zur Abkürzung $g(z)=b^M f(z)$ gesetzt ist; dann ergibt sich

$$a\int_0^\infty + e^{\beta_1}\int_0^\infty + e^{\beta_2}\int_0^\infty + \cdots + e^{\beta_M}\int_0^\infty$$

und dieser Ausdruck zerlegt sich in die Summe der beiden folgenden Ausdrücke:

$$P_1 = a\int_0^\infty + e^{\beta_1}\int_{\beta_1}^\infty + e^{\beta_2}\int_{\beta_2}^\infty + \cdots + e^{\beta_M}\int_{\beta_M}^\infty,$$

$$P_2 = \qquad e^{\beta_1}\int_0^{\beta_1} + e^{\beta_2}\int_0^{\beta_2} + \cdots + e^{\beta_M}\int_0^{\beta_M},$$

wo allgemein das Integral $\int_{\beta_i}^\infty$ in der komplexen z-Ebene vom Punkte $z=\beta_i$ längs einer zur Achse der reellen Zahlen parallelen Geraden bis zu $z=+\infty$ hin und das $\int_0^{\beta_i}$ vom Punkte $z=0$ längs der geraden Verbindungslinie bis zum Punkte $z=\beta_i$ hin zu erstrecken ist.

Das Integral $\int_0^\infty$ ist wieder gleich einer ganzen rationalen durch $\varrho!$ teilbaren Zahl, und zwar gilt, wie man sieht, nach dem Modul $\varrho+1$ die Kongruenz

$$\frac{1}{\varrho!}\int_0^\infty \equiv b^{\varrho M+M} b_M^{\varrho+1}, \qquad (\varrho+1).$$

Mittels der Substitution $z=z'+\beta_i$ und wegen $g(\beta_i)=0$ ergibt sich ferner

$$e^{\beta_i}\int_{\beta_i}^\infty = \int_0^\infty (z'+\beta_i)^\varrho [g(z'+\beta_i)]^{\varrho+1} e^{-z'}\,dz' = (\varrho+1)!\;\; G(\beta_i),$$

wo $G(\beta_i)$ eine ganze ganzzahlige Funktion von β_i bedeutet, deren Grad in β_i unterhalb der Zahl $\varrho M+M$ bleibt und deren Koeffizienten sämtlich durch $b^{\varrho M+M}$ teilbar sind. Da $\beta_1,\ldots,\beta_M$ die Wurzeln der ganzzahligen Gleichung $f(z)=0$ sind und mithin durch Multiplikation mit dem ersten Koeffizienten b zu *ganzen* algebraischen Zahlen werden, so ist

$$G(\beta_1)+G(\beta_2)+\cdots+G(\beta_M)$$

notwendig eine *ganze rationale* Zahl. Hieraus folgt, daß der Ausdruck P_1 gleich einer ganzen rationalen durch $\varrho!$ teilbaren Zahl wird, und zwar gilt

nach dem Modul $\varrho+1$ die Kongruenz

$$\frac{P_1}{\varrho!} = a b^{\varrho M+M} b_M^{\varrho+1}, \qquad (\varrho+1). \tag{3}$$

Andrerseits ist, wenn mit K bezüglich k die größten absoluten Beträge bezeichnet werden, welche die Funktionen $zg(z)$ bezüglich $g(z)e^{-z}$ auf den geradlinigen Integrationsstrecken zwischen $z=0$ bis $z=\beta_i$ annehmen:

$$\left|\int_0^{\beta_i}\right| < |\beta_i|\, k\, K^\varrho \qquad (i=1,2,\ldots,M)$$

und hieraus folgt, wenn zur Abkürzung

$$\varkappa = \{|\beta_1 e^{\beta_1}| + |\beta_2 e^{\beta_2}| + \cdots + |\beta_M e^{\beta_M}|\}\, k$$

gesetzt wird, die Ungleichung

$$|P_2| < \varkappa K^\varrho. \tag{4}$$

Nun bestimme man eine ganze positive Zahl ϱ, welche erstens durch abb_M teilbar ist und für welche zweitens $\frac{\varkappa K^\varrho}{\varrho!} < 1$ wird. Es ist dann $\frac{P_1}{\varrho!}$ infolge der Kongruenz (3) eine nicht durch $\varrho+1$ teilbare und daher notwendig von 0 verschiedene ganze Zahl, und da überdies $\frac{P_2}{\varrho!}$ infolge der Ungleichung (4), absolut genommen, kleiner als 1 wird, so ist die Gleichung

$$\frac{P_1}{\varrho!} + \frac{P_2}{\varrho!} = 0$$

unmöglich.

Es ist leicht zu erkennen, wie auf dem eingeschlagenen Wege ebenso einfach auch der allgemeinste Lindemannsche Satz über die Exponentialfunktion sich beweisen läßt.

Königsberg i. Pr., den 5. Januar 1893.

2. Zwei neue Beweise für die Zerlegbarkeit der Zahlen eines Körpers in Primideale.

[Jahresbericht der Deutschen Mathematikervereinigung Bd. 3, S. 59 (1894).]

Die Grundlage für die Theorie der algebraischen Zahlen bildet der von Dedekind und Kronecker zuerst allgemein ausgesprochene und bewiesene Satz, daß jedes Ideal eines Zahlkörpers auf eine und nur auf eine Weise in Primideale zerlegt werden kann. Der Kroneckersche Beweis bedient sich der Methode der unbestimmten Koeffizienten und ferner des Prinzips, den Satz zunächst für einen Galoisschen Körper zu entwickeln, während der Dedekindsche Beweis diese beiden Hilfsmittel nicht verwendet. Durch eine Abänderung in der Reihenfolge der Schlüsse läßt sich der Kroneckersche Beweis so führen, daß das letztgenannte Prinzip dabei vermieden wird und mithin der so entstehende Beweis lediglich mit dem Hilfsmittel der unbestimmten Koeffizienten auskommt. Der Vortragende legt einen zweiten neuen Beweis des Satzes dar, welcher im Gegensatz zu dem eben charakterisierten Beweis wesentlich das Prinzip der Zugrundelegung eines Galoisschen Körpers benutzt und welcher aus mannigfachen, vornehmlich bei der Weiterentwicklung der Theorie der Körper hervortretenden Gründen den Vorzug vor den früheren Beweisen zu verdienen scheint.

3. Über die Zerlegung der Ideale eines Zahlkörpers in Primideale.

[Mathem. Annalen Bd. 44, S. 1—8 (1894).]

Die Grundlage für die Theorie der algebraischen Zahlen bildet der Satz, daß jedes Ideal eines Zahlkörpers auf eine und nur auf eine Weise in Primideale zerlegt werden kann. Dieser Satz ist zuerst von R. DEDEKIND[1] allgemein ausgesprochen und bewiesen worden. Einen zweiten, wesentlich hiervon verschiedenen Beweis gab L. KRONECKER[2]. Die vorliegende Abhandlung enthält einen neuen Beweis[3] dieses Satzes.

Es sei ein beliebiger Zahlkörper vom n-ten Grade vorgelegt; dann stelle ich folgende Definitionen auf:

Ein unendliches System von ganzen algebraischen Zahlen $\alpha_1, \alpha_2, \ldots$ des Körpers, welches die Eigenschaft besitzt, daß eine jede lineare Kombination $\varkappa_1\alpha_1 + \varkappa_2\alpha_2 + \ldots$ derselben wiederum dem Systeme angehört, heißt ein *Ideal* $\mathfrak{j}$ des Körpers; dabei bedeuten $\varkappa_1, \varkappa_2, \ldots$ *beliebige* ganze algebraische Zahlen des Körpers. Sind $\alpha_1, \ldots, \alpha_m$ solche m Zahlen des Ideals $\mathfrak{j}$, durch deren lineare Kombination unter Benutzung ganzer algebraischer Koeffizienten alle Zahlen des Ideals erhalten werden können, so setze ich kurz

$$\mathfrak{j} = (\alpha_1, \ldots, \alpha_m).$$

Wie leicht gezeigt werden kann, gibt es im Ideal $\mathfrak{j}$ stets n Zahlen $\alpha_1^0, \ldots, \alpha_n^0$ von der Art, daß eine jede Zahl des Ideals gleich einer linearen Kombination derselben von der Gestalt $k_1\alpha_1^0 + \cdots + k_n\alpha_n^0$ ist, wo $k_1, \ldots, k_n$ ganze *rationale* Zahlen sind. Die Zahlen $\alpha_1^0, \ldots, \alpha_n^0$ heißen eine *Basis* des Ideals $\mathfrak{j}$.

Ein Ideal, welches alle und nur die Zahlen von der Gestalt $\varkappa\eta$ enthält, wo $\varkappa$ jede beliebige ganze Zahl des Körpers darstellt, heißt ein *Hauptideal* und wird mit (η) oder auch kurz mit η bezeichnet.

Eine jede Zahl α des Ideals $\mathfrak{j} = (\alpha_1, \ldots, \alpha_m)$ heißt *kongruent* 0 nach dem Ideal $\mathfrak{j}$ oder in Zeichen:

$$\alpha \equiv 0, \quad (\mathfrak{j}).$$

[1] Vorlesungen über Zahlentheorie von DIRICHLET. Supplement XI.

[2] Grundzüge einer arithmetischen Theorie der algebraischen Größen. Journ. für Math., Bd. 92 (1882).

[3] Den Gedankengang dieses Beweises habe ich in der Versammlung der deutschen Mathematiker-Vereinigung München 1893 vorgetragen. (Siehe dieser Bd., Abhandlung 2.)

Wenn alle Zahlen eines Ideals $\mathfrak{k}$ kongruent 0 nach $\mathfrak{j}$ sind, so heißt das Ideal $\mathfrak{k}$ *kongruent* 0 nach $\mathfrak{j}$ oder in Zeichen

$$\mathfrak{k} \equiv 0, \quad (\mathfrak{j}).$$

Offenbar ist jedes Ideal $\mathfrak{j}$ kongruent 0 nach dem Ideal 1 und nach dem Ideal $\mathfrak{j}$ selbst.

Ein von 1 verschiedenes Ideal $\mathfrak{p}$, welches nach keinem anderen Ideal außer nach 1 und nach sich selbst $\equiv 0$ ist, heißt *Primideal*.

