Théorie des modules (peut-être : Théorèmes généraux sur les modules, ordres et congruences)

Auteurs : Dedekind, Richard

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

16 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

TitreThéorie des modules (peut-être : Théorèmes généraux sur les modules, ordres et congruences)
Date1876 ca.
Sujet

- congruences
- divisibilité
- modules
- nombres de classes
- notation v
- ordnung
- théorie des nombres

CoteCod. Ms. Dedekind XI 1, 36-43
Format8 f. ; 16 p.
LangueAllemand

Description & Analyse

DescriptionTexte rédigé sur la théorie des modules. Titre alternatif : "Théorèmes généraux sur les modules, ordres et congruences". Définition des opérations et étude de diverses propriétés. Un des premiers écrits sur le sujet.
Mode(s) d'écritureTexte rédigé
Auteur·es de la descriptionHaffner, Emmylou

Relations

Collection Cod. Ms. Dedekind XI 1

Ce document est à lire avec :

Dualité dans la théorie des modules entre ppcm et pgcd.

Ce document utilise la même notation que :

Dualité dans la théorie des modules entre ppcm et pgcd.

Afficher la visualisation des relations de la notice.

Mots-clefs

congruences, divisibilité, modules, nombres de classes, notation v, ordnung, théorie des nombres

Notice créée par Emmylou Haffner Notice créée le 26/10/2018 Dernière modification le 17/09/2020

Titel vielleicht: Allgemeine Sätze über Moduln, Ordnungen und Congruenzen.

Theorie der Moduln.

1.

Definition eines Moduls (D. § 161, 1).

2.

Definition eines Vielfachen und eines Theilers (D. § 161, 2.)

3.

Definition des ~~kleinsten~~ größten gemeinschaftlichen Theilers $a+b$ zweier Moduln a und b, $a+b = b+a$.

Satz. Jeder gemeinschaftliche Theiler von a, b ist ein Theiler von $a+b$.

4.

Die Theilbarkeit von a durch d wird ausgedrückt durch $a+d = d$.

5.

Folgt $a+a = a$.

6.

Also folgt $(a+b)+c = a+(b+c)$. Hierauf (auf D. § 161) Definition des größten gemeinschaftlichen Theilers mehrerer Moduln $a, b, c, d \ldots$ in beliebiger Anzahl.

7.

Auch für eine unzählbare Anzahl von Moduln ergiebt sich ein gültig bestimmter größter gemeinschaftlicher Theiler, System aller derjenigen Zahlen, deren jede eine Summe einer endlichen Anzahl von Zahlen, deren jede in einem der gegebenen Moduln enthalten ist.

8.

Definition des kleinsten gemeinschaftlichen Vielfachen $a \vee b = b \vee a$ zweier Moduln a, b.

Satz. Jedes gemeinschaftliche Vielfache von a, b ist ein Vielfaches von $a \vee b$.

9.

Es ist $a+(a \vee b) = a$, und aus

$$\left\{\begin{matrix} c+a = a \\ c+b = b \end{matrix}\right\}$$

folgt $c+(a \vee b) = a \vee b$

und umgekehrt.

Die Theilbarkeit von a durch d, d. h. a Vielfaches von d, d Theiler von a vielleicht anzudeuten durch

$a < d$, $d > a$

oder vielleicht gerade umgekehrt durch

$a > d$, $d < a$.

$a > d$, $d < a$

Aus
$$\left\{\begin{matrix} a > a' \\ b > b' \end{matrix}\right\}$$
folgt
$$a+b > a'+b'$$

Bezeichnungen:

$a > d$, $d < a$ heißt a theilbar durch d

$a+b$ heisst gr. g. Th. von a, b

$a \vee b$ " kl. g. V. " a, b

Die Theilbarkeit von a durch d wird ausgedrückt durch $a \vee d = a$.

Folgt $a \vee a = a$

Folgt $(a+b) \vee a = a$

Aus
$$\left\{\begin{matrix} c > a \\ c > b \end{matrix}\right\}$$
folgt
$$c > a \vee b$$
und umgekehrt.

10.

Es ist $(a \vee b) \vee c = a \vee (b \vee c)$. Hieraus (nach 2. u. 2) Definition des kleinsten gemeinschaftlichen Vielfachen mehrerer Moduln $a, b, c \ldots$ (in gegebener Anzahl).

