# Quelques théorèmes sur les Modul-Gruppen.

### 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

TitreQuelques théorèmes sur les Modul-Gruppen.
Date1894-1897
Sujet

- chaînes
- divisibilité
- longueur (Länge)
- modules
- Modulgruppen
- notation2

CoteCod. Ms. Dedekind XI 1, p. 29-34
Format6 f. ; 12 p.
LangueAllemand

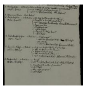
## Description & Analyse

DescriptionDéfinition des opérations entre modules, études des propriétés. Certains résultats se retrouvent dans les Dualgruppen, d'autres en théorie des nombres.
NB seulement des modules.
Mode(s) d'écritureTexte rédigé
Auteur·es de la descriptionHaffner, Emmylou

## Relations

**Collection Cod. Ms. Dedekind X 11-1**

Ce document *utilise la même notation que :*

 [Meilleure présentation pour 3 modules a, b, c](#)

**Collection Cod. Ms. Dedekind X 11-2**

Ce document *est une version préliminaire de :*

[Première rédaction de l'article de 1900](#)

**Collection Cod. Ms. Dedekind XI 1**

[Sur le dualisme dans la théorie des modules](#)

*est à lire avec ce document*

[Afficher la visualisation des relations de la notice](#).

## Mots-clefs

[chaînes](#), [divisibilité](#), [longueur (Länge)](#), [modules](#), [Modulgruppen](#), [notation2](#)

Notice créée par [Emmylou Haffner](#) Notice créée le 25/10/2018 Dernière modification le 21/07/2021

# Einige Sätze über Modul-Gruppen

Zu der (mit L zu schliessenden) zweiten Auflage von Dirichlet's Zahlentheorie (S. 169, Bemerkung auf S. 499) ist auf den folgenden Begriff hinzuweisen:

1. Ein System M von Moduln heisst eine Gruppe, wenn die aus je zwei Moduln a, b des Systems M gebildeten Moduln a+b, a−b demselben System angehören. – Daraus folgt
2. Jeder einzelne Modul a bildet für sich eine Gruppe (a), weil a+a = a−a = a ist.
3. Das System G aller Moduln bildet eine Gruppe.
4. Sind A, B, C ... Modulgruppen, so bildet das System aller derjenigen Moduln, welche allen diesen Gruppen gleichzeitig angehören, eine Gruppe, welche die Gemeinheit von A, B, C ... genannt und mit A − B − C ... bezeichnet werden kann. – Aber diese Gemeinheit braucht nicht zu existiren; sind z. B. a, b verschiedene Moduln, so besitzen die beiden Gruppen (a), (b) keine Gemeinheit. – Vielleicht Einführung eines Symbols für den "leeren" Modul [illegible] System.
5. Ist M irgend ein System von Moduln a, b, c ..., so giebt es Modulgruppen M (z. B. G), in welchen alle diese Moduln enthalten sind; die (stets existirende) Gemeinheit aller dieser Gruppen M bildet (nach 4.) eine Gruppe, die mit (M) = (a, b, c ...) bezeichnet werden kann (vergl. 2.) – das System M kann die Basis der Gruppe (M) heissen.
6. Sind A, B, C ... Gruppen, und bildet M das System aller derjenigen Moduln, welche mindestens einer oder mehreren dieser Gruppen angehören, so kann die Gruppe (M) auch mit (A, B, C ...) bezeichnet werden.

---

Zu verarbeiten in die Abhandlung „Über die [illegible] in der Modultheorie" (besser: „Über Dualgruppen"). – Statt a+b, a−b lieber [illegible], und a∓b statt a+b, a±b statt a−b.

Hier ist nur die specielle (z. Modul-) Art von Dualgruppen behandelt, in welcher der Satz (M) auf S. 499 im S. 169 der Aufl. 4 von Dirichlet's Zahlentheorie gilt.