Wenn man jede Zahl eines Ideals $\mathfrak{j} = (\alpha_1, \ldots, \alpha_m)$ mit jeder Zahl eines zweiten Ideals $\mathfrak{k} = (\beta_1, \ldots, \beta_l)$ multipliziert und die so erhaltenen Zahlen linear mittels beliebiger ganzer algebraischer Koeffizienten kombiniert, so wird das so entstehende neue Ideal das *Produkt* jener beiden Ideale genannt, d. h. in Zeichen

$$\mathfrak{j}\mathfrak{k} = (\alpha_1\beta_1, \ldots, \alpha_m\beta_1, \ldots, \alpha_1\beta_l, \ldots, \alpha_m\beta_l).$$

Ein Ideal $\mathfrak{r}$ heißt durch das Ideal $\mathfrak{j}$ *teilbar*, wenn ein Ideal $\mathfrak{k}$ existiert, derart, daß $\mathfrak{r} = \mathfrak{j}\mathfrak{k}$ ist. Ist $\mathfrak{r}$ durch $\mathfrak{j}$ teilbar, so ist $\mathfrak{r} \equiv 0$ nach dem Ideal $\mathfrak{j}$.

1. Ein Ideal $\mathfrak{j}$ kann nur nach einer *endlichen* Anzahl von Idealen $\equiv 0$ sein.

Zum Beweise bilde man die Norm a einer beliebigen Zahl α des Ideals $\mathfrak{j}$; ist dann etwa $\mathfrak{k}$ ein Ideal, nach welchem $\mathfrak{j} \equiv 0$ ist, so muß offenbar auch $a \equiv 0$ nach $\mathfrak{k}$ sein. Die n Basiszahlen von $\mathfrak{k}$ seien von der Gestalt

$$\begin{aligned} &k_{11}\omega_1 + k_{12}\omega_2 + \cdots + k_{1n}\omega_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &k_{n1}\omega_1 + k_{n2}\omega_2 + \cdots + k_{nn}\omega_n, \end{aligned}$$

wo $\omega_1, \ldots, \omega_n$ eine Basis der ganzen Zahlen des Körpers und wo $k_{11}, k_{12}, \ldots, k_{nn}$ ganze rationale Zahlen sind. Bedeuten $k'_{11}, k'_{12}, \ldots, k'_{nn}$ bezüglich die kleinsten positiven Reste der Zahlen $k_{11}, k_{12}, \ldots, k_{nn}$ nach dem Modul a, so wird

$$\begin{aligned} \mathfrak{k} &= (k_{11}\omega_1 + \cdots + k_{1n}\omega_n, \ldots, k_{n1}\omega_1 + \cdots + k_{nn}\omega_n) \\ &= (k'_{11}\omega_1 + \cdots + k'_{1n}\omega_n, \ldots, k'_{n1}\omega_1 + \cdots + k'_{nn}\omega_n, a), \end{aligned}$$

und diese Darstellung des Ideals $\mathfrak{k}$ läßt unmittelbar die Richtigkeit der Behauptung erkennen.

2. Ein jedes von 1 verschiedene Ideal $\mathfrak{j}$ ist $\equiv 0$ nach mindestens einem Primideal $\mathfrak{p}$.

Denn falls $\mathfrak{j}$ nicht schon selbst ein Primideal ist, so gibt es ein von $\mathfrak{j}$ und von 1 verschiedenes Ideal $\mathfrak{j}_1$, nach welchem $\mathfrak{j} \equiv 0$ ist. Es sei ferner $\mathfrak{j}_2$ ein von 1 und von $\mathfrak{j}_1$ verschiedenes Ideal, nach welchem $\mathfrak{j}_1 \equiv 0$ ist; $\mathfrak{j}_3$ ein von $\mathfrak{j}_2$ und 1 verschiedenes Ideal, nach welchem $\mathfrak{j}_2 \equiv 0$ ist usw. In der Reihe $\mathfrak{j}, \mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \ldots$ ist jedes Ideal $\equiv 0$ nach allen folgenden Idealen. Überdies sind sämtliche Ideale dieser Reihe untereinander verschieden. Denn die Annahme $\mathfrak{j}_r = \mathfrak{j}_s$, $r > s$ hätte $\mathfrak{j}_r \equiv 0$ nach $\mathfrak{j}_s$ und mithin auch nach $\mathfrak{j}_{r-1}$ zur Folge; da jedoch auch $\mathfrak{j}_{r-1} \equiv 0$ nach $\mathfrak{j}_r$ ist, so wäre notwendig $\mathfrak{j}_{r-1} = \mathfrak{j}_r$ und dieser Umstand wider-

spricht der Voraussetzung. Nach Satz 1 bricht die Reihe dieser Ideale $\mathfrak{j}, \mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \ldots$ ab. Das letzte Ideal ist ein Primideal.

Der eben bewiesene Satz kann auch wie folgt ausgesprochen werden. Wenn ein Ideal nach keinem Primideal $\equiv 0$ ist, so ist es das Ideal 1.

3. Wenn das Produkt $\mathfrak{j}\mathfrak{k}$ zweier Ideale $\mathfrak{j}$ und $\mathfrak{k}$ $\equiv 0$ ist nach einem Primideal $\mathfrak{p}$, so ist entweder $\mathfrak{j} \equiv 0$ oder $\mathfrak{k} \equiv 0$ nach dem Primideal $\mathfrak{p}$.

Ist etwa $\mathfrak{j}$ nicht $\equiv 0$ nach $\mathfrak{p}$, so bestimme man eine Zahl α des Ideals $\mathfrak{j}$, welche nicht $\equiv 0$ nach $\mathfrak{p}$ ist. Ferner bilde man aus $\mathfrak{p} = (\pi_1, \ldots, \pi_r)$ durch Hinzufügung der Zahl α das Ideal $(\pi_1, \ldots, \pi_r, \alpha)$. Dieses Ideal ist offenbar weder nach $\mathfrak{p}$ noch nach irgendeinem anderen Primideal $\equiv 0$ und folglich nach Satz 2 gleich dem Ideal 1, d. h.

$$1 = \varkappa\alpha + \varkappa_1\pi_1 + \cdots + \varkappa_r\pi_r,$$

wo $\varkappa, \varkappa_1, \ldots, \varkappa_r$ geeignet gewählte ganze algebraische Zahlen des Körpers sind. Die erhaltene Gleichung lautet als Kongruenz geschrieben: $1 \equiv \varkappa\alpha$ nach dem Primideal $\mathfrak{p}$. Bezeichnet nun β irgendeine Zahl des Ideals $\mathfrak{k}$, so ist nach Voraussetzung $\alpha\beta \equiv 0$ nach $\mathfrak{p}$. Und hieraus folgt nach Multiplikation mit $\varkappa$ die Kongruenz $\beta \equiv 0$ nach dem Primideal $\mathfrak{p}$.

4. Wenn ein Ideal $\mathfrak{j} \equiv 0$ nach einem Hauptideal (η) ist, so ist $\mathfrak{j}$ durch (η) teilbar. Aus $\eta\mathfrak{j} = \eta\mathfrak{k}$ folgt notwendig $\mathfrak{j} = \mathfrak{k}$.

In der Tat, da alle Zahlen des Ideals $\mathfrak{j} = (\alpha_1, \ldots, \alpha_m)$ durch die Zahl η teilbar sind, so kann man $\alpha_1 = \eta\beta_1, \ldots, \alpha_m = \eta\beta_m$ setzen und hat dann $\mathfrak{j} = (\eta)(\beta_1, \ldots, \beta_m)$. Ist ferner $\eta\mathfrak{j} \equiv 0$ nach $\eta\mathfrak{k}$, so folgt nach Division durch die Zahl η, daß $\mathfrak{j} \equiv 0$ nach $\mathfrak{k}$ ist. Da wegen $\eta\mathfrak{k} \equiv 0$ nach $\eta\mathfrak{j}$ in gleicher Weise auch $\mathfrak{k} \equiv 0$ nach $\mathfrak{j}$ ist, so folgt notwendig $\mathfrak{j} = \mathfrak{k}$.

5. In einem jeden Primideal $\mathfrak{p}$ gibt es stets eine rationale Primzahl p von der Art, daß eine jede andere ganze rationale Zahl des Ideals $\mathfrak{p}$ diese Primzahl p als Faktor enthält.

Zum Beweise nehme man die Norm a einer Zahl von $\mathfrak{p}$ und zerlege a in seine rationalen Primfaktoren. Faßt man diese als Hauptideale auf, so ist nach Satz 3 einer derselben etwa $p \equiv 0$ nach dem Primideal $\mathfrak{p}$. Gäbe es nun in $\mathfrak{p}$ noch eine ganze rationale Zahl b, welche nicht durch p teilbar wäre, so bestimme man zwei ganze rationale Zahlen r und s derart, daß $1 = rp + sb$ ist; hieraus würde $1 \equiv 0$ nach $\mathfrak{p}$ folgen, was nicht möglich ist.

