Über den Dualismus in den Gesetzen der Zahlen-Moduln

Auteurs : Dedekind, Richard

En passant la souris sur une vignette, le titre de l'image apparaît.

12 Fichier(s)

Contributeur·ricesHaffner, Emmylou
ÉditeursEmmylou Haffner (Institut des textes et manuscrits modernes, CNRS-ENS) ; Niedersächsische Staats- und Universitätsbibliothek, Göttingen ; projet EMAN (Thalim, CNRS-ENS-Sorbonne nouvelle).

Présentation

TitreÜber den Dualismus in den Gesetzen der Zahlen-Moduln
Date1877-1879
Sujet

- dualisme
- dualité
- modules
- modules finis
- normes
- théorie des nombres

CoteCod. Ms. Dedekind X 9, p. 3-8
Format6 f., 12 p.
LangueAllemand

Description & Analyse

DescriptionTexte rédigé mais incomplet? sur le "dualisme" dans la théorie des modules de nombres.

(Description à compléter page à page)
NotesRédigé seulement sur les rectos.
Référence à la seconde édition des Vorlesungen de Dirichlet (base datation mais doute possible).
Mode(s) d'écritureTexte rédigé
Auteur·es de la descriptionHaffner, Emmylou

Mots-clefs

dualisme, dualite, modules, modules finis, normes, théorie des nombres
Notice créée par Emmylou Haffner Notice créée le 20/06/2018 Dernière modification le 07/02/2022

Über den Dualismus in den Gesetzen der Zahlen-Moduln.

Von R. Dedekind.

1.

Die folgenden Betrachtungen setzen keine anderen mathematischen Kenntnisse voraus, als die der Addition und Subtraction, und beziehen sich auf den von mir eingeführten Begriff eines Zahlen-Moduls*), dessen Eigenschaften, so weit sie hier von Wichtigkeit sind, zunächst entwickelt werden sollen.

Ein System $\mathfrak{a}$ von irgend welchen Zahlen α soll ein Modul heissen, wenn die Differenzen von je zwei solchen Zahlen α immer demselben System $\mathfrak{a}$ angehören. Hieraus folgt, dass $\mathfrak{a}$ auch die Zahl Null ($= \alpha - \alpha$), also auch alle Zahlen $-\alpha$ ($= 0 - \alpha$) und folglich auch alle Summen von je zwei Zahlen α enthalten muss. nämlich nämlich Sind ferner $\alpha_1, \alpha_2 \ldots \alpha_n$ bestimmte Zahlen des Moduls $\mathfrak{a}$, während $x_1, x_2 \ldots x_n$ willkürlich zu wählende ganze rationale Zahlen ~~so~~ bedeuten, so sind auch alle Zahlen μ von der Form

$$\mu = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

in $\mathfrak{a}$ enthalten; offenbar bilden diese Zahlen μ ebenfalls einen Modul, der zweckmässig durch das Symbol

$$[\alpha_1, \alpha_2 \ldots \alpha_n]$$

*) Dirichlet, Vorlesungen über Zahlentheorie, zweite Auflage, §. 161.

bezeichnet werden kann. So z. B. ist der Modul [1] das System aller ganzen rationalen Zahlen, der Modul [2] besteht aus allen geraden Zahlen. Die in ~~allen~~ jedem Moduln enthaltene Zahl Null bildet für sich allein einen Modul, jeder andere Modul besteht aus unendlich vielen Zahlen.

