Zur Theorie der Ideale.

Von

R. Dedekind.

Aus den Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikal. Klasse. 1894. Nr. 4.

Aus den Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen.
Mathematisch-physikalische Klasse. 1894. Nr. 4.

Zur Theorie der Ideale.

Von

R. Dedekind in Braunschweig, ausw. Mitglied.

Vorgelegt am 10. September 1894.

Nachdem es mir in den Jahren 1869 und 1870 endlich gelungen war, durch Einführung neuer Begriffe die letzten Schwierigkeiten zu überwinden, welche sich meinen früheren Versuchen, eine strenge und ausnahmelose Theorie der Ideale zu begründen, entgegengestellt hatten, diente mir die hiermit gewonnene Grundlage in den nächstfolgenden Jahren theils zur Untersuchung specieller, insbesondere der cubischen Körper, theils zur Erforschung der allgemeinen Gesetze, welche die Beziehungen zwischen den Idealen verschiedener Körper beherrschen. Die letztere Frage, welche im Wesentlichen auf die Betrachtung derjenigen Körper zurückkommt, die ich Galois'sche Körper oder Normalkörper genannt habe, bot keine erheblichen Schwierigkeiten dar und konnte daher bald zu einem vollständigen Abschlusse gebracht werden. Von der Veröffentlichung dieser Untersuchung bin ich immer durch andere Beschäftigungen abgezogen, und nur gelegentlich habe ich ihrer Erwähnung gethan, z. B. im § 27 meiner Schrift Sur la théorie des nombres entiers algébriques (1877), wo ich den Satz ausgesprochen habe, daß aus den Idealen eines Normalkörpers die Ideale eines jeden in ihm als Divisor enthaltenen Körpers nach bestimmten Gesetzen abgeleitet werden können, und wo auch an einem sehr einfachen Beispiele die Kraft dieser von mir gefundenen Gesetze dargelegt ist[1]). Dies hat Herrn Frobenius, wie er mir in einem Schreiben vom 3. Juni 1882 aus Zürich mittheilte, zur selbständigen

1) Vergl. auch Compte rendu der Pariser Akademie vom 24. Mai 1880, und die Anmerkung auf S. 618 der vierten Auflage von Dirichlet's Vorlesungen über Zahlentheorie (1894).

Durchforschung des Gegenstandes angeregt, durch welche er, wie sich bald herausstellte, zu einer nahezu vollständigen Uebereinstimmung mit mir gelangt war; da er zugleich wegen einer Nebenfrage eine Mittheilung meiner Resultate wünschte, so verfaßte ich in der Eile eine kurze Uebersicht derselben und fügte sie am 8. Juni meiner Antwort bei. Obgleich nun vor Kurzem Herr Hilbert seine auf denselben Gegenstand bezügliche Untersuchung in diesen Nachrichten (7. Juli 1894) veröffentlicht hat, so erlaube ich mir doch, die eben erwähnte Uebersicht, weil in ihr die Zerlegungen der Ideale noch allgemeiner ausgeführt sind[1]), ohne jeden Zusatz, nur mit Auslassung einiger unwesentlichen Worte jetzt mitzutheilen. —

Einige Sätze aus der Untersuchung der Beziehungen zwischen den Idealen in verschiedenen Körpern.

I. Ideale in Normalkörpern.

Bezeichnungen:

Ω ein Normalkörper vom Grade n.

Φ die Gruppe aller n Permutationen φ, durch welche Ω in sich selbst übergeht. — Bedeutet z irgend ein System von Zahlen des Körpers Ω oder auch eine einzelne solche Zahl, so bezeichne ich durch das Symbol $z\varphi$ das durch die Permutation φ aus z hervorgehende System[2]).

$\mathfrak{o}$ das Gebiet aller ganzen Zahlen ω des Körpers Ω. — Wenn ich in einer Gleichung oder Congruenz den Buchstaben ω benutze, so will ich damit sagen, daß sie für jede in $\mathfrak{o}$ enthaltenen Zahl ω, also gewissermaßen identisch gilt.