Sind alle Elemente Moduln der Gruppe D auch in der Gruppe M enthalten, so heisse D ein Theiler von M, und M ein Vielfaches von D.

Grösster gemeinsamer Theiler der Gruppen A, B, C ...

Kleinstes gemeinsames Vielfaches der Gruppen A, B, C.

Das Vorstehende genügt allgemein. Im Folgenden wird nur eine einzige Gruppe $\mathfrak{M}$ betrachtet, und jeder ihrer Moduln wird stets als in $\mathfrak{M}$ enthaltener Modul gedacht.

~~7. Satz (D. S. 499). Bedeuten a, b, ... diejenigen Moduln, welche den Bedingungen~~

~~$a + b < a' < a$, $a - b > b_1 > b$~~

~~genügen, so findet gegenseitig der Moduln $a, b_1$~~

7. Satz (D. S. 499). Sind $a$, $b$ zwei beliebige Moduln, so findet zwischen der Gruppe aller Moduln $a'$, welche den Bedingungen

$$a + b < a' < a \qquad (1)$$

genügen, und der Gruppe aller Moduln $b_1$, welche den Bedingungen

$$a - b > b_1 > b \qquad (2)$$

genügen, eine gegenseitig eindeutige Correspondenz statt, welche durch jede der beiden, wechselseitig aus einander folgenden Beziehungen

$$b_1 = b - a' \qquad (3)$$

$$a' = a + b_1 \qquad (4)$$

ausgedrückt wird.

Beweis. Die Behauptung besteht darin, daß aus (1) und (3) sich (2) und (4) ergiebt, und umgekehrt. Dies folgt aus dem Satze (D. S. 498), daß aus

$$m > d \qquad (5)$$

stets

$$m + (n - d) = (m + n) - d \qquad (6)$$

folgt (und umgekehrt). Ist der Fall, wo (1) und (3) angenommen, so folgt zunächst

$b - b_1 = b$, d. h. $b_1 > b$

$a - b_1 = b - a$, d. h. $a - b > b_1$,

also (2); setzt man ferner

$m = a$, $d = a'$, $n = b$,

wodurch (5) zufolge (1) erfüllt ist, so ergiebt sich nach (6)

$$a + (b - a') = (a + b) - a',$$

was zufolge (1) und (3) und (4) identisch ist. Umgekehrt, wird (2) und (4) angenommen, so folgt

Eingeführte Bezeichnung: Sind $a, b, c \ldots$ irgend welche Moduln der Gruppe $\mathfrak{M}$, so sei mit $\mathfrak{M}_{a,b,c\ldots}$ die Gruppe aller derjenigen in $\mathfrak{M}$ enthaltenen Moduln verstanden, welche den Bedingungen

$$a + b + c + \ldots < m < a - b - c - \ldots$$

genügen. Offenbar ist

$$\mathfrak{M}_{a,b,c\ldots} = \mathfrak{M}_{a+b+c+\ldots,\ a-b-c\ldots}$$

Also: die Bedingungen

$a + b < a' < a$ und $b_1 = b - a'$

sind gleichbedeutend mit den Bedingungen

$a - b > b_1 > b$ und $a' = a + b_1$.

Zugleich ist

$$(a', a) = (b_1, a) = (b_1, a - b)$$

$$(b, b_1) = (b, a') = (a + b, a')$$

$a + a' = a + b_1 = a'$, weil $a > a'$
$b + a' = a + b$ , , $a' > a + b$
entspricht), setzt man ferner
$m = b_1,\ d = b,\ n = a$
wodurch (5) zufolge (4) erfüllt ist, und bedenkt, daß zufolge (2)
$$b_1 + (a - b) = b_1$$
ist, so geht (7) in (8) über. – W. z. b. w.