Nunmehr nehmen wir zunächst an, daß der vorgelegte Zahlkörper ein Galoisscher[1] Körper sei; dann wird aus jedem Ideal des Körpers jedenfalls wieder ein Ideal des nämlichen Körpers entstehen, wenn wir in jenem Ideal

[1] Auch KRONECKER beweist den Satz von der Zerlegung in Primideale zuerst für einen Galoisschen Körper; doch ist es bemerkenswert, daß für die Kroneckersche Schlußweise dieser Gedanke keineswegs wesentlich ist. Vielmehr läßt sich das Kroneckersche Beweisverfahren durch eine geringfügige Abänderung in der Reihenfolge der Schlüsse unmittelbar auf beliebige Körper anwenden. Der so abgeänderte Kroneckersche Beweis kommt somit lediglich mit dem Hilfsmittel der unbestimmten Koeffizienten aus.

statt einer jeden Zahl eine konjugierte Zahl einsetzen. Sind insbesondere alle aus einem vorgelegten Ideal $\mathfrak{a}$ auf diese Weise entstehenden $n-1$ konjugierten Ideale mit dem vorgelegten Ideal $\mathfrak{a}$ identisch, so nenne ich das Ideal $\mathfrak{a}$ ein *ambiges* Ideal. Dieser Begriff des ambigen Ideals ist ein wesentliches Hilfsmittel meines Beweises. Von einem ambigen Ideal gilt der Satz:

I. *Wenn ein ambiges Ideal* $\mathfrak{a} \equiv 0$ *nach einem Primideal* $\mathfrak{p}$ *ist, so sind alle Zahlen von* $\mathfrak{a}$ *durch* $p^{\frac{1}{n}}$ *teilbar, wo* p *die zu* $\mathfrak{p}$ *gehörige Primzahl bedeutet.*

In der Tat, wenn α eine Zahl des Ideals $\mathfrak{a}$ ist, so gehören auch die zu α konjugierten Zahlen dem Ideal $\mathfrak{a}$ an; dieselben sind folglich sämtlich $\equiv 0$ nach dem Primideal $\mathfrak{p}$. Nun sei

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$$

die Gleichung n-ten Grades mit ganzen rationalen Koeffizienten $a_1, a_2, \ldots, a_n$, welcher die Zahl α genügt. Diese Koeffizienten sind als homogene Funktionen der Wurzeln der Gleichung ebenfalls $\equiv 0$ nach dem Primideal $\mathfrak{p}$ und mithin nach Satz 5 durch p teilbar. Die Zahl $\beta = \frac{\alpha}{p^{\frac{1}{n}}}$ genügt der Gleichung

$$\beta^n + \frac{a_1}{p}p^{\frac{n-1}{n}}\beta^{n-1} + \frac{a_2}{p}p^{\frac{n-2}{n}}\beta^{n-2} + \cdots + \frac{a_n}{p} = 0$$

und da die Koeffizienten dieser Gleichung sämtlich ganze algebraische Zahlen sind, so ist auch β eine ganze algebraische Zahl.

Ferner läßt sich für ein ambiges Ideal leicht die Richtigkeit des folgenden Satzes erkennen:

II. *Wenn ein ambiges Ideal* $\mathfrak{a} \equiv 0$ *nach einem Primideal* $\mathfrak{p}$ *ist, so gibt es immer eine rationale Zahl* r *von der Art, daß die Zahlen des Ideals* $\mathfrak{a}$ *durch* p^r, *aber nicht sämtlich durch eine höhere ganze oder gebrochene Potenz von* p *teilbar sind.*

Zum Beweise wähle man eine beliebige Zahl α des Ideals $\mathfrak{a}$; dieselbe genüge der Gleichung n-ten Grades

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0,$$

wo allgemein a_i eine ganze rationale Zahl bedeutet, welche durch die ganze Potenz p^{g_i}, aber durch keine höhere Potenz von p teilbar ist. Die kleinste der Zahlen $\frac{g_1}{1}, \frac{g_2}{2}, \ldots, \frac{g_n}{n}$ werde r_α genannt. In allen anderen Zahlen $\alpha', \alpha'', \ldots$ des Ideals $\mathfrak{a}$ denke man sich in gleicher Weise die zugehörigen rationalen Zahlen $r_{\alpha'}, r_{\alpha''}, \ldots$ bestimmt. Da die Nenner dieser rationalen Zahlen die Zahl n nicht übersteigen, so gibt es unter ihnen notwendig eine kleinste Zahl; ist etwa r_α diese kleinste Zahl, dann erfüllt die Zahl $r = r_\alpha$ die Bedingungen des Satzes. Denn erstens sind offenbar sämtliche Zahlen des Ideals $\mathfrak{a}$ durch p^{r_α} teilbar. Zweitens nehmen wir an, es wären sämtliche Zahlen des

Ideals $\mathfrak{a}$ durch p^R teilbar, wo R eine rationale Zahl bedeutet; es müßten dann auch die Zahl α und die zu α konjugierten Zahlen durch p^R teilbar sein, und dann wären die Koeffizienten $a_1, a_2, \ldots, a_n$ der obigen Gleichung bezüglich durch $p^R, p^{2R}, \ldots, p^{nR}$ teilbar. Hieraus folgt allgemein $iR \leqq g_i$ oder $R \leqq \frac{g_i}{i}$, und da r_α selbst eine der Zahlen $\frac{g_i}{i}$ ist, so ergibt sich $R \leqq r_\alpha$; d. h. die Zahlen des Ideals $\mathfrak{a}$ sind nicht sämtlich durch eine höhere als die r_α-te Potenz von p teilbar.

Wir beweisen nun für den Galoisschen Körper der Reihe nach die folgenden Sätze:

III. *Zu jedem vorgelegten Primideal* $\mathfrak{p}$ *läßt sich stets ein Ideal* $\mathfrak{k}$ *so bestimmen, daß das Produkt* $\mathfrak{p}\mathfrak{k}$ *ein Hauptideal ist.*

Zum Beweise bilde man die $n-1$ zu $\mathfrak{p}$ konjugierten Ideale $\mathfrak{p}', \ldots, \mathfrak{p}^{(n-1)}$. Wie man durch Übergang zu den konjugierten Körpern leicht einsieht, sind diese Ideale sämtlich ebenfalls Primideale und allen gehört die nämliche Primzahl p zu. Das Produkt $\mathfrak{a} = \mathfrak{p}\mathfrak{p}' \ldots \mathfrak{p}^{(n-1)}$ ist offenbar ein ambiges Ideal[1]. Nach Satz II gibt es eine rationale Zahl $r = \frac{t}{u}$, wo t und u ganze Zahlen sind, von der Beschaffenheit, daß die Zahlen von $\mathfrak{a}$ durch p^r, aber durch keine höhere Potenz von p teilbar sind. Das Ideal $\mathfrak{a}^u$ wird folglich durch p^t teilbar und der Quotient $\mathfrak{b} = \frac{\mathfrak{a}^u}{p^t}$ ist offenbar wieder ein ambiges Ideal. Wir nehmen nun an, es sei $\mathfrak{q}$ ein Primideal, nach welchem $\mathfrak{b} \equiv 0$ ist. Da dann auch $\mathfrak{a}^u \equiv 0$ nach $\mathfrak{q}$ ist, so müßte nach Satz 3 entweder $\mathfrak{p} \equiv 0$ oder $\mathfrak{p}' \equiv 0, \ldots,$ oder $\mathfrak{p}^{(n-1)} \equiv 0$ nach $\mathfrak{q}$ sein. Es sei etwa $\mathfrak{p}^{(m)} \equiv 0$ nach $\mathfrak{q}$, so würde, da $\mathfrak{p}^{(m)}$ ein Primideal ist, $\mathfrak{q} = \mathfrak{p}^{(m)}$ folgen, d. h. $\mathfrak{b} \equiv 0$ nach dem Primideal $\mathfrak{p}^{(m)}$ und folglich müßte nach Satz I das Ideal $\mathfrak{b}$ durch $p^{\frac{1}{n}}$ teilbar sein, d. h. $\mathfrak{a}^u$ wäre durch $p^{t+\frac{1}{n}}$ und folglich wären die Zahlen von $\mathfrak{a}$ sämtlich durch eine höhere als die r-te Potenz von p teilbar; dies widerspricht der Wahl des Exponenten r. Aus Satz 2 folgt somit $\mathfrak{b} = 1$, d. h. $\mathfrak{a}^u = p^t$. Setzen wir $\mathfrak{k} = \mathfrak{p}' \ldots \mathfrak{p}^{(n-1)}\, \mathfrak{a}^{u-1}$, so folgt $\mathfrak{p}\mathfrak{k} = p^t$.

IV. *Ein Ideal* $\mathfrak{j}$ *kann nur auf eine einzige Weise als Produkt von Primidealen dargestellt werden.*

Zum Beweise nehmen wir an, es gebe zwei Zerlegungen des Ideals $\mathfrak{j}$ etwa:

$$\mathfrak{j} = \mathfrak{p}\,\mathfrak{q}\,\mathfrak{r} \ldots \mathfrak{l},$$
$$\mathfrak{j} = \mathfrak{p}'\mathfrak{q}'\mathfrak{r}' \ldots \mathfrak{l}',$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{l}$ und $\mathfrak{p}', \mathfrak{q}', \mathfrak{r}', \ldots, \mathfrak{l}'$ Primideale sind. Da wegen der ersten Zerlegung das Ideal $\mathfrak{j} \equiv 0$ nach $\mathfrak{p}$ ist, so folgt aus der zweiten Zerlegung nach

[1] Bezeichnet man mit $\mathfrak{p}, \mathfrak{p}', \ldots, \mathfrak{p}^{(\nu-1)}$ die ν voneinander verschiedenen unter den n konjugierten Idealen, so ist auch bereits das Produkt dieser ν Ideale ein ambiges Ideal und daher gemäß der nachfolgenden Beweisführung gleich einer gebrochenen Potenz von p.

Satz 3, daß eines der Primideale $\mathfrak{p}', \mathfrak{q}', \mathfrak{r}', \ldots, \mathfrak{l}' \equiv 0$ nach $\mathfrak{p}$ ist. Es sei etwa $\mathfrak{p}' \equiv 0$ nach $\mathfrak{p}$; dann wird, weil $\mathfrak{p}'$ ein Primideal ist, notwendig $\mathfrak{p}' = \mathfrak{p}$. Nun konstruiere man nach Satz III ein Ideal $\mathfrak{k}$ von der Art, daß $\mathfrak{p}\mathfrak{k}$ gleich einem Hauptideal η wird und multipliziere die beiden obigen Darstellungen von $\mathfrak{j}$ mit $\mathfrak{k}$. Wegen $\mathfrak{p} = \mathfrak{p}'$ folgt dann

$$\eta\,\mathfrak{q}\,\mathfrak{r} \cdots \mathfrak{l} = \eta\,\mathfrak{q}'\mathfrak{r}' \cdots \mathfrak{l}'$$

und hieraus nach Satz 4:

$$\mathfrak{j}' = \mathfrak{q}\,\mathfrak{r} \cdots \mathfrak{l} = \mathfrak{q}'\mathfrak{r}' \cdots \mathfrak{l}'.$$

Auf diese doppelte Zerlegung des Ideals $\mathfrak{j}'$ wende man das eben eingeschlagene Verfahren von neuem an: man erkennt so schließlich die Identität der beiden vorgelegten Darstellungen des Ideals $\mathfrak{j}$.