$\boxed{\mathfrak{a} \text{ [illegible] } \mathfrak{d}\,!}$

Wenn alle Zahlen eines Moduls $\mathfrak{a}$ auch dem Modul $\mathfrak{d}$ angehören, so ~~soll $\mathfrak{a}$ ein Multiplum von $\mathfrak{a}$~~ heißt $\mathfrak{a}$ theilbar durch $\mathfrak{d}$ oder ein Multiplum von $\mathfrak{d}$, und umgekehrt $\mathfrak{d}$ ein Divisor von $\mathfrak{a}$. [So z. B. ist [6] ~~theilbar durch~~ $>$ [2], der Modul Null ist ein Multiplum von jedem Modul $\mathfrak{a}$, und wenn $\alpha_1, \alpha_2 \ldots \alpha_n$ bestimmte Zahlen des Moduls $\mathfrak{a}$ sind, so ist $\mathfrak{a}$ ein Divisor von $[\alpha_1, \alpha_2 \ldots \alpha_n]$.

In Zeichen wollen wir diese Theilbarkeit auch kürzer durch $\mathfrak{a} > \mathfrak{d}$ oder $\mathfrak{d} < \mathfrak{a}$ (1) ausdrücken.

Sind zwei Moduln $\mathfrak{a}$, $\mathfrak{d}$ gegenseitig durch einander theilbar, so sind sie identisch, was wir durch $\mathfrak{a} = \mathfrak{d}$ bezeichnen.

Bedeutet α jede Zahl des Moduls $\mathfrak{a}$, und β jede Zahl des Moduls $\mathfrak{b}$, so bilden alle Zahlen von der Form $\alpha + \beta$ offenbar wieder einen Modul, welchen wir die Summe der Moduln $\mathfrak{a}$, $\mathfrak{b}$ nennen und mit $\mathfrak{a} + \mathfrak{b}$ bezeichnen wollen. Aus dieser Erklärung ergeben sich unmittelbar die für beliebige Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ geltenden Gesetze

$$\mathfrak{a} + \mathfrak{a} = \mathfrak{a} \qquad (2)$$

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a} \qquad (3)$$

$$(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}). \qquad (4)$$

~~Den letzten dieser Moduln kann man daher auch einfach durch a + b + c bezeichnen~~ Da unter den Zahlen $\alpha + \beta$ des Moduls $\mathfrak{a} + \mathfrak{b}$ sich auch alle Zahlen $\alpha + 0$ und $0 + \beta$ befinden, so ist $\mathfrak{a} + \mathfrak{b}$ ein gemeinsamer Divisor von $\mathfrak{a}$, $\mathfrak{b}$, und da, wenn $\mathfrak{d}$ irgend ein gemeinsamer

Divisor von $\mathfrak{a}, \mathfrak{b}$ ist, alle Zahlen α, β und folglich auch alle Zahlen $\alpha+\beta$ in $\mathfrak{d}$ enthalten sind, so ist die Summe $\mathfrak{a}+\mathfrak{b}$ theilbar durch jeden solchen Modul $\mathfrak{d}$ und kann daher zugleich der größte gemeinsame Divisor von $\mathfrak{a}, \mathfrak{b}$ genannt werden. In demselben Sinne bildet der Modul (3), den man auch kurz durch $\mathfrak{a}+\mathfrak{b}+\mathfrak{c}$ bezeichnen kann, die Summe oder den größten gemeinsamen ~~Theiler~~ Divisor der ~~Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$,~~ in beliebiger Ordnung auf einander folgenden Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$. Offenbar läßt sich dieser Begriff auf beliebig viele (sogar unendlich viele) Moduln ausdehnen, und es ist z. B.

$$[\alpha_1, \alpha_2 \ldots \alpha_n] = [\alpha_1] + [\alpha_2] + \cdots + [\alpha_n].$$

Ist ferner $\mathfrak{m}$ theilbar durch $\mathfrak{d}$, so ist

$$\mathfrak{m} + \mathfrak{d} = \mathfrak{d}, \qquad (1')$$ 5

und umgekehrt.