$\mathfrak{p}$ ein Primideal des Körpers Ω.

p die durch $\mathfrak{p}$ theilbare positive rationale Primzahl.

---

1) Auch die auf S. 235 von Herrn Hilbert aufgestellten Sätze über Partial-Discriminanten — von welchen die folgende Uebersicht unmittelbar gar nicht handelt — scheinen die Allgemeinheit derjenigen Resultate nicht ganz zu erreichen, zu welchen ich durch die am Schlusse der Einleitung zu meiner Abhandlung Ueber die Discriminanten endlicher Körper (1882) erwähnte Untersuchung gelangt war; auf diese gedenke ich später einzugehen. Dagegen ist mir die von Herrn Hilbert ausgeführte weitere Zerlegung der von ihm mit g_t, von mir mit X bezeichneten Gruppe neu gewesen.

2) Die im Originale benutzte Bezeichnung $z|\varphi$ ersetze ich hier durch die einfachere, welche ich in § 161 der vierten Auflage von Dirichlet's Vorlesungen über Zahlentheorie (1894) eingeführt habe.

X die Gruppe aller derjenigen g Permutationen χ, für welche (identisch)

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}}.$$

Dann giebt es eine Permutation

ψ_0 (oder vielmehr genau g solche Permutationen $\chi\psi_0$), für welche

$$\omega^{p} \equiv \omega\psi_0 \pmod{\mathfrak{p}}.$$

Daraus folgen die Eigenschaften:

$$\psi_0^{-1} X \psi_0 = X, \text{ d. h. } X\psi_0 = \psi_0 X,$$

und der Grad von $\mathfrak{p}$ ist der kleinste positive Exponent

f, für welchen

$$X\psi_0^{f} = X, \text{ d. h. } \psi_0^{f} \text{ in } X \text{ enthalten.}$$

Also

$$N(\mathfrak{p}) = p^{f}.$$

Ferner ist die Gruppe (Bezeichnungsweise von Galois)

$$\Psi = X + X\psi_0 + X\psi_0^2 + \cdots + X\psi_0^{f-1} \text{ (vom Grade } fg)$$

der Inbegriff aller derjenigen Permutationen ψ, welche der Bedingung

$$\mathfrak{p}\psi = \mathfrak{p}$$

genügen (d. h. die Gruppe, zu welcher $\mathfrak{p}$ gehört). Setzt man endlich

$$\Phi = \Psi\varphi_1 + \Psi\varphi_2 + \cdots + \Psi\varphi_e, \text{ also } n = efg,$$

so entspricht jedem dieser e Complexe $\Psi\varphi_s$ ein mit $\mathfrak{p}$ conjugirtes Primideal

$$\mathfrak{p}_s = \mathfrak{p}\varphi_s;$$

diese e Primideale

$$\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_e$$

sind verschieden von einander, und es ist

$$\mathfrak{o}p = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_e)^{g}$$
$$N(\mathfrak{p}_s) = p^{f} \text{ (unabhängig von } s).$$

Wird $\mathfrak{p}$ durch $\mathfrak{p}_s$ ersetzt, so ist X, ψ_0, Ψ zu ersetzen durch $X_s = \varphi_s^{-1} X \varphi_s$, $\psi_{s,0} = \varphi_s^{-1}\psi_0\varphi_s$, $\Psi_s = \varphi_s^{-1}\Psi\varphi_s$. —

II. Ideale in den Divisoren eines Normalkörpers Ω.

Kennt man die (in I. erörterte) Constitution aller Primideale $\mathfrak{p}$ des Normalkörpers Ω, so folgt daraus für jeden in Ω als

Divisor enthaltenen Körper

Ω' durch alleinige Anwendung von Gruppen-Zerlegungen (also gewissermaßen aus rein algebraischen Principien) die vollständige Kenntniß aller Primideale

$\mathfrak{p}'$ in Ω'. Die Bezeichnungen in I. werden beibehalten. Bekannt ist:

Ω' gehört zu einer Permutations-Gruppe

Φ', bestehend aus allen denjenigen m (in Φ enthaltenen) Permutationen φ', die jede in Ω' enthaltene Zahl ungeändert lassen; dann ist

$$n = mn',$$

und n' ist der Grad von Ω' (umgekehrt, wenn Φ' eine in Φ enthaltene Gruppe ist, so giebt es immer einen und nur einen zugehörigen Körper Ω'). Es wird daher das erstrebte Ziel lediglich durch Vergleichung von Φ' mit den in I. betrachteten Permutationen und Gruppen erreicht. Dazu dient zunächst Folgendes, was weniger oder zum Theil gar nicht bekannt scheint.

Bedeutet φ_r eine bestimmte Permutation, so bezeichne ich mit $\Psi\varphi_r\Phi'$ den Complex aller von einander verschiedenen Permutationen von der Form $\psi\varphi_r\varphi'$, wo ψ, φ' resp. alle in den Gruppen Ψ, Φ' enthaltenen Permutationen durchlaufen; ist h_r der Grad des größten gemeinschaftlichen Theilers Ψ'_r der Gruppen $\varphi_r^{-1}\Psi\varphi_r = \Psi_r$ und Φ' (d. h. besteht Ψ'_r aus h_r Permutationen), so werden immer je h_r Producte $\psi\varphi_r\varphi'$ identisch, und das Product aus den Graden der Gruppen Ψ, Φ' (hier fg und m) ist daher das h_r-fache von der Anzahl der in $\Psi\varphi_r\Phi'$ enthaltenen Permutationen. Da ferner zwei solche Complexe $\Psi\varphi_r\Phi'$, $\Psi\varphi_s\Phi'$ entweder ganz identisch sind, oder keine einzige gemeinschaftliche Permutation haben, so kann man setzen:

$$\Phi = \Psi\varphi_1\Phi' + \Psi\varphi_2\Phi' + \cdots + \Psi\varphi_{e'}\Phi'.$$

Dies ist, beiläufig gesagt, die Grundlage für die Untersuchung der algebraischen Reciprocität zwischen zwei beliebigen endlichen Körpern, nämlich denen, welche zu den Gruppen Ψ und Φ' gehören (Einwirkung zweier beliebigen irreducibelen Gleichungen auf einander, Zerlegung jeder in e' Factoren). Zugleich ist

$$\Phi = \Phi'\varphi_1^{-1}\Psi + \cdots + \Phi'\varphi_e^{-1}\Psi.$$

Diese allgemeine Zerlegung einer Gruppe Φ nach zwei

in ihr enthaltenen Gruppen Ψ, Φ' giebt für unseren Fall Alles, was wir wünschen; durch folgende Bestimmungen.

Es sei φ_r eine bestimmte der in der obigen Zerlegung benutzten c' Permutationen $\varphi_1, \varphi_2 \dots \varphi_{c'}$, und

$\mathfrak{p}_r = \mathfrak{p}\varphi_r$,

$\mathfrak{p}'_r$ das durch $\mathfrak{p}_r$ theilbare Primideal in Ω',

g_r der Grad des grössten gemeinsamen Theilers

X'_r von $X_r = \varphi_r^{-1} X \varphi_r$ und Φ', daher

a_r definirt durch $g = a_r g_r$, so ist

$$\mathfrak{o}'\mathfrak{p} = \mathfrak{p}_1'^{a_1}\mathfrak{p}_2'^{a_2}\dots\mathfrak{p}_{c'}'^{a_{c'}}, \text{ wo}$$

$\mathfrak{o}'$ das System aller ganzen Zahlen des Körpers Ω'.