---

Wir nehmen jetzt an, $M$ sei eine endliche Modulgruppe, d. h. die Anzahl der in $M$ enthaltenen Moduln sei endlich. Diese Anzahl kann vielleicht der Grad von $M$ genannt werden. Wir bezeichnen ferner mit $o$ den größten gemeinsamen Theiler, mit $y$ das kleinste gemeinsame Vielfache aller (in $M$ enthaltenen) Moduln, beide sind ebenfalls in $M$ enthalten, und jeder Modul $m$ (in $M$) genügt den Bedingungen
$$o < m < y.$$
Es soll ferner $m$ ein nächster Theiler von $n$, und $n$ ein nächstes Vielfaches von $m$ heißen (in $M$), wenn
1) $m < n$ ist,
2) $m$, $n$ verschieden sind,
3) $m$ und $n$ die beiden einzigen Moduln (in $M$) sind, die zugleich Theiler von $n$ und Vielfache von $m$ sind.

2) $M$ … besteht aus zwei verschiedenen Moduln $m, n$.
3) { $m$ ein nächster Theiler von $n$, $n$ ein nächstes Vielfaches von $m$ }

Dann gilt Folgendes:
5. Satz: Ist $m$ verschieden von $y$, so giebt es mindestens ein nächstes Vielfaches von $m$; ist $m$ verschieden von $o$, so giebt es mindestens einen nächsten Theiler von $m$.
Beweis: Denn wenn $m$ verschieden von $y$ ist, so ist entweder $y$ selbst ein nächstes Vielfaches von $m$, oder es giebt einen von beiden verschiedenen Modul $y'$, welcher den Bedingungen $m < y' < y$ genügt; und wenn $y'$ kein nächstes Vielfaches von $m$ ist, so giebt es einen von $m$, $y'$ verschiedenen Modul $y''$, welcher den Bedingungen $m < y'' < y'$ genügt, und so kann man fortfahren, endlich muß in der Reihe der abnehmenden Moduln $y, y', y'' \ldots$ ein nächstes Vielfaches von $m$ auftreten, weil die Anzahl aller Moduln in $M$ endlich ist. Ebenso ist der Beweis des zweiten Theils.

9. Satz. Besitzt der Modul m zwei verschiedene nächste Vielfache a, b, so ist

$$a + b = m;$$

und a − b ist ein nächstes Vielfaches sowohl von a, als von b. Besitzt der Modul m zwei verschiedene nächste Theiler a, b, so ist

$$a - b = m;$$

und a + b ist ein nächster Theiler sowohl von a, als von b.

Beweis der ersten Hälfte. Jedenfalls ist m ein gemeinschaftlicher Theiler von a, b, also

$$a > a + b > m,$$
$$b > a + b > m;$$

wäre nun a + b verschieden von m, so müsste, weil a und b nächste Vielfache von m sind, a + b = a = b sein, während doch a, b als verschieden vorausgesetzt sind; also ist wirklich a + b = m. Nun sei $b_1$ irgend ein den Bedingungen

$$a - b > b_1 > b$$

genügender Modul; setzt man dann

$$a' = a + b_1,$$

so ist (nach 7.)

$$a + b < a' < a, \text{ also } m < a' < a$$

und

$$b_1 = b - a'.$$

Da nun a ein nächstes Vielfaches von m ist, so muss a' mit einem der beiden Moduln m, a, und folglich $b_1$ mit einem der beiden Moduln b − m = b, a − b identisch sein; folglich ist a − b ein nächstes Vielfaches von b, und der Symmetrie wegen auch ein nächstes Vielfaches von a. w. z. b. w.

Auch sind a − b verschieden von b (ebenso von a); denn wäre a − b = b, also b > a, so wäre, weil a, m einander verschieden sind, b offenbar kein nächstes Vielfaches von m.

[weil a − b außerdem verschieden von b ist.]