V. *Ein jedes Ideal* $\mathfrak{j}$ *läßt sich stets als Produkt von Primidealen darstellen.*

Ist $\mathfrak{p}$ ein Primideal, nach welchem $\mathfrak{j} \equiv 0$ wird, so bestimme man nach Satz III ein Ideal $\mathfrak{k}$ derart, daß $\mathfrak{p}\mathfrak{k}$ gleich einem Hauptideal η wird. Durch Multiplikation jener Kongruenz mit $\mathfrak{k}$ folgt dann $\mathfrak{k}\mathfrak{j} \equiv 0$ nach dem Ideal $\mathfrak{p}\mathfrak{k}$ und gemäß Satz 4 ist daher $\mathfrak{k}\mathfrak{j} = \eta\mathfrak{j}'$. Nach Multiplikation dieser Gleichung mit $\mathfrak{p}$ und Division durch η ergibt sich $\mathfrak{j} = \mathfrak{p}\mathfrak{j}'$. Wenden wir auf das Ideal $\mathfrak{j}'$ das nämliche Verfahren an, wie soeben auf $\mathfrak{j}$, so ergibt sich $\mathfrak{j}' = \mathfrak{q}\mathfrak{j}''$, wo $\mathfrak{q}$ ein Primideal bedeutet, nach welchem $\mathfrak{j}' \equiv 0$ ist. In gleicher Weise erhalten wir $\mathfrak{j}'' = \mathfrak{r}\mathfrak{j}'''$, wo $\mathfrak{r}$ ein Primideal bedeutet, nach welchem $\mathfrak{j}'' \equiv 0$ ist usw. Die Einsetzung dieser Werte von $\mathfrak{j}', \mathfrak{j}'', \ldots$ liefert für das Ideal $\mathfrak{j}$ der Reihe nach die Darstellungen $\mathfrak{j} = \mathfrak{p}\mathfrak{q}\mathfrak{j}''$, $\mathfrak{j} = \mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{j}''', \ldots$. Nun gibt es nach Satz 1 nur eine endliche Anzahl von Idealen, nach denen $\mathfrak{j} \equiv 0$ ist. Ist m diese Anzahl, so wird jedenfalls das eingeschlagene Verfahren nach m-maliger Anwendung abbrechen. Denn es ist $\mathfrak{j} \equiv 0$ nach den Idealen $\mathfrak{p}, \mathfrak{p}\mathfrak{q}, \mathfrak{p}\mathfrak{q}\mathfrak{r}, \ldots$ und diese Ideale sind nach IV sämtlich voneinander verschieden. Nach Beendigung des Verfahrens erhalten wir für das Ideal $\mathfrak{j}$ die verlangte Zerlegung:

$$\mathfrak{j} = \mathfrak{p}\,\mathfrak{q}\,\mathfrak{r} \cdots \mathfrak{l},$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{l}$ Primideale sind.

Damit ist der Beweis des Satzes von der Zerlegung in Primideale für einen Galoisschen Körper vollständig geführt.

Wir betrachten nun einen beliebigen Körper niederen als n-ten Grades, dessen Zahlen sämtlich auch Zahlen des eben behandelten Galoisschen Körpers sind und bezeichnen zur Unterscheidung die Zahlen und Ideale dieses niederen Körpers mit großen Buchstaben. Wir denken uns die Zahlen des Galoisschen Körpers als rationale Funktionen der Wurzel ϑ einer irreduziblen Gleichung n-ten Grades dargestellt und bezeichnen dann die übrigen $n-1$ Wurzeln dieser Gleichung mit $\vartheta', \vartheta'', \ldots, \vartheta^{(n-1)}$. Diese Wurzeln sind dann rationale Funktionen von ϑ und die Einsetzung derselben an Stelle von ϑ bewirkt den Übergang zu den konjugierten Körpern. Es gibt, wie die Galoissche Theorie lehrt, eine gewisse Gruppe G von ν Substitutionen: $\vartheta = \vartheta, \vartheta = \vartheta', \ldots, \vartheta = \vartheta^{(\nu-1)}$

von der Eigenschaft, daß jede Zahl des niederen Körpers bei einer Substitution dieser Gruppe ungeändert bleibt und daß auch umgekehrt jede bei diesen Substitutionen ungeändert bleibende Zahl des Galoisschen Körpers dem niederen Körper angehört. Nun zerlege man ein Ideal $\mathfrak{J}=(\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_l)$ des niederen Körpers im Galoisschen Körper in Primideale etwa $\mathfrak{J}=\mathfrak{p}_1 \ldots \mathfrak{p}_m$ und bestimme dann die Ideale $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ derart, daß die Produkte $\mathfrak{p}_1\mathfrak{f}_1, \ldots, \mathfrak{p}_m\mathfrak{f}_m$ Hauptideale werden. Setzen wir $\mathfrak{f}=\mathfrak{f}_1 \ldots \mathfrak{f}_m$, so wird auch $\mathfrak{J}\mathfrak{f}$ gleich einem Hauptideal η und es gilt daher eine Gleichung von der Gestalt

$$\eta = \mathsf{A}_1\varkappa_1 + \mathsf{A}_2\varkappa_2 + \cdots + \mathsf{A}_l\varkappa_l,$$

wo $\varkappa_1, \varkappa_2, \ldots, \varkappa_l$ Zahlen des Ideals $\mathfrak{f}$ sind. Auf diese Gleichung wende man die Substitutionen $\vartheta=\vartheta', \ldots, \vartheta=\vartheta^{(\nu-1)}$ an; es ergeben sich dann der Reihe nach $\nu-1$ Gleichungen von der Gestalt

$$\begin{aligned} \eta' &= \mathsf{A}_1\varkappa_1' + \mathsf{A}_2\varkappa_2' + \cdots + \mathsf{A}_l\varkappa_l', \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta^{(\nu-1)} &= \mathsf{A}_1\varkappa_1^{(\nu-1)} + \mathsf{A}_2\varkappa_2^{(\nu-1)} + \cdots + \mathsf{A}_l\varkappa_l^{(\nu-1)}. \end{aligned}$$

Die Multiplikation aller ν Gleichungen liefert

$$\mathsf{H} = \mathsf{A}_1^\nu\mathsf{K}_1 + \mathsf{A}_1^{\nu-1}\mathsf{A}_2\mathsf{K}_2 + \mathsf{A}_1^{\nu-2}\mathsf{A}_2^2\mathsf{K}_3 + \cdots + \mathsf{A}_l^\nu\mathsf{K}_M,$$

wo sowohl $\mathsf{H}=\eta\eta' \ldots \eta^{(\nu-1)}$ als auch die Koeffizienten $\mathsf{K}_1, \ldots, \mathsf{K}_M$ bei Anwendung der Substitutionen der Gruppe G ungeändert bleiben und daher Zahlen des niederen Körpers sind. Bezeichnen wir das Ideal $(\mathsf{K}_1, \ldots, \mathsf{K}_M)$ des niederen Körpers mit $\mathfrak{K}$, so gilt im niederen Körper die Gleichung $\mathsf{H}=\mathfrak{J}^\nu\mathfrak{K}$. In der Tat ist H infolge der vorigen Gleichung eine Zahl des Ideals $\mathfrak{J}^\nu\mathfrak{K}$ und es bedarf daher nur des Nachweises, daß jede Zahl des Ideals $\mathfrak{J}^\nu\mathfrak{K}$ durch H teilbar ist. Nun ergibt wegen $\eta=\mathfrak{J}\mathfrak{f}$ jede der Zahlen $\mathsf{A}_1, \ldots, \mathsf{A}_l$ mit jeder der Zahlen $\varkappa_1, \ldots, \varkappa_l$ multipliziert ein durch η teilbares Produkt, ebenso ergibt jede der Zahlen $\mathsf{A}_1, \ldots, \mathsf{A}_l$ mit jeder der Zahlen $\varkappa_1', \ldots, \varkappa_l'$, multipliziert ein durch η' teilbares Produkt usw. und hieraus folgt, daß das Produkt von irgend ν Zahlen $\mathsf{A}_1, \ldots, \mathsf{A}_l$ multipliziert mit einer der Zahlen $\mathsf{K}_1, \ldots, \mathsf{K}_M$ durch $\eta\eta' \ldots \eta^{(\nu-1)}=\mathsf{H}$ teilbar ist. Setzen wir $\mathfrak{J}^{\nu-1}\mathfrak{K}=\mathfrak{L}$, so wird $\mathfrak{J}\mathfrak{L}=\mathsf{H}$ und diese Gleichung zeigt, daß zu jedem vorgelegten Ideal des niederen Körpers stets ein Ideal $\mathfrak{L}$ des niederen Körpers derart bestimmt werden kann, daß das Produkt $\mathfrak{J}\mathfrak{L}$ ein Hauptideal H des niederen Körpers wird. Aus diesem Satze kann der Satz von der eindeutigen Zerlegung eines Ideals in Primideale für den niederen Körper genau so geschlossen werden, wie oben aus Satz III die Sätze IV und V abgeleitet worden sind. Da ferner ein jeder beliebige Körper als ein Körper aufgefaßt werden kann, welcher in einem Galoisschen Körper als niederer Körper enthalten ist, so haben wir hiermit den Satz von der eindeutigen Zerlegung eines Ideals allgemein als gültig erkannt.

Ostseebad Cranz, den 26. September 1893.

4. Grundzüge einer Theorie des Galoisschen Zahlkörpers[1].

[Nachrichten der Gesellschaft der Wissenschaften zu Göttingen 1894. S. 224—236.]

Da ein jeder beliebige Zahlkörper als ein Körper aufgefaßt werden kann, welcher in einem Galoisschen Körper als niederer Körper enthalten ist, so bedeutet es keine wesentliche Einschränkung, wenn wir bei der Erforschung der Theorie der algebraischen Zahlen von vornherein die Annahme machen, daß der zugrunde liegende Zahlkörper ein Galoisscher Körper ist. Insbesondere erweist sich der systematische Ausbau der allgemeinen Theorie der Ideale eines Galoisschen Körpers als notwendig, wenn wir den in KUMMERS Abhandlungen über die höheren Reziprozitätsgesetze enthaltenen Anregungen mit Erfolg nachgehen und über die in denselben gewonnenen Resultate zur vollen Herrschaft gelangen wollen. Die vorliegende Note enthält in Kürze die Grundzüge einer solchen Theorie des Galoisschen Körpers.