11.

Auch für eine unzählbare Anzahl von Moduln ergiebt sich ein völlig bestimmtes kleinstes gemeinschaftliches Vielfache, System aller der Zahlen, deren jede in jedem der gegebenen Moduln enthalten ist.

12.

Ist a theilbar durch b, b durch c, so ist a theilbar durch c; in Zeichen: aus

$$a + b = b\,,\quad b + c = c$$

folgt durch Addition von c zu der ersten Gleichung

$$(a+b) + c = b + c$$

also

$$a + (b+c) = b + c$$

also

$$a + c = c.$$

[illegible].

Aus $a > b$, $b > c$ folgt $a > c$, zusammengefaßt in

$$a > b > c$$

13.

Satz über drei beliebige Moduln a, b, c:

$$(c+a) \vee (a+b) = a + (b \vee (a+c))$$
$$= a + (c \vee (a+b))$$

Jede in $(c+a) \vee (a+b)$ enthaltene Zahl [illegible] ist

$$\nu = x + \gamma = x_1 + \beta\,,$$

wo x, x_1 in a, β in b, γ in c enthalten; hieraus folgt, daß

$$\beta = (x - x_1) + \gamma$$

in $b \vee (a+c)$, folglich $\nu = x_1 + \beta$ in $a + (b \vee (a+c))$ enthalten ist, d. h. $(c+a) \vee (a+b)$ theilbar durch $a + (b \vee (a+c))$. Umgekehrt jede in $a + (b \vee (a+c))$ enthaltene Zahl ν ist

$$\nu = x + \lambda\,,$$

wo x in a, und

$$\lambda = \beta = x_1 + \gamma\,,$$

wo β in b, x_1 in a, γ in c enthalten;

13. b.

Ist $a + b$ schon erkannt, so ist dieser Satz [illegible] für den Fall [illegible]

$$a + b = b + a$$
$$(a+b) + b = b$$

[illegible], wenn a ein gem. Vielfaches von b, c, also

$$a + b = b\,,\quad a + c = c$$

ist, so folgt aus diesem Satze

$$c \vee b = a + (b \vee c)$$

d. h. a ist theilbar durch $(b \vee c)$.

Durch Vertauschung von b, c ergiebt sich die erste der drei folgenden Gleichungen

$$(a, b \vee c) = (a, b)(a \vee b, c) = (a, c)(c \vee a, b)$$
$$(b, c \vee a) = (b, c)(b \vee c, a) = (b, a)(a \vee b, c)$$
$$(c, a \vee b) = (c, a)(c \vee a, b) = (c, b)(b \vee c, a)$$

Ist nun speciell a ein Theiler von b, und b ein Theiler von c, also

$$(b, a) = 1, \quad (c, b) = 1,$$

so folgt

$$(a, c) = (a, b)(b, c).$$

Da nun aber, wenn a, b, c irgendwelche Moduln angenommen werden, gewiss

$a + c$ ein Theiler von $(a \vee b) + c$

$(a \vee b) + c$ ein Theiler von c

welches ist

$$(a + c, c) = (a + c, (a \vee b) + c)((a \vee b) + c, c)$$

und da ferner (zufolge II.)

$$(a, c) = (a + c, c)$$
$$(a, (a \vee b) + c) = (a + (a \vee b) + c, (a \vee b) + c) = (a + c, (a \vee b) + c)$$
$$(a \vee b, c) = ((a \vee b) + c, c)$$

ist, so folgt allgemein

$$(a, c) = (a, (a \vee b) + c)(a \vee b, c)$$
$$(b, a) = (b, (b \vee c) + a)(b \vee c, a)$$
$$(c, b) = (c, (c \vee a) + b)(c \vee a, b)$$

und

$$(a, b) = (a, (c \vee a) + b)(c \vee a, b)$$
$$(b, c) = (b, (a \vee b) + c)(a \vee b, c)$$
$$(c, a) = (c, (b \vee c) + a)(b \vee c, a)$$