Beweis der zweiten Hälfte (ebenso). Jedenfalls ist m ein gemeinschaftliches Vielfaches von a, b, also

$$a < a - b < m$$
$$b < a - b < m;$$

wäre a − b verschieden von m, so müsste, weil a, b nächste Theiler von m sind, a − b = a = b, während a, b doch verschieden sind; also a − b = m. Nun sei a' irgend ein den Bedingungen

$$a + b < a' < a$$

genügender Modul; setzt man dann

$$b_1 = b - a',$$

so ist (nach 7.)

$$a - b > b_1 > b, \text{ also } m > b_1 > b$$

und

$$a' = a + b_1.$$

Zugleich ist a + b verschieden von a (ebenso von b); denn wäre a + b = a, also b < a < m, so wäre, weil a, b, m alle verschieden sind, b kein nächster Theiler von m.

4. 10. 87.

Da nun b ein nächster Theiler von m ist, so muss $b_1$ mit einem der beiden Moduln $m = a - b$, $b$, welcher $a'$ mit einem der beiden Moduln $a_1$, $a+b$ übereinstimmen, und die letzteren verschieden sind, so ist der eine $a+b$ ein nächster Theiler von $a_1$, und der Symmetrie wegen auch von b. W. z. b. w.

Nun bilde man, von 0 beginnend, eine Kette von Moduln

$0, a, a_1, a_2 \ldots,$

indem jeder ~~[illegible]~~ ein nächster Theiler des folgenden ist; da kein späteres Glied dieser Kette mit einem früheren übereinstimmen kann, und es überhaupt nur eine endliche Anzahl von Moduln in M giebt, so muss diese Kette nothwendig endlich sein und mit einem Gliede schliessen, welches $= g$ ist, weil sonst (nach 8.) die Kette noch fortgesetzt werden könnte. Eine solche Reihe von Moduln soll eine vollständige Kette der endlichen Gruppe M heissen. Dann gilt Folgendes:

11. Satz. Alle vollständigen Ketten einer endlichen Gruppe bestehen aus gleich vielen Gliedern (von nicht gleichem Grade); diese stets gleiche Anzahl soll die Länge der Gruppe heissen (Aufsteigzahl).

Beweis. Ist m irgend eine natürliche Zahl $> 1$, so nehmen wir an, der Satz sei schon für alle Modulgruppen bewiesen, deren Grad $< m$ ist, und zeigen, dass er dann auch für jede Gruppe M ~~vom~~ vom Grade m gilt (die Richtigkeit des Satzes für Gruppen ersten, zweiten, dritten Grades leuchtet unmittelbar ein). Sind nun

$0, m, a_1, a_2 \ldots g$

$0, b, b_1, b_2 \ldots g$

irgend zwei vollständige Ketten der Gruppe M vom Grade m, so ~~seien zwei solche denkbar. Ist zunächst $a = b$, so betrachte man die Gruppe $M_1$ aller Moduln m, für M, welche den Bedingungen $a < m < g$ genügen. Da a nicht in M enthalten ist, so ist der Grad von $M_1$ [illegible], alle anderen [illegible] Glieder der beiden Ketten sind nur Moduln der Gruppe $M_1$, und da $M_1$ aus [illegible] Moduln besteht, die in M enthalten sind, so ist in jeder der beiden Ketten~~

~~$a, a_1, a_2 \ldots g$~~

~~$b, b_1, b_2 \ldots g$~~

Länge einer endlichen Gruppe M zu bezeichnen mit $\ell M$

Besser vorauszuschicken:

10. Satz. Bilden die Moduln ~~[illegible]~~

$a, a_1, a_2 \ldots g$

eine vollständige Kette der Gruppe M, so bilden die Moduln

$a, a_1, \ldots g$

eine vollständige Kette der Gruppe A aller derjenigen in M enthaltenen Moduln m, welche den Bedingungen

$a < m < g$

genügen.