Der Galoissche Körper K vom M-ten Grade werde durch die Zahl Θ bestimmt, welche einer irreduziblen ganzzahligen Gleichung M-ten Grades genügt. Die Wurzeln derselben seien $\Theta=s_1\Theta, s_2\Theta, \ldots, s_M\Theta$, wo die Substitutionen $s_1, s_2, \ldots, s_M$ eine Gruppe G vom M-ten Grade bilden. $\mathfrak{P}$ sei ein Primideal f-ten Grades in K; p die durch $\mathfrak{P}$ teilbare rationale Primzahl und P sei eine Primitivzahl für das Primideal $\mathfrak{P}$, d. h. P sei von der Beschaffenheit, daß jede ganze Zahl des Körpers K einer Potenz von P nach dem Primideal $\mathfrak{P}$ kongruent wird.

Die Primitivzahl P genügt nach dem Primideal $\mathfrak{P}$ einer Kongruenz von der Gestalt

$$\Phi(x) \equiv 0, \qquad (\mathfrak{P}),$$

wo $\Phi(x)$ eine ganze Funktion f-ten Grades in x mit ganzen rationalen Koeffizienten bedeutet, welche im Sinne der Kongruenz nach der rationalen Primzahl p irreduzibel ist. Es gilt ferner der Hilfssatz:

Wenn Ω irgendeine ganze Zahl in K ist, so gibt es unter den Substitutionen $s_1, s_2, \ldots, s_M$ stets wenigstens eine Substitution s von der Art, daß nach dem Primideal $\mathfrak{P}$ die Kongruenz

$$s\,\Omega \equiv \Omega^p, \qquad (\mathfrak{P})$$

besteht.

[1] Man sehe hierzu auch die Ausführungen im „Bericht über die Theorie der algebraischen Zahlkörper", dieser Band, Abh. 7, S. 129—146.

Zum Beweise dieses Hilfssatzes bilden wir die ganze ganzzahlige Funktion

$$F(x) = (x - s_1\Omega)(x - s_2\Omega) \ldots (x - s_M\Omega)$$

und erhalten dann wegen

$$F(x^p) \equiv [F(x)]^p, \qquad (p)$$

die Kongruenz

$$(\Omega^p - s_1\Omega)(\Omega^p - s_2\Omega) \ldots (\Omega^p - s_M\Omega) \equiv 0, \qquad (\mathfrak{P}),$$

welche die Richtigkeit des Hilfssatzes erkennen läßt.

Nun seien $z, z', z'', \ldots$ diejenigen sämtlichen r_z Substitutionen der Gruppe G, welche das Primideal $\mathfrak{P}$ ungeändert lassen; dieselben bilden eine Gruppe vom r_z-ten Grade, welche die *Zerlegungsgruppe* des Primideals $\mathfrak{P}$ genannt und mit g_z bezeichnet werden soll.

Nehmen wir $\Omega = A^{p^f-1}P$, wo A eine nicht durch $\mathfrak{P}$, wohl aber durch alle zu $\mathfrak{P}$ konjugierten und von $\mathfrak{P}$ verschiedenen Primideale teilbare ganze Zahl ist, so zeigt die Anwendung des Hilfssatzes die Existenz einer Substitution s von der Art, daß die Kongruenz

$$s[A^{p^f-1}P] \equiv A^{p(p^f-1)}P^p, \qquad (\mathfrak{P}),$$

oder

$$[sA]^{p^f-1}sP \equiv P^p, \qquad (\mathfrak{P})$$

gilt. Hieraus folgt $sA \not\equiv 0$ nach $\mathfrak{P}$ und $sP \equiv P^p$ nach $\mathfrak{P}$. Die erste Inkongruenz lehrt, daß A nicht durch $s^{-1}\mathfrak{P}$ teilbar ist; folglich wird $s^{-1}\mathfrak{P} = \mathfrak{P}$ oder $\mathfrak{P} = s\mathfrak{P}$ d. h. die Substitution s gehört der Zerlegungsgruppe g_z an. Wir setzen $s = z$ und haben dann die Kongruenz

$$zP \equiv P^p, \qquad (\mathfrak{P}).$$

Die wiederholte Anwendung der Substitution z liefert die Kongruenzen

$$z^2P \equiv P^{p^2}, \quad z^3P \equiv P^{p^3}, \ \ldots, \ z^fP \equiv P^{p^f} \equiv P, \qquad (\mathfrak{P}),$$

Infolge der letzten Kongruenz ist $t = z^f$ eine Substitution von der Beschaffenheit, daß für jede beliebige ganze Zahl Ω des Körpers K die Kongruenz

$$t\Omega \equiv \Omega, \qquad (\mathfrak{P})$$

erfüllt ist. Es seien $t, t', t'', \ldots$ diejenigen sämtlichen r_t Substitutionen der Gruppe G, denen ebenfalls die genannte Eigenschaft zukommt; dann wird leicht gezeigt, daß diese r_t Substitutionen eine Gruppe r_t-ten Grades bilden. Diese Gruppe werde die *Trägheitsgruppe* des Primideals $\mathfrak{P}$ genannt und mit g_t bezeichnet. Da, wie ebenfalls leicht ersichtlich ist, das Primideal $\mathfrak{P}$ bei der Anwendung einer jeden der Substitutionen $t, t', t'', \ldots$ ungeändert bleibt, so ist die Trägheitsgruppe g_t eine Untergruppe der Zerlegungsgruppe g_z; es ergibt sich ferner leicht der Satz:

Die Trägheitsgruppe g_t eines Primideals ist eine invariante (d. h. ausgezeichnete) Untergruppe der Zerlegungsgruppe g_z.

Ist z^* eine beliebige Substitution der Zerlegungsgruppe, so folgt aus der Kongruenz $\Phi(P) \equiv 0$ nach $\mathfrak{P}$ notwendig $\Phi(z^*P) \equiv 0$ nach $\mathfrak{P}$ und da die Kongruenz $\Phi(x) \equiv 0$ nach $\mathfrak{P}$ nur die f Kongruenzwurzeln $P, P^p, P^{p^2}, \ldots, P^{p^{f-1}}$ besitzt, so folgt $z^*P \equiv P^{p^i}$ nach $\mathfrak{P}$, wo i einen der f Werte $0, 1, \ldots, f-1$ hat. Da andrerseits $P^{p^i} \equiv z^iP$ ist, so wird $z^{-i}z^*P \equiv P$ nach $\mathfrak{P}$ und mithin ist $z^{-i}z^*$ eine Substitution t der Trägheitsgruppe, d. h. $z^* = z^it$. In dieser letzteren Gestalt sind also sämtliche Substitutionen $z, z', z'', \ldots$ der Zerlegungsgruppe darstellbar und da auch umgekehrt z^it für $i = 0, 1, \ldots, f-1$ lauter voneinander verschiedene Substitutionen darstellt, so ist $r_z = fr_t$. Wir fassen diese Resultate in folgendem Satze zusammen:

Der Grad der Zerlegungsgruppe g_z eines Primideals $\mathfrak{P}$ ist gleich dem Produkte des Grades f von $\mathfrak{P}$ in den Grad der Trägheitsgruppe g_t. Man erhält die Substitutionen der Zerlegungsgruppe, wenn man die Substitutionen der Trägheitsgruppe mit $1, z, z^2, \ldots, z^{f-1}$ multipliziert, wo z eine geeignet gewählte Substitution der Zerlegungsgruppe ist. z^f gehört der Trägheitsgruppe an.

Es erweist sich jetzt die Einführung der folgenden allgemeinen Begriffe als notwendig. Bilden die r Substitutionen $s_1 = 1, s_2, \ldots, s_r$ von G eine Untergruppe g vom r-ten Grade, so bestimmt die Gesamtheit aller Zahlen des Körpers K, welche bei Anwendung einer jeden Substitution von g ungeändert bleiben, einen in K enthaltenen Unterkörper $\varkappa$ vom Grade $m = \frac{M}{r}$.

Ist A eine beliebige Zahl, $\mathfrak{J}$ ein beliebiges Ideal in K, so heißt das Produkt

$$\nu(A) = s_1A \cdot s_2A \ldots s_rA$$

die Partialnorm von A in bezug auf die Gruppe g oder den Unterkörper $\varkappa$; des gleichen heißt

$$\nu(\mathfrak{J}) = s_1\mathfrak{J} \cdot s_2\mathfrak{J} \ldots s_r\mathfrak{J}$$

die *Partialnorm* des Ideals $\mathfrak{J}$ in bezug auf den Körper $\varkappa$.

Die Partialnorm $\lambda(A)$ einer Zahl A ist offenbar stets eine Zahl in $\varkappa$. Wir sagen nun, ein Ideal $\mathfrak{J}$ des Körpers K *liege im Körper* $\varkappa$ oder *sei ein Ideal des Körpers* $\varkappa$, wenn dasselbe als größter gemeinsamer Teiler von Zahlen des Körpers $\varkappa$ dargestellt werden kann. Die Partialnorm $\nu(\mathfrak{J})$ eines Ideals $\mathfrak{J}$ ist stets ein Ideal, welches im Körper $\varkappa$ liegt.

Der zur Zerlegungsgruppe g_z gehörige Körper $\varkappa_z$ werde *Zerlegungskörper* genannt; derselbe ist vom Grade $m_z = \frac{M}{r_z}$.

Der zur Trägheitsgruppe g_t gehörige Körper $\varkappa_t$ werde *Trägheitskörper* genannt; derselbe ist vom Grade $m_t = \frac{M}{r_t}$ und enthält den Zerlegungskörper als Unterkörper.

Das algebraische Verhältnis zwischen Zerlegungskörper und Trägheitskörper wird durch den folgenden Satz klargelegt:

Ist ϑ_t eine den Trägheitskörper bestimmende Zahl, so genügt ϑ_t einer Gleichung f-ten Grades von der Gestalt

$$\vartheta_t^f + \alpha_z \vartheta_t^{f-1} + \alpha_z' \vartheta_t^{f-2} + \cdots = 0,$$

deren Koeffizienten Zahlen des Körpers $\varkappa_z$ sind, und welche im Rationalitätsbereiche $\varkappa_z$ eine Galoissche Gleichung mit der zyklischen Gruppe f-ten Grades ist.