Setzt man dies in die ursprünglichen Gleichungen ein, so gehen sie über in

$$(a, b \vee c) = (a, (c \vee a) + b)(c \vee a, b)(a \vee b, c)$$
$$= (a, (a \vee b) + c)(c \vee a, b)(a \vee b, c)$$

oder wenn man

$$b \vee c = a_1, \quad c \vee a = b_1, \quad a \vee b = c_1 \qquad (1)$$

setzt, in

$$(a, a_1) = (a, b_1 + b)(b_1, b)(c_1, c)$$
$$= (a, c_1 + c)(b_1, b)(c_1, c)$$

Da der Theil ist nun (zufolge II.a)

$$a \vee (b_1 + b) = a \vee (c_1 + c) = b_1 + c_1 \qquad (2)$$

Weil nun (zufolge II.)

$$\left.\begin{aligned}(a, b_1 + b) = (a, c_1 + c) = (a, b_1 + c_1)\\ (b, c_1 + c) = (b, a_1 + a) = (b, c_1 + a_1)\\ (c, a_1 + a) = (c, b_1 + b) = (c, a_1 + b_1)\end{aligned}\right\} \quad (3)$$

also, wenn alles symmetrisch dargestellt wird,

Aus den drei einfachen Sätzen

(I) $(a, b) = (a + b, b)$

(II) $(a, b) = (a, a \vee b)$

(III) $(a, c) = (a, b)(b, c)$, wenn b Vielfaches von a und Theiler von c

folgen die zusammengesetzteren Sätze über drei beliebige Moduln a, b, c in folgender Weise.

Da $a \vee b$ Vielfaches von a und Theiler von $a \vee b \vee c$ ist, so ist nach (III)

$$(a, a \vee b \vee c) = (a, a \vee b)(a \vee b, a \vee b \vee c);$$

nun ist aber nach (II)

$$(a, a \vee b \vee c) = (a, b \vee c)$$
$$(a, a \vee b) = (a, b)$$
$$(a \vee b, a \vee b \vee c) = (a \vee b, c)$$

folglich

(IV) $(a, b \vee c) = (a, b)(a \vee b, c)$

Ebenso ergiebt sich, weil $a + b$ Vielfaches von $a + b + c$ und Theiler von a ist, nach (III)

$$(a + b + c, a) = (a + b + c, a + b)(a + b, a);$$

nun ist aber nach (I)

$$(a + b + c, a) = (b + c, a)$$
$$(a + b + c, a + b) = (c, a + b)$$
$$(a + b, a) = (b, a)$$

folglich

(V) $(b + c, a) = (c, a + b)(b, a)$

der zu (IV) correlative Satz.

Da ist ferner $(c \vee a) + b$ Vielfaches von $a + b$ und Theiler von b, folglich nach (III):

$$(a + b, b) = (a + b, (c \vee a) + b)((c \vee a) + b, b),$$

nun ist aber nach (I)

$$(a + b, b) = (a, b)$$
$$(a + b, (c \vee a) + b) = (a + b + (c \vee a), (c \vee a) + b)$$
$$= (a, (c \vee a) + b)$$

und nach

$$((c \vee a) + b, b) = (c \vee a, b)$$

folglich

(VI) $(a, b) = (a, (c \vee a) + b)(c \vee a, b).$

Ebenso ergiebt sich der correlative Satz; weil $(c + a) \vee b$ Vielfaches von b und Theiler von $a \vee b$, (bezogen auf a', b', c') folglich nach (III):

$$(b, a \vee b) = (b, (c + a) \vee b)((c + a) \vee b, a \vee b),$$

nun ist aber nach (II)

$$(b, a \vee b) = (b, a)$$
$$(b, (c + a) \vee b) = (b, c + a)$$
$$((c + a) \vee b, a \vee b) = ((c + a) \vee b, (c + a) \vee b \vee a)$$
$$= ((c + a) \vee b, a)$$

folglich

(VII) $(b, a) = (b, c + a)((c + a) \vee b, a)$

Schreibt man die Sätze (IV), (V), (VI), (VII) in folgender Form (durch Permutation):

$(b, c) = (b, c_1 + a_1)(c_1, c)$
$(c, a) = (c, a_1 + b_1)(a_1, a)$
$(a, b) = (a, b_1 + c_1)(b_1, b)$
und
$(c, b) = (c, a_1 + b_1)(b_1, b)$
$(a, c) = (a, b_1 + c_1)(c_1, c)$
$(b, a) = (b, c_1 + a_1)(a_1, a)$
und
$(a, a_1) = (a, b_1 + c_1)(b_1, b)(c_1, c)$
$(b, b_1) = (b, c_1 + a_1)(c_1, c)(a_1, a)$
$(c, c_1) = (c, a_1 + b_1)(a_1, a)(b_1, b)$
Endlich
$(b, c)(c, a)(a, b) = (c, b)(a, c)(b, a)$

22.