Sind wieder $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, so bildet die Gesammtheit aller derjenigen Zahlen μ, welche, wie z. B. die Zahl Null, beiden ~~Zahlen~~ Moduln $\mathfrak{a}, \mathfrak{b}$ gemeinsam angehören, ebenfalls einen Modul, weil jede Differenz von zwei solchen Zahlen μ sowohl in $\mathfrak{a}$, als auch in $\mathfrak{b}$ enthalten, also wieder eine Zahl μ ist. Diesen Modul wollen wir mit $\mathfrak{a}-\mathfrak{b}$ bezeichnen und, so unpassend es auch erscheinen mag, die Differenz von $\mathfrak{a}, \mathfrak{b}$ nennen. [der Kürze wegen,] Dann gelten offenbar die Gesetze

$$\mathfrak{a} - \mathfrak{a} = \mathfrak{a} \qquad (2')$$

$$\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a} \qquad (3')$$

$$(\mathfrak{a} - \mathfrak{b}) - \mathfrak{c} = \mathfrak{a} - (\mathfrak{b} - \mathfrak{c}). \qquad (4')$$

Es leuchtet ferner ein, daß $\mathfrak{a}-\mathfrak{b}$ sowohl durch $\mathfrak{a}$, als durch $\mathfrak{b}$ theilbar und zugleich Divisor jedes Moduls ist,

der ein gemeinsames Multiplum von a, b ist, weshalb die Differenz a − b auch das ~~kleinste~~ gemeinsame Multiplum von a, b genannt werden kann. In demselben Sinne bildet der Modul (3'), den man auch durch a − b − c bezeichnen kann, die Differenz oder das kleinste gemeinsame Multiplum der in beliebiger Ordnung auf einander folgenden Moduln a, b, c, und es leuchtet ein, wie dieser Begriff auf beliebig viele Moduln auszudehnen ist. Endlich kann die Theilbarkeit (3) oder (1') von m durch d, welche ihren Ausdruck schon in ~~[illegible]~~ gefunden hat, ebenso auch durch

$$m - d = m \qquad (1'')$$

dargestellt werden.

Zur Rechtfertigung der hier für Moduln benutzten Ausdrücke Theilbarkeit, Multiplum, Divisor wollen ~~wir~~ man bemerken, dass, wenn ~~a, b irgend zwei ganze rationale Zahlen und~~ m ~~den~~ das kleinste gemeinsame Multiplum, und d den größten gemeinsamen Divisor der beiden ganzen Zahlen a, b bedeutet, wirklich [m] das kleinste gemeinsame ~~Vielfache~~ Multiplum, und [d] der größte gemeinsame Divisor der beiden Moduln [a], [b] ist, was in unseren Bezeichnungen durch

$$[a] + [b] = [a, b] = [d], \quad [a] - [b] = [m]$$

ausgedrückt wird. Zur Rechtfertigung der Benutzung der Zeichen >, <, + ~~[illegible]~~ und namentlich des Zeichens − für Moduln, sowie der Ausdrücke Summe und Differenz von Moduln kann ich freilich nur den Umstand anführen, dass diese einmal vorhandenen Zeichen und zum Schreiben geläufig sind und bei einiger Aufmerksamkeit gewiss keine Missverständnisse herbeiführen können.

Auch die Producte und Quotienten von Moduln, die für die Theorie der Ideale von großer Wichtigkeit sind, haben wir hier keine Veranlassung einzugehen. Dagegen bedürfen wir folgenden ~~auch des~~ Begriffes ~~der Congruenz der Zahlen~~. Zwei Zahlen α, β heißen congruent in Bezug auf den Modul m, ~~als~~ wenn ihre Differenz $\alpha - \beta$ in m enthalten ist, und wir bezeichnen dies durch die Congruenz $\alpha \equiv \beta \pmod{m}$; ist nun zugleich $\alpha \equiv \gamma \pmod{m}$, ist also auch $\alpha - \gamma$ in m enthalten, so gilt dasselbe von $(\alpha - \gamma) - (\beta - \gamma) = \beta - \gamma$, und folglich ist auch $\beta \equiv \gamma \pmod{m}$. Man kann daher in Bezug auf m alle Zahlen in Zahlclassen eintheilen, indem man je zwei congruente Zahlen in dieselbe, je zwei incongruente Zahlen in verschiedene Zahlclassen aufnimmt; jede ~~bestimmte~~ einer solchen Classe Zahl α ~~kann~~ als Repräsentant angesehen werden, und diese Classe besteht aus allen Zahlen von der Form $\alpha + \mu$, wo μ ~~alle~~ jede Zahl des Moduls m bedeutet. Der Modul m ist selbst eine solche Classe, als deren Repräsentant die Zahl Null angesehen werden kann. 7