Die Anzahl c' der Complexe $\Psi\varphi_r\Phi'$, aus denen Φ besteht, ist daher zugleich die Anzahl aller von einander verschiedenen, in p aufgehenden Primideale $\mathfrak{p}'_1, \mathfrak{p}'_2 \dots \mathfrak{p}'_{c'}$ des Körpers Ω', und die Zerlegung von p in diesem Körper ist gefunden; die Bestimmung der Normen dieser Primideale $\mathfrak{p}'$ und ihre Zerlegung in Ω folgt jetzt. Es sei, wie oben,

Ψ'_r der größte gemeinsame Theiler der Gruppen

$\Psi_r = \varphi_r^{-1}\Psi\varphi_r$ und Φ',

h_r der Grad von Ψ'_r, folglich

$$\Phi' = \Psi'_r\varphi'_{r,1} + \Psi'_r\varphi'_{r,2} + \dots + \Psi'_r\varphi'_{r,e_r}; \quad m = h_r e_r,$$

$\mathfrak{p}_{r,s} = \mathfrak{p}_r\varphi'_{r,s}$, so ist

$$\mathfrak{o}\mathfrak{p}'_r = (\mathfrak{p}_{r,1}\mathfrak{p}_{r,2}\dots\mathfrak{p}_{r,e_r})^{g_r}$$

$$e_1 + e_2 + \dots + e_{c'} = e.$$

Hiermit ist die Zerlegung erledigt (die letzte Gleichung folgt daraus, daß $e_r fg$ die Anzahl der in $\Psi\varphi_r\Phi'$ enthaltenen Permutationen ist). Endlich: da X'_r auch der größte gemeinsame Theiler von X_r und Ψ'_r ist (weil X_r Divisor von Ψ'_r), so ist h_r theilbar durch g_r, also

f_r definirt durch $h_r = f_r g_r$,

und nach der obigen Regel besteht der Complex $X_r\Psi'_r$ aus $f_r g$ Permutationen, welche alle in Ψ_r enthalten sind (weil X_r und Ψ'_r Divisoren von Ψ_r), und da dieser Complex $X_r\Psi'_r$ zugleich eine Gruppe ist (weil $X_r\psi_r = \psi_r X_r$), so ist fg (als Grad von Ψ_r) theilbar durch $f_r g$ (als Grad von $X_r\Psi'_r$), mithin

f'_r definirt durch $f = f_r f'_r$. Dann ist

$$N'(\mathfrak{p}'_r) = (\mathfrak{o}', \mathfrak{p}'_r) = p^{f'_r}$$

und

$$\mathfrak{N}(\mathfrak{p}_{r,s}) = \mathfrak{p}_r'^{f_r} \text{ (unabhängig von } s),$$

wo $\mathfrak{N}$ das Symbol für die in Bezug auf Ω' genommene Partialnorm von Zahlen oder Idealen des Körpers Ω bedeutet. — Sind Ω, Ω' zwei beliebige endliche Körper, so gehört zu jedem Ideal $\mathfrak{a}$ des Körpers Ω ein bestimmtes Ideal $\mathfrak{a}' = \mathfrak{N}(\mathfrak{a})$ des Körpers Ω', die Partialnorm von $\mathfrak{a}$ nach Ω', und es ist $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$. —

III. Verallgemeinerung.

Dieselben Sätze gelten ohne nennenswerthe Wortänderung, wenn man an Stelle des Körpers k der rationalen Zahlen einen beliebigen endlichen Körper P setzt, und unter Ω einen endlichen Körper versteht, welcher P als einen Divisor enthält und zwar ein Normalkörper in Bezug auf P ist (d. h. daß Ω durch alle diejenigen Permutationen, welche jede Zahl in P ungeändert lassen, in sich selbst übergeht). Für die Zerlegung der Primideale p des Körpers P in Primideale $\mathfrak{p}$ des Körpers Ω gelten genau dieselben Gesetze wie in I. Sind ferner alle diese Zerlegungen bekannt, so erhält man daraus nach den in II. angegebenen Gesetzen sowohl die Zerlegung jedes Primideals p in Primideale $\mathfrak{p}'$ eines Körpers Ω', welcher Multiplum von P und Divisor von Ω ist, als auch die Zerlegung dieser Primideale $\mathfrak{p}'$ in Primideale $\mathfrak{p}$ des Körpers Ω. Und diese Verallgemeinerung kann noch weiter getrieben werden. —

8. Juni 1882.