Alle Zahlen eines Moduls a werden durch Multiplication mit (a, b) in Zahlen des Moduls b verwandelt.

Ist nämlich (a, b) = m von Null verschieden, und stellen die Zahlen $x_1, x_2, \ldots x_m$ die incongruenten Zahlen (mod. b) vor, so sind, wenn α irgend eine in a enthaltene Zahl bedeutet, auch die Zahlen

$\alpha + x_1, \alpha + x_2, \ldots \alpha + x_m$ (mod. b)

incongruent und gleichfalls in a enthalten, folglich den Zahlen $x_1, x_2, \ldots x_m$ congruent, wenn auch in anderer Folge; durch Addition folgt

$m\alpha + \Sigma x_r \equiv \Sigma x_r$ (mod. b),

also

$m\alpha \equiv 0$ (mod. b)

w. z. b. w.

NB. Der Satz ist selbstverständlich, wenn (a, b) = 0 ist.

23.

Definition. Zwei Moduln a, b heißen verwandt, wenn (a, b) und (b, a) von Null verschieden sind.

24.

Sind zwei Moduln b, c mit einem dritten a verwandt, so sind sie auch mit einander verwandt.

Denn wenn (a, b), (b, a), (a, c), (c, a) von Null verschieden, so sind (zufolge 21.) auch

$(a, b_1 + c_1)$ und (b_1, b)
$(b, c_1 + a_1)$ " (a_1, a)
" " (c_1, c)
$(c, a_1 + b_1)$ " "

also auch (b, c) und (c, b) von Null verschieden.

(4) $(a, b - c) = (a, c)(a - c, b)$
(7) $(a, b) = (a, b + c)((b + c) - a, b)$
(8) $(a + c, b) = (a, b + c)(c, b)$
(6) $(a, b) = (a, (c - a) + b)(c - a, b)$

Hieraus erkennt man, daß folgt
(7) aus (6), wenn c durch b + c
(4) " (7), " b " b − c (mit Rücksicht auf 2)
(6) " (8), " c " c − a
(8) " (6), " a " a + c (mit Rücksicht auf 1)
(8) " (4), " { a " a + c ; c " b + c } (mit Rücksicht auf 1)
(4) " (8), " { b " b − c ; c " a − c }

(a, b) a > a − b

25.

Definition: Sind a, b zwei beliebige Moduln, so bilden alle Producte $\alpha\beta$ aus einer Zahl α in a und einer Zahl β in b, und alle Summen solcher Producte einen Modul, der das Product aus a und b heißen und mit ab bezeichnet werden soll. (Keine Verwechselung mit Theiler ...!)

26.

Sätze: ab = ba, (ab)c = a(bc). Folglich Verallgemeinerung (auch für eine größere Anzahl von Factoren a, b, c, d ..., z. B. 2.). Potenzen mit ganzen positiven Exponenten.

Bedeutet $\mathfrak{z}$ den aus allen ganzen rationalen Zahlen bestehenden Modul, so ist $\mathfrak{a}\mathfrak{z} = \mathfrak{a}$.

27.

Definition: Ist a ein Modul, η irgend eine Zahl, so bilden die Producte $\alpha\eta$, wo α alle Zahlen in a durchläuft, einen Modul, der mit $a\eta = \eta a$ bezeichnet werden soll. Derselbe ist in Wahrheit das Product aus a und aus dem Modul, welcher aus allen Zahlen $k\eta$ besteht, wo k alle ganzen rationalen Zahlen durchläuft. Natürlich ist

$(a\eta)\eta' = a(\eta\eta') = (a\eta')\eta$

$(a\eta)b = a(b\eta) = (ab)\eta$

u.s.w.

$\eta\mathfrak{z} = \mathfrak{z}(\eta)$

$a(\eta \pm \eta') > a\eta + a\eta'$

28.