Die Partialnormen des Primideals $\mathfrak{P}$ in bezug auf die Körper $\varkappa_z$ und $\varkappa_t$ sind

$$\nu_z(\mathfrak{P}) = \mathfrak{P}^{r_z} \quad \text{und} \quad \nu_t(\mathfrak{P}) = \mathfrak{P}^{r_t}.$$

Um nun die niedrigste in $\varkappa_z$ liegende Potenz des Primideals $\mathfrak{P}$ zu ermitteln, denken wir uns den größten gemeinsamen Teiler aller derjenigen ganzen Zahlen des Körpers $\varkappa_z$ bestimmt, welche durch $\mathfrak{P}$ teilbar sind. Dieser Teiler ist notwendig im Körper $\varkappa_z$ ein Primideal $\mathfrak{p}$ und da $\mathfrak{P}^{r_z}$ in $\varkappa_z$ liegt, so ist $\mathfrak{p}$ jedenfalls eine Potenz von $\mathfrak{P}$; wir setzen $\mathfrak{p} = \mathfrak{P}^u$. Zur Bestimmung des Exponenten u dient die folgende Betrachtung. Soll eine durch $\mathfrak{P}$ nicht teilbare Zahl A des Körpers K der Kongruenz $A \equiv zA$ nach $\mathfrak{P}$ genügen und ist etwa $A \equiv P^i$ nach $\mathfrak{P}$, so muß notwendig $i \equiv pi$ nach $p^f - 1$ und folglich i eine durch $1 + p + p^2 + \ldots + p^{f-1}$ teilbare Zahl sein, d. h. es gibt nur $p - 1$ untereinander nach $\mathfrak{P}$ inkongruente Zahlen von der gewünschten Beschaffenheit, und es wird daher $A \equiv a$ nach $\mathfrak{P}$, wo a eine ganze rationale Zahl bedeutet. Aus dieser Betrachtung folgt insbesondere, daß jede Zahl α des Körpers $\varkappa_z$ einer rationalen Zahl a nach $\mathfrak{P}$ und mithin auch nach $\mathfrak{p}$ kongruent ist, d. h. $\mathfrak{p}$ ist im Körper $\varkappa_z$ ein Primideal ersten Grades und die Norm $n(\mathfrak{p})$ im Körper $\varkappa_z$ ist folglich gleich p. Andrerseits ist die Norm von $\mathfrak{p}$ im Körper K durch die Formel $N(\mathfrak{p}) = [n(\mathfrak{p})]^{r_z}$ gegeben, und wegen $\mathfrak{p} = \mathfrak{P}^u$ und $N(\mathfrak{P}) = p^f$ folgt somit $p^{uf} = p^{r_z}$ d. h. $u = r_t$. Daraus folgt der Satz:

Das Ideal $\mathfrak{p} = \mathfrak{P}^{r_t}$ liegt im Zerlegungskörper $\varkappa_z$ und ist in diesem ein Primideal ersten Grades: es wird also jede ganze Zahl des Körpers $\varkappa_z$ einer rationalen Zahl kongruent nach $\mathfrak{p}$.

Da notwendig die bezüglich $\varkappa_z$ zu $\mathfrak{p}$ konjugierten $m_z - 1$ Ideale zu $\mathfrak{p}$ prim sind und mit $\mathfrak{p}$ multipliziert das Produkt p ergeben, so ist der Zerlegungskörper zugleich der Körper niedrigsten Grades, in welchem die Zerlegung der rationalen Primzahl p soweit bewirkt wird, daß dabei eine Trennung der Faktoren $\mathfrak{P}$ von den übrigen stattfindet.

Um den Bau der Trägheitsgruppe näher zu erforschen, bezeichnen wir mit A eine durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare Zahl des Körpers K und bilden für alle Substitutionen $t, t', t'', \ldots$, der Trägheitsgruppe die Kongruenzen

$$\left.\begin{aligned} tA &\equiv P^a A, \\ t'A &\equiv P^{a'} A, \\ t''A &\equiv P^{a''} A, \\ &\cdots\cdots\cdots \end{aligned}\right\} \qquad (\mathfrak{P}^2)$$

wo $a, a', a'', \ldots$ Zahlen aus der Reihe $0, 1, 2, \ldots, p^f - 2$ bedeuten. Diejenigen unter den Substitutionen $t, t', t'', \ldots$, für welche die betreffenden Exponenten $a, a', a'', \ldots$ den Wert 0 haben, mögen mit $v, v', v'' \ldots$ bezeichnet werden; ihre Zahl sei r_v; sie bilden, wie leicht ersichtlich, eine invariante Untergruppe der Trägheitsgruppe. Diese Untergruppe r_v-ten Grades werde die *Verzweigungsgruppe* des Primideals $\mathfrak{P}$ genannt und mit g_v bezeichnet. Der zu g_v gehörige Körper heiße der *Verzweigungskörper* des Primideals $\mathfrak{P}$.

Es sei $\mathfrak{P}^u$ eine so hohe Potenz von $\mathfrak{P}$, daß für jede von 1 verschiedene Substitution v der Verzweigungsgruppe die Inkongruenz $vA \not\equiv A$ nach $\mathfrak{P}^u$ gilt. Setzen wir nun $vA \equiv A + BA^2$ nach $\mathfrak{P}^3$, wo B eine ganze Zahl in K bedeutet, so folgt leicht $v^p A \equiv A$ nach $\mathfrak{P}^3$ und hieraus in gleicher Weise $v^{p^2} A \equiv A$ nach $\mathfrak{P}^4$ und endlich $v^{p^{u-2}} A \equiv A$ nach $\mathfrak{P}^u$. Demnach ist $v^{p^{u-2}} = 1$, d. h. der Grad r_v der Verzweigungsgruppe ist gleich einer Potenz von p; wir setzen $r_v = p^l$.

Es sei nun a der kleinste von 0 verschiedene unter den Exponenten $a, a', a'' \ldots$ und es gebe im ganzen h voneinander verschiedene solcher Exponenten. Dann sind diese Exponenten notwendig Vielfache von a und stimmen mit den Zahlen $0, a, 2a, \ldots, (h-1)a$ überein; es ist ferner $ha = p^f - 1$. Zugleich erkennen wir, daß alle Substitutionen der Trägheitsgruppe in die Gestalt $t^i v$ gebracht werden können, wo i die Werte $0, 1, \ldots, h-1$ annimmt und v alle Substitutionen der Verzweigungsgruppe g_v durchläuft. Es ist folglich $r_t = hr_v$. Wir fassen wiederum die erhaltenen Sätze zusammen:

Die Verzweigungsgruppe g_v ist eine invariante Untergruppe der Trägheitsgruppe, der Grad r_v derselben ist eine Potenz von p. Der Grad der Trägheitsgruppe ist gleich dem h-fachen Grade der Verzweigungsgruppe, wo h einen Teiler von $p^f - 1$ bedeutet und daher nicht den Faktor p enthält. Man erhält die Substitutionen der Trägheitsgruppe, indem man die Substitutionen der Verzweigungsgruppe mit $1, t, t^2, \ldots, t^{h-1}$ multipliziert, wo t eine geeignet gewählte Substitution der Trägheitsgruppe ist. t^h ist eine Substitution der Verzweigungsgruppe.

Das algebraische Verhältnis zwischen Trägheitskörper und Verzweigungskörper wird durch den folgenden Satz klargelegt:

Ist ϑ_v eine den Verzweigungskörper bestimmende Zahl, so genügt ϑ_v einer Gleichung h-ten Grades von der Gestalt

$$\vartheta_v^h + \alpha_t \vartheta_v^{h-1} + \alpha_t' \vartheta_v^{h-2} + \cdots = 0,$$

deren Koeffizienten Zahlen des Körpers $\varkappa_t$ sind und welche im Rationalitätsbereiche $\varkappa_t$ eine Galoissche Gleichung mit der zyklischen Gruppe h-ten Grades ist.

Um nun vor allem Aufschluß über das Verhalten des Ideals $\mathfrak{p}$ im Körper $\varkappa_t$ zu gewinnen, setzen wir

$$\pi = \{vP \cdot v'P \cdot v''P \ldots\}^{p^{l(f-1)}}$$

$$\varrho = \frac{1}{h}(\pi + t\pi + t^2\pi + \cdots + t^{h-1}\pi).$$

Die Zahl π liegt im Körper $\varkappa_v$ und ϱ im Körper $\varkappa_t$; beide Zahlen sind nach dem Primideal $\mathfrak{P}$ der Primitivzahl P kongruent. Da es folglich im Körper $\varkappa_t$ genau p^f nach $\mathfrak{P}$ inkongruente Zahlen gibt, so ist notwendigerweise $\mathfrak{p} = \mathfrak{P}^{r_t}$ im Körper $\varkappa_t$ unzerlegbar und wird in demselben ein Primideal f-ten Grades.

Die aus der eben angestellten Betrachtung folgenden Eigenschaften des Trägheitskörpers sprechen wir wie folgt aus:

Jede Zahl des Körpers K ist nach $\mathfrak{P}$ einer Zahl des Trägheitskörpers kongruent. Der Trägheitskörper bewirkt keine Zerlegung des Ideals $\mathfrak{p}$, sondern nur eine Graderhöhung desselben, insofern $\mathfrak{p}$ beim Übergang vom Körper $\varkappa_z$ in den höheren Körper $\varkappa_t$ aus einem Primideal ersten Grades sich in ein Primideal f-ten Grades verwandelt.

Es sei die beliebige Zahl Ω in K der Zahl ω des Trägheitskörpers nach $\mathfrak{P}$ kongruent und dementsprechend werde $\Omega - \omega \equiv BA$ nach $\mathfrak{P}^2$ gesetzt, wo A die obige Bedeutung hat und B eine geeignete ganze Zahl in K ist. Durch die Anwendung einer Substitution v des Verzweigungskörpers ergibt sich $v\Omega - \omega \equiv v(BA) \equiv BA \equiv \Omega - \omega$, d. h. $v\Omega \equiv \Omega$ nach $\mathfrak{P}^2$ und wir erhalten so den Satz:

Die Substitutionen v der Verzweigungsgruppe g_v haben die charakteristische Eigenschaft, daß für sämtliche Zahlen Ω des Körpers K die Kongruenz

$$v\Omega \equiv \Omega, \qquad (\mathfrak{P}^2)$$

besteht.

Zugleich erkennen wir leicht die folgenden weiteren Sätze über den Verzweigungskörper.