Sind nun a, b irgend zwei Moduln, so kann man offenbar aus a immer ein endliches oder unendliches System von Zahlen α' so auswählen, daß jede in a enthaltene Zahl mit einer, aber auch nur mit einer einzigen dieser Zahlen α' congruent ist in Bezug auf den Modul b; ~~ein solches System von~~ diese Zahlen α' ~~heißt~~ bilden ein Repräsentantensystem des Moduls a in Bezug auf b. Ist ihre Anzahl endlich, so soll dieselbe durch das Symbol

$$(a, b)$$

bezeichnet werden; ist aber die Anzahl der Repräsentanten ~~Zahlen~~ α'

unendlich groß, so soll $(\mathfrak{a}, \mathfrak{b}) = 0$ gesetzt werden. Offenbar bilden nun die Zahlen α' auch ein Repräsentanten-System des Moduls $\mathfrak{a}+\mathfrak{b}$ in Bezug auf $\mathfrak{b}$, und folglich ist

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}+\mathfrak{b}, \mathfrak{b}); \qquad (5)$$

aber sie bilden auch ein Repräsentanten-System des Moduls $\mathfrak{a}$ in Bezug auf $\mathfrak{a}-\mathfrak{b}$, und folglich ist

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a}-\mathfrak{b}); \qquad (5')$$

und die Theilbarkeit eines Moduls $\mathfrak{m}$ durch den Modul $\mathfrak{d}$ wird, wie durch ~~(1) oder (1')~~ [(1) oder (1') oder (1''), so auch durch

$$(\mathfrak{m}, \mathfrak{d}) = 1 \qquad (1''')$$

ausgedrückt.

Ist ferner $\mathfrak{a}$ ein Divisor von $\mathfrak{b}$, und $\mathfrak{b}$ ein Divisor von $\mathfrak{c}$, so bilden, wenn ~~die~~ Zahlen α' ein Repräsentanten-System von $\mathfrak{a}$ in Bezug auf $\mathfrak{b}$, und ~~die Zahlen~~ β' ein Repräsentanten-System von $\mathfrak{b}$ in Bezug auf $\mathfrak{c}$ durchlaufen, die Zahlen $\alpha'+\beta'$ ein Repräsentanten-System von $\mathfrak{a}$ in Bezug auf $\mathfrak{c}$, und folglich ist

$$(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}, \mathfrak{b})(\mathfrak{b}, \mathfrak{c}), \qquad (6)$$

$$\text{wenn } \mathfrak{a} < \mathfrak{b} < \mathfrak{c}.$$

Alles Bisherige ist schon an verschiedenen Orten (z. B. in §. 165 der dritten Auflage von Dirichlet's Zahlentheorie) ausführlich von mir dargestellt; im Folgenden ~~beabsichtige ich, theils die Begriffe von einigen Sätzen mitzutheilen, so genau welche ich früher gelegentlich erwähnt und benutzt habe, theils auch einige neue Untersuchungen über gewisse Gruppen von Moduln anzustellen~~ erlaube ich mir, eine noch nicht veröffentlichte Untersuchung über diejenige Gruppe von Moduln mitzutheilen, welche aus drei beliebigen Moduln durch wiederholte Bildung der Summen und Differenzen entsteht.