Satz: Es ist $(a+b)c = ac + bc$

Beweis: Jede in $(a+b)c$ enthaltene Zahl ist von der Form

$\Sigma(\alpha+\beta)\gamma = \Sigma\alpha\gamma + \Sigma\beta\gamma$

und folglich in $(ac+bc)$ enthalten; umgekehrt ist jede in $(ac+bc)$ enthaltene Zahl von der Form

$\Sigma\alpha\gamma + \Sigma\beta\gamma'$

und ist, weil jedes einzelne Product $\alpha\gamma$ oder $\beta\gamma'$ in $(a+b)c$ enthalten, weil α und β in $(a+b)$ enthalten sind. W.z.b.w.

29.

Folgerung: Ist a theilbar durch b, so ist ac theilbar durch bc; denn weil $a+b = b$, so wird

$(a+b)c = ac + bc = bc$

d.h. ac theilbar durch bc (Gleichung?).

29.

Ist $a > d$, so ist

$ab > ad$.

Ist $a > a'$,

$b > b'$,

so ist $ab > a'b'$,

denn es ist $ab > a'b > a'b'$.

30.

Satz: Das Product aus dem kleinsten gemeinschaftlichen $a \vee b$ zweier Moduln a, b und aus einem Modul r ist theilbar durch das kleinste gem. Vielfache $(ar) \vee (br)$ der Producte ar und br, d. h.

$$(a \vee b)r + ((ar) \vee (br)) = (ar) \vee (br)$$

Beweis. Jede in $(a \vee b)r$ enthaltene Zahl ist von der Form $\Sigma \mu \rho$, wo jedes μ [illegible] [illegible] [illegible] [illegible] $\Sigma \alpha \rho$ [illegible] [illegible] $\Sigma \beta \rho$, also in ar und in br, mithin in $(ar) \vee (br)$ enthalten. W. z. b. w.

Beweis $a \vee b > a$

$a \vee b > b$

folglich

$(a \vee b) r > ar$

$(a \vee b) r > br$

folglich

$(a \vee b) r > (ar) \vee (br)$

31.

Satz und Definition: Sind a, b zwei beliebige Moduln, so bilden alle Zahlen η, für welche $a\eta$ durch b theilbar wird, einen Modul, welcher der Quotient der Moduln b, a heißen und mit $\frac{b}{a} = b : a$ bezeichnet werden soll. — Ist nämlich $a\eta$ und $a\eta'$ theilbar durch b, so ist auch $a(\eta \pm \eta')$ theilbar durch b (und [illegible] ist $a \cdot r$ theilbar durch b).

Oder auch: $\frac{b}{a}$ das gr. gem. Theiler aller Moduln r, welche (nach 30 [illegible]) der Bedingung $ar > b$ genügen. ([illegible] Definition 3. und Satz 18. gelten auch für Systeme [illegible] [illegible] [illegible] Moduln.)

$$\frac{b}{3} = b$$

32.

Satz: [illegible] Es ist $a(b : a)$ theilbar durch b, d. h.

$$a\left(\frac{b}{a}\right) + b = b$$

Beweis. Durchläuft η den Modul $\frac{b}{a}$, α den Modul a, so ist [illegible] $\alpha\eta$ stets, also auch $\Sigma \alpha\eta$ in b enthalten. W. z. b. w.

Und es ist b theilbar durch $\frac{ab}{a}$, d. h.

$$b + \frac{ab}{a} = \frac{ab}{a}$$

In der Theilbarkeit geschrieben

$$a\left(\frac{b}{a}\right) > b$$

$b > \frac{ab}{a}$ ([illegible] [illegible] $b > b\left(\frac{a}{a}\right) > \frac{ab}{a}$)

33.

Satz: Ist ar theilbar durch b, so ist r theilbar durch $\frac{b}{a}$; d. h. aus

$ar + b = b$

folgt

$r + \frac{b}{a} = \frac{b}{a}$ } und umgekehrt!

Aus $ar > b$ folgt

$r > \frac{b}{a}$

und umgekehrt.

Ist nämlich ρ in r enthalten, so ist $a\rho$ theilbar durch ar, also auch durch b, mithin ρ in $\frac{b}{a}$ enthalten.

Satz. $a \frac{ab}{a} = ab$ (wenn $b > \frac{ab}{a}$)

[illegible] [illegible] $u > v$ [illegible] $u + v > u + v$ [illegible]

34.