Das Ideal $\mathfrak{p}_v = \mathfrak{P}^{p^f}$ liegt im Verzweigungskörper $\varkappa_v$ und ist in demselben ein Primideal f-ten Grades: es findet somit im Verzweigungskörper die Spaltung des Ideals $\mathfrak{p} = \mathfrak{p}_v^h$ in h gleiche Primfaktoren statt.

Unsere nächste Aufgabe besteht darin, die Spaltung des Ideals $\mathfrak{p}_v$ zu verfolgen. Zu dem Zwecke nehmen wir an, es sei L der höchste Exponent von der Art, daß für eine jede Substitution v der Verzweigungsgruppe die sämtlichen ganzen Zahlen des Körpers K der Kongruenz

$$v\Omega \equiv \Omega, \qquad (\mathfrak{P}^L)$$

genügen und bestimmen dann alle diejenigen Substitutionen $\bar{v}$ der Verzweigungsgruppe, für welche

$$\bar{v}\Omega \equiv \Omega, \qquad (\mathfrak{P}^{L+1})$$

wird; dieselben bilden eine invariante Untergruppe $g_{\bar{e}}$ der Verzweigungsgruppe, die wir die *einmal überstrichene Verzweigungsgruppe* nennen wollen. Der Grad derselben sei $r_{\bar{e}} = p^{\bar{l}}$. Die Eigenschaften dieser Untergruppe $g_{\bar{e}}$ lassen sich wiederum ohne besondere Schwierigkeit feststellen und führen, wenn der Kürze wegen der zu $g_{\bar{e}}$ gehörige Körper $\varkappa_e$ der *einmal überstrichene Verzweigungskörper* genannt und $l - \bar{l} = \bar{e}$ gesetzt wird, zu den Sätzen:

Ist $\vartheta_{\bar{e}}$ eine den einmal überstrichenen Verzweigungskörper $\varkappa_{\bar{e}}$ bestimmende Zahl, so genügt $\vartheta_{\bar{e}}$ einer Abelschen Gleichung $p^{\bar{e}}$-ten Grades von der Gestalt

$$\vartheta_{\bar{e}}^{p^{\bar{e}}} + \alpha_e \vartheta_{\bar{e}}^{p^{\bar{e}-1}} + \alpha_e' \vartheta_{\bar{e}}^{p^{\bar{e}-2}} + \cdots = 0,$$

deren Koeffizienten Zahlen des Körpers $\varkappa_e$ sind und deren Gruppe lediglich Substitutionen p-ten Grades enthält. Es wird $\mathfrak{p}_e = \mathfrak{p}_{\bar{e}}^{p^{\bar{e}}}$, wo $\mathfrak{p}_{\bar{e}}$ Primideal des Körpers $\varkappa_{\bar{e}}$ ist. Der Exponent $\bar{e}$ überschreitet keinenfalls die Zahl f.

Nunmehr ist ersichtlich, in welcher Weise das eingeschlagene Verfahren fortzusetzen ist. Bedeutet $\bar{L}$ den höchsten Exponenten von der Art, daß für jede Substitution $\bar{v}$ die sämtlichen Zahlen des Körpers K der Kongruenz

$$\bar{v}\Omega \equiv \Omega, \qquad (\mathfrak{P}^{\bar{L}})$$

genügen, so bestimmen wir alle diejenigen Substitutionen $\bar{v}$, für welche

$$\bar{v}\Omega \equiv \Omega, \qquad (\mathfrak{P}^{\bar{L}+1})$$

wird. Dieselben bilden eine invariante Untergruppe $g_{\bar{\bar{e}}}$ der Gruppe $g_{\bar{e}}$, die *zweimal überstrichene Verzweigungsgruppe*; ihr Grad sei $r_{\bar{\bar{e}}} = p^{\bar{\bar{l}}}$; wir setzen $\bar{l} - \bar{\bar{l}} = \bar{\bar{e}}$. Es gelten die Sätze:

Ist $\vartheta_{\bar{\bar{e}}}$ eine den zweimal überstrichenen Verzweigungskörper $\varkappa_{\bar{\bar{e}}}$ bestimmende Zahl, so genügt $\vartheta_{\bar{\bar{e}}}$ einer Abelschen Gleichung $p^{\bar{\bar{e}}}$-ten Grades von der Gestalt

$$\vartheta_{\bar{\bar{e}}}^{p^{\bar{\bar{e}}}} + \alpha_{\bar{e}} \vartheta_{\bar{\bar{e}}}^{p^{\bar{\bar{e}}-1}} + \alpha_{\bar{e}}' \vartheta_{\bar{\bar{e}}}^{p^{\bar{\bar{e}}-2}} + \cdots = 0,$$

deren Koeffizienten Zahlen des Körpers $\varkappa_{\bar{\bar{e}}}$ sind und deren Gruppe lediglich Substitutionen p-ten Grades enthält. Es wird $\mathfrak{p}_{\bar{e}} = \mathfrak{p}_{\bar{\bar{e}}}^{p^{\bar{\bar{e}}}}$, wo $\mathfrak{p}_{\bar{\bar{e}}}$ Primideal des Körpers $\varkappa_{\bar{\bar{e}}}$ ist. Der Exponent $\bar{\bar{e}}$ überschreitet keinenfalls die Zahl f.

So fortfahrend gelangen wir zu einer dreimal überstrichenen Verzweigungsgruppe $g_{\bar{\bar{\bar{e}}}}$ usw. Ist etwa die $k$mal überstrichene Verzweigungsgruppe diejenige, welche lediglich aus der Substitution 1 besteht, so ist der Körper K selbst der $k$mal überstrichene Verzweigungskörper und die Struktur der Verzweigungsgruppe g_v ist dann vollständig bekannt.

Durch die vorstehende Entwicklung erlangen wir einen vollständigen Einblick in die bei der Zerlegung einer rationalen Primzahl p sich abspielenden Vorgänge:

Die rationale Primzahl p wird zunächst im Zerlegungskörper in der Form $p = \mathfrak{p}\mathfrak{a}$ zerlegt, wo $\mathfrak{p}$ ein Primideal ersten Grades und $\mathfrak{a}$ ein durch $\mathfrak{p}$ nicht teilbares Ideal des Zerlegungskörpers ist. Der Zerlegungskörper ist als Unterkörper in dem Trägheitskörper enthalten, welcher seinerseits keine weitere Zerlegung von $\mathfrak{p}$ bewirkt, sondern lediglich dieses Ideal $\mathfrak{p}$ zu einem Primideal f-ten Grades erhebt. Ist der Körper K selbst der Zerlegungskörper oder der Trägheitskörper, so ist nach diesem ersten Schritte die Zerlegung bereits abgeschlossen. Im anderen Falle läßt sich $\mathfrak{p}$ in gleiche Faktoren spalten, und zwar

wird $\mathfrak{p}$ zunächst im Verzweigungskörper die Potenz eines Primideals $\mathfrak{p}_e$, deren Exponent in $p'-1$ aufgeht und folglich nicht durch p teilbar ist. Die Spaltung von $\mathfrak{p}$ ist mit diesem zweiten Schritte notwendig dann und nur dann abgeschlossen, wenn p im Grade der Trägheitsgruppe nicht aufgeht und mithin der Körper K selbst der Verzweigungskörper ist. In den nun folgenden überstrichenen Verzweigungskörpern schreitet die Spaltung ohne Aussetzen fort, und zwar sind die bezüglichen Potenzexponenten Zahlen von der Gestalt $p^{\bar{e}}$, $p^{\bar{\bar{e}}}, \ldots$, wo $\bar{e}, \bar{\bar{e}}, \ldots$ die Zahl f nicht überschreiten. Der Trägheitskörper und der Verzweigungskörper sind durch zyklische Gleichungen, die überstrichenen Verzweigungskörper durch solche Abelsche Gleichungen bestimmt, deren Gruppen nur Substitutionen vom Primzahlgrade p enthalten. Die Spaltung in *gleiche* Faktoren geschieht also stets mittels einer Kette Abelscher Gleichungen. Dieses Resultat drückt eine neue überraschende Eigenschaft des Zerlegungskörpers aus:

Der Zerlegungskörper bestimmt einen Rationalitätsbereich, in welchem die Zahlen des ursprünglichen Galoisschen Körpers K lediglich durch Wurzelausdrücke darstellbar sind.

Der gefundene Satz rückt zugleich die Bedeutung der Theorie der durch Wurzelziehen lösbaren Gleichungen in grelles Licht, insofern derselbe zeigt, daß innerhalb der durch solche Gleichungen bestimmten Zahlkörper gerade die hauptsächlichsten Schwierigkeiten ihre Lösung finden, welche die Aufstellung der Primideale bietet.

Die Übersicht über die aufgezählten Resultate wird durch die folgende Tabelle erleichtert, in deren Zeilen der Reihe nach die Grade der Gruppen, die Grade der Körper, die Grade der den Körper bestimmenden Abelschen Gleichungen, dann die Primideale der Körper und ihre Zerlegung, bezüglich Spaltung sich angegeben finden. Der Körper K ist dabei als ein dreimal überstrichener Verzweigungskörper angenommen.

$\varkappa_s$	$\varkappa_t$	$\varkappa_e$	$\varkappa_{\bar{e}}$	$\varkappa_{\bar{\bar{e}}}$	K
r_s	r_t	r_e	$r_{\bar{e}}$	$r_{\bar{\bar{e}}}$	1
$m_s = \frac{M}{r_s}$	$m_t = \frac{M}{r_t}$	$m_e = \frac{M}{r_e}$	$m_{\bar{e}} = \frac{M}{r_{\bar{e}}}$	$m_{\bar{\bar{e}}} = \frac{M}{r_{\bar{\bar{e}}}}$	M
	$f = \frac{r_s}{r_t}$	$h = \frac{r_t}{r_e}$	$p^{\bar{e}} = \frac{r_e}{r_{\bar{e}}}$	$p^{\bar{\bar{e}}} = \frac{r_{\bar{e}}}{r_{\bar{\bar{e}}}}$	$p^{\bar{\bar{\bar{e}}}} = r_{\bar{\bar{e}}}$
$\mathfrak{p} = \mathfrak{p}_e^h = \mathfrak{P}^{r_t}$		$\mathfrak{p}_e = \mathfrak{p}_{\bar{e}}^{p^{\bar{e}}} = \mathfrak{P}^{r_e}$	$\mathfrak{p}_{\bar{e}} = \mathfrak{p}_{\bar{\bar{e}}}^{p^{\bar{\bar{e}}}} = \mathfrak{P}^{r_{\bar{e}}}$	$\mathfrak{p}_{\bar{\bar{e}}} = \mathfrak{P}^{p^{\bar{\bar{\bar{e}}}}} = \mathfrak{P}^{r_{\bar{\bar{e}}}}$	$\mathfrak{P}$

Von den mannigfachen Folgerungen und Anwendungen, welche die vorstehend entwickelte Theorie zuläßt, seien hier nur einige erwähnt, welche die Erforschung der Diskriminanten der betrachteten Zahlkörper bezwecken.