Beweis. A ist eine Gruppe, a ist der grösste gemeinsame Divisor, g das ~~[illegible]~~ kleinste gemeinsame Vielfache aller in A enthaltenen Moduln, und $a_1$ ist ein nächster Theiler von $a$ in dieser Gruppe A, [illegible]. Daraus folgt leicht.

[Somit hat jede solche Gruppe nur eine einzige vollständige Kette besitzt]

Entsprechen nun die Gruppen A, B allen in M enthaltenen Moduln m, n, welche resp. den Bedingungen $a < m < g$, $b < n < g$ genügen. Nun gilt, wenn gegen Satz [illegible] (falls zunächst) $a = b$, so ist auch $A = B$, und da (nach 10.) sowohl

$a, a_1, a_2 \ldots g$

als

$b, b_1, b_2 \ldots g$

vollständige Ketten dieser Gruppe A sind, deren Grad $< m$ ist, so bestehen sie aus gleich vielen Gliedern, und folglich gilt dasselbe von den beiden mit 0 beginnenden vollständigen Ketten der Gruppe M, w. z. b. w. (die Länge der Gruppe M ist = 1 + die Länge der Gruppe A) [illegible]

~~[illegible] auf die Gruppe $M_1$) ein nächster Teiler des folgenden, so sind diese vollständige Ketten der endlichen Gruppe $M_1$, deren Länge $= n$ ist, und die [illegible] mit einem gleichen Gliede $m$ [illegible] auf die beiden [illegible] Ketten [illegible] gleich vielen Gliedern [illegible], und [illegible] für diesen Fall der Satz bewiesen (die Länge von $M$ ist $n+1$ = der Länge von $M_1$).~~

Sind also gegeben die Moduln $a$, $b$, welche auf die Gruppen $A$, $B$ [illegible], so ist (zufolge 8.) der Modul $a - b = c$ ein nächster Teiler zugleich von $a$ und von $b$, also auch in $A$ und in $B$ enthalten. Bezeichnet man nun die Gruppe $C$ aller Moduln $x$, welche den Bedingungen $c < x < y$ genügen, und ist

$c, c_1, c_2, \ldots y$

eine vollständige Kette dieser Gruppe, so ist (Beweis der Umkehrung des Satzes 10.)

$a, c, c_1, \ldots y$

eine vollständige Kette von $A$, ebenso

$b, c, c_1, \ldots y$

eine vollständige Kette von $B$; ist daher $n$ die Länge von $C$, so ist (da die Glieder von $A$ und $B$ kleiner als $m$ sind) $n+2$ die Gliederanzahl der obigen Ketten

$a, a_1, a_2, \ldots y$

$b, b_1, b_2, \ldots y$

und folglich $n+3$ die gemeinschaftliche Gliederzahl der beiden ursprünglichen Ketten

$m, a, a_1, \ldots y$

$m, b, b_1, \ldots y$,

was z. b. w.

---

Hierauf beruht die folgende Anordnung aller Moduln einer endlichen Gruppe $M$ auf Stufen, deren Anzahl um 1 größer ist als die Länge von $M$. Nachdem man eine beliebige ganze rationale Zahl $\sigma$ (z. B. Null) gewählt hat, soll unter der Stufenzahl $s(m)$ des Moduls $m$ die Zahl $\sigma + l$ verstanden werden, wo $l$ die Länge der Gruppe $M_{v,m}$ bedeutet. Dann gilt der Satz.

12. Satz. Sind $a$, $b$ beliebige Moduln der Gruppe $M$, so ist

$$s(a) + s(b) = s(a+b) + s(a-b)$$

Beweis beruht auf Satz 7. Bilden die drei Moduln

~~[illegible]~~

~~[illegible]~~

[illegible]

~~[illegible] vollständige Kette [illegible]~~

NB! schon bei Satz 10. hinzuzufügen!

Umkehrung zum Satz 10.