Es sei $\varkappa$ ein beliebiger Zahlkörper vom Grade m; $\omega_1, \omega_2, \ldots, \omega_m$ mögen eine Basis der ganzen Zahlen des Körpers $\varkappa$ bilden und die zu der Zahl ω konjugierten $m-1$ Zahlen bezeichnen wir allgemein mit $\omega', \ldots, \omega^{(m-1)}$. Das Produkt der $m-1$ Ideale[1]

$$\begin{aligned}&(\omega_1 - \omega_1', \quad \omega_2 - \omega_2', \ldots, \quad \omega_m - \omega_m')\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ &(\omega_1 - \omega_1^{(m-1)}, \quad \omega_2 - \omega_2^{(m-1)}, \ldots, \quad \omega_m - \omega_m^{(m-1)})\end{aligned}$$

ist ein Ideal des Körpers $\varkappa$ und stimmt mit demjenigen überein, welches R. Dedekind das Grundideal dieses Körpers nennt. R. Dedekind hat bewiesen, daß die Norm des Grundideals die Diskriminante des Körpers liefert[2].

Es seien $s_1 = 1, s_2, \ldots, s_r$ die r Substitutionen einer Untergruppe g der Gruppe G und $\varkappa$ sei der zu g gehörige Körper. Sind dann $\Omega_1, \Omega_2, \ldots, \Omega_M$ eine Basis der ganzen Zahlen des Körpers K und bildet man alle r-reihigen Determinanten $\Delta, \Delta', \ldots$ der Matrix

$$\begin{aligned}&s_1\Omega_1, s_1\Omega_2, \ldots, s_1\Omega_M,\\ &s_2\Omega_1, s_2\Omega_2, \ldots, s_2\Omega_M,\\ &\cdots\cdots\cdots\\ &s_r\Omega_1, s_r\Omega_2, \ldots, s_r\Omega_M,\end{aligned}$$

so wird das Quadrat des größten gemeinsamen Idealteilers der Zahlen Δ, $\Delta', \ldots$ die *Partialdiskriminante*[3] des Körpers K in bezug auf den Körper $\varkappa$ genannt. Bei Benutzung der von mir angewandten Bezeichnungsweise ist diese also

$$\mathfrak{d} = (\Delta, \Delta', \ldots)^2 = (\Delta^2, \Delta'^2, \ldots).$$

Die Partialdiskriminante $\mathfrak{d}$ ist ein Ideal, welches im Körper $\varkappa$ liegt.

Auch der Dedekindsche Begriff des Grundideals bedarf einer Verallgemeinerung: wir verstehen unter dem *Partialgrundideal* $\mathfrak{G}_\varkappa$ des Körpers K in bezug auf $\varkappa$ das Produkt der folgenden $r-1$ Ideale

$$\begin{aligned}&\mathfrak{E}_2 = (\Omega_1 - s_2\Omega_1, \Omega_2 - s_2\Omega_2, \ldots, \Omega_M - s_2\Omega_M),\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ &\mathfrak{E}_r = (\Omega_1 - s_r\Omega_1, \Omega_2 - s_r\Omega_2, \ldots, \Omega_M - s_r\Omega_M).\end{aligned}$$

[1] Wegen dieser schon mehrmals von mir angewandten Bezeichnungsweise der Ideale vgl. Über die Zerlegung der Ideale eines Zahlkörpers in Primideale. Math. Ann. **44**. (Dieser Band Abh. 3, S. 6.)

[2] Der nämliche Satz folgt auch auf Grund der schönen Untersuchungen, durch welche neuerdings K. Hensel die Kroneckersche Theorie der algebraischen Zahlen in einem wesentlichen Punkte vervollständigt hat. Vgl. J. Math. **113** (1894).

[3] Dieser Begriff der Partialdiskriminante stimmt im wesentlichen mit dem von Kronecker aufgestellten allgemeinen Diskriminantenbegriffe überein, vgl. Grundzüge einer arithmetischen Theorie der algebraischen Größen § 8. J. Math. **92** (1882).

Es gelten die drei allgemeinen Theoreme:

$$\text{I.}\quad \mathfrak{d} = \nu(\mathfrak{G}_\varkappa),$$
$$\text{II.}\quad \mathfrak{G} = \mathfrak{g}\,\mathfrak{G}_\varkappa,$$
$$\text{III.}\quad D = d^r\, n(\mathfrak{d});$$

hierin bedeuten D, d, $\mathfrak{d}$, bezüglich die Diskriminanten der Körper K, $\varkappa$ und die Partialdiskriminante des Körpers K in bezug auf $\varkappa$, ferner $\mathfrak{G}$, $\mathfrak{g}$, $\mathfrak{G}_\varkappa$ bezüglich die Grundideale von K, $\varkappa$ und das Partialgrundideal des Körpers K in bezug auf $\varkappa$; endlich bedeutet $\nu(\mathfrak{G}_\varkappa)$ die Partialnorm von $\mathfrak{G}_\varkappa$ und $n(\mathfrak{d})$ die Norm von $\mathfrak{d}$ für den Körper $\varkappa$. Diese Theoreme geben einen klaren Einblick in den Bau der Diskriminanten. Das Theorem I ist die Erweiterung des Dedekindschen Satzes für den Begriff des Partialgrundideals. Nach Theorem II ist das Verhalten der Grundideale beim Übergange von dem niederen in den höheren Körper von merkwürdiger Einfachheit: man bekommt das Grundideal des höheren Körpers, indem man das Grundideal des niederen Körpers mit dem betreffenden Partialgrundideal multipliziert. Das Theorem III entsteht, wenn man von der Gleichung II die Norm bildet. Daß die Diskriminante eines Körpers durch die Diskriminante eines jeden Unterkörpers teilbar ist, hat bereits Kronecker[1] bewiesen. Das Theorem III gibt die Potenz der letzteren an, welche in der Diskriminante des höheren Körpers aufgeht und deckt auch zugleich die einfache Bedeutung des übrigbleibenden Faktors der Diskriminante des höheren Körpers auf.

Nunmehr folgen mit Hilfe der oben entwickelten Theorie die Sätze:

Das Grundideal des zum Primideal $\mathfrak{P}$ gehörigen Trägheitskörpers ist nicht durch $\mathfrak{P}$ teilbar. Der Trägheitskörper umfaßt sämtliche in K enthaltenen Unterkörper, deren Grundideale nicht durch $\mathfrak{P}$ teilbar sind.

Das Partialgrundideal des Verzweigungskörpers in bezug auf den Trägheitskörper ist durch

$$\mathfrak{P}^{r_t - r_v} = \mathfrak{p}_v^{h-1}$$

und durch keine höhere Potenz von $\mathfrak{P}$ teilbar.

Das Partialgrundideal des einmal überstrichenen Verzweigungskörpers in bezug auf den Verzweigungskörper enthält genau die Potenz

$$\mathfrak{P}^{L(r_{\bar v} - r_v)} = \mathfrak{p}_{\bar v}^{L(p^{\bar r}-1)}.$$

Das Partialgrundideal des zweimal überstrichenen Verzweigungskörpers in bezug auf den einmal überstrichenen Verzweigungskörper enthält genau die Potenz

$$\mathfrak{P}^{\bar L(r_{\bar v} - r_{\bar v})} = \mathfrak{p}_{\bar{\bar v}}^{\bar L(p^{\bar{\bar r}}-1)}$$

usw.

[1] Vgl. Grundzüge einer arithmetischen Theorie der algebraischen Größen § 9. J. Math. 92 (1882).

Das Grundideal $\mathfrak{G}$ des Körpers K enthält das Primideal $\mathfrak{P}$ genau in der

$$r_t - r_v + L(r_v - r_{\bar v}) + \bar L(r_{\bar v} - r_{\bar{\bar v}}) + \cdots$$

ten Potenz.

Da nun K ein Galoisscher Körper ist und mithin das Grundideal $\mathfrak{G}$ mit seinen konjugierten übereinstimmt, so ist die Diskriminante D von K die M-te Potenz von $\mathfrak{G}$; D enthält folglich das Primideal $\mathfrak{P}$ genau Mmal so oft. Hieraus ergibt sich unmittelbar der Satz:

Der Exponent der Potenz, zu welcher die rationale Primzahl p in der Diskriminante D des Körpers K als Faktor vorkommt, ist

$$m_t\{r_t - r_v + L(r_v - r_{\bar v}) + \bar L(r_{\bar v} - r_{\bar{\bar v}}) + \cdots\}.$$

Im Falle, daß keine überstrichenen Verzweigungskörper vorhanden sind, wird $r_v = 1$, $r_{\bar v} = 1, \ldots$ und es folgt dann das von R. Dedekind und K. Hensel bewiesene Resultat, demzufolge der Exponent der in D aufgehenden Potenz von p den Wert $m_t(r_t - 1)$ besitzt.

Da man für die Exponenten $L, \bar L, \ldots$ ohne Schwierigkeit eine obere Grenze findet, so kann hiernach auch der eben bestimmte Exponent der in der Diskriminante D aufgehenden Potenz von p eine gewisse nur vom Grade M des Körpers K abhängige Grenze nicht überschreiten. Dieser Satz ist besonders deshalb von Wichtigkeit, weil er die Möglichkeiten, die sich hinsichtlich der in M aufgehenden Primzahlen p bieten, von vornherein auf eine endliche Anzahl einschränkt. Rechnen wir demnach alle diejenigen Körper vom Grade M, welche hinsichtlich der in M aufgehenden Primzahlen das nämliche Verhalten zeigen, zu einem Typus, so folgt, daß es für einen gegebenen Grad M nur eine endliche Anzahl von möglichen Körpertypen gibt.

Königsberg i. Pr., den 25. Juni 1894.