Ist $c$ ein nächster Teiler von $v$, und bilden die Moduln

$c, a_1, a_2, \ldots y$

eine vollständige Kette der Gruppe $C$ aller derjenigen Moduln $m$ in $M$, welche den Bedingungen $c < m < y$ genügen, so bilden die Moduln

$v, c, a_1, a_2, \ldots y$

eine vollständige Kette der Gruppe $M$.

Allgemeiner: Ist $m$ irgend ein Modul der Gruppe $M$, sind ferner $A$, $B$ die Gruppen derjenigen Moduln $a$, $b$ in $M$, welche den Bedingungen $v < a < m$, $m < b < y$ genügen, und bilden die Moduln

$v, a_1, a_2, \ldots m$ eine vollst. Kette von $A$

$m, b_1, b_2, \ldots y$ " " " $B$

so bilden die Moduln

$v, a_1, a_2, \ldots m, b_1, b_2, \ldots y$

eine vollst. Kette von $M$.

Die Länge von $M$ = Länge von $A$ + Länge von $B$.

$$lM = lM_{v,m} + lM_{m,y}$$

$$\left\{ \begin{aligned} lM_{a,c} &= lM_{a+b,a} + lM_{a,a-b} \\ &= lM_{a+b,b} + lM_{b,a-b} \end{aligned} \right.$$

$s(m) = \sigma + lM_{v,m}$ ; $s(v) = \sigma$

12. Satz: $lM_{a+b,a} = lM_{b,a-b}$

$a'_n < a+b,\ a'_{n-1} \dots a'_1,\ a'_0 = a$
eine zusammenhängende Kette der Gruppe $\mathfrak{M}_{a+b,a}$,
und setzt man

$$b_1^{(r)} = b - a'_r$$

so bilden die $n+1$ Moduln

$$b_1^{(n)} = b,\ b_1^{(n-1)} \dots b_1',\ b_1^{(0)} = a-b$$

eine zusammenhängende Kette der Gruppe $\mathfrak{M}_{b,a-b}$,
und folglich ist

$$L\mathfrak{M}_{a+b,a} = L\mathfrak{M}_{b,a-b},$$

d.h.

$$L(a) - L(a+b) = L(a-b) - L(-b),$$

w.z.b.w. — Da nämlich

$$a'_{r+1} \succ a'_r, \quad \text{also } a'_{r+1} - a'_r = a'_r,$$

so folgt

$$b_1^{(r)} - b_1^{(r+1)} = (b-a'_r) - (b-a'_{r+1}) = b - a'_r = b_1^{(r)}$$

d.h.

$$b_1^{(r+1)} < b_1^{(r)}.$$

Da ferner (nach Satz ?)

$$a'_r = a + b_1^{(r)}$$

ist, so sind $b_1^{(r)}$ und $b_1^{(r+1)}$ verschieden, weil sonst auch $a'_r = a'_{r+1}$ wäre. Genügt ferner ein Modul $b'$ den Bedingungen

$$b_1^{(r+1)} < b_1 < b_1^{(r)},$$

so setze man

$$a' = a + b_1,$$

weil (wegen $b < b_1 < a-b$)

$$b_1 = b - a' \quad (\text{also } a+b < a' < a)$$

ferner

$$a'_r + a' = (a+b_1^{(r)}) + (a+b_1) = a + b_1 = a'$$

$$a'_{r+1} + a' = (a+b_1^{(r+1)}) + (a+b_1) = a + b_1^{(r+1)} = a'_{r+1}$$

also

$$a'_{r+1} < a' < a'_r;$$

müsste also $a'$ mit einem der beiden Moduln $a'_r$, $a'_{r+1}$, folglich auch $b_1$ ($= b - a'$) mit einem der beiden Moduln

$$b - a'_r = b_1^{(r)}, \quad b - a'_{r+1} = b_1^{(r+1)}$$

übereinstimmen, d.h. $b_1^{(r)}$ ist ein nächster Theiler von $b_1^{(r+1)}$, w.z.b.w.