Satz: [illegible] $\frac{a}{r} + \frac{b}{r}$ theilbar durch $\frac{a+b}{r}$, d. h.

$$\frac{a}{r} + \frac{b}{r} + \frac{a+b}{r} = \frac{a+b}{r}$$

$r\left(\frac{a}{r} + \frac{b}{r}\right) = r\left(\frac{a}{r}\right) + r\left(\frac{b}{r}\right) > a + b$

folglich (33)

$\frac{a}{r} + \frac{b}{r} > \frac{a+b}{r}$

[illegible]

Jede in $\frac{a}{r} + \frac{b}{r}$ enthaltene Zahl ist nämlich von der Form $u + v$, wo ru durch a, rv durch b, also beide durch $a+b$ theilbar sind; welcher ist auch $r(u+v)$ durch $a+b$ theilbar, also $u+v$ in $\frac{a+b}{r}$ enthalten. W. z. b. w.

35*.

Satz: Es ist

$$\frac{a \vee b}{r} = \frac{a}{r} \vee \frac{b}{r}.$$

Denn ist jede in $\frac{a \vee b}{r}$ enthaltene Zahl η ist $r\eta$ durch $a \vee b$, d. h. zugleich durch a und durch b theilbar, welcher ist η zugleich in $\frac{a}{r}$ und in $\frac{b}{r}$ enthalten, also ist $\frac{a \vee b}{r}$ theilbar durch $\frac{a}{r} \vee \frac{b}{r}$; umgekehrt, ist η in $\frac{a}{r} \vee \frac{b}{r}$ enthalten, also in $\frac{a}{r}$ und auch in $\frac{b}{r}$, so ist $r\eta$ theilbar durch a und auch durch b, also auch durch $a \vee b$, welcher ist η in $\frac{a \vee b}{r}$ enthalten, also ist $\frac{a}{r} \vee \frac{b}{r}$ theilbar durch $\frac{a \vee b}{r}$. W. z. b. w.

36.

Satz: Es ist $a\left(\frac{b}{r}\right)$ theilbar durch $\frac{ab}{r}$, wir schreiben

$$a\left(\frac{b}{r}\right) > \frac{ab}{r}.$$

Denn jede in $a\left(\frac{b}{r}\right)$ enthaltene Zahl u ist von der Form $\sum \alpha\eta$, wo α in a, η in $\left(\frac{b}{r}\right)$ enthalten ist; welcher ist $r\eta$ theilbar durch b, folglich $\alpha r\eta$ theilbar durch αb, also auch durch ab, also ist $\alpha\eta$ theilbar durch $\frac{ab}{r}$, also auch $u = \sum \alpha\eta$ theilbar durch $\frac{ab}{r}$. W. z. b. w.

37.

Satz: Es ist

$$\frac{a}{br} = \frac{\left(\frac{a}{b}\right)}{r} = \frac{\left(\frac{a}{r}\right)}{b}$$

Ist nämlich η in $\frac{a}{br}$ enthalten, so ist $\eta br = (\eta b) r$ theilbar durch a, folglich (32) ηb theilbar durch $\frac{a}{r}$, folglich (32) η theilbar durch $\frac{\left(\frac{a}{r}\right)}{b}$, also $\frac{a}{br}$ theilbar durch $\frac{\left(\frac{a}{r}\right)}{b}$; umgekehrt, ist η in $\frac{\left(\frac{a}{r}\right)}{b}$ enthalten, so ist ηb theilbar durch $\frac{a}{r}$, folglich (33) ηbr theilbar durch a, folglich η enthalten in $\frac{a}{br}$, also ist $\frac{\left(\frac{a}{r}\right)}{b}$ theilbar durch $\frac{a}{br}$. W. z. b. w.

38. (Vergl. 34.)

Satz: Es ist $\frac{a}{b} + \frac{a}{r}$ theilbar durch $\frac{a}{b \vee r}$, d. h. es ist

$$\frac{a}{b} + \frac{a}{r} + \frac{a}{b \vee r} = \frac{a}{b \vee r}.$$

Denn jede in $\frac{a}{b} + \frac{a}{r}$ enthaltene Zahl ist von der Form $\eta + \zeta$, wo $b\eta$ und $r\zeta$ durch a theilbar sind, da nun $(b \vee r)\eta$ durch $b\eta$, und $(b \vee r)\zeta$

35 a.

Satz: $\frac{r}{a+b} = \frac{r}{a} \vee \frac{r}{b}$

Einfacher Satz:

Ist b theilbar durch r, so ist

$\frac{b}{a}$ < $\frac{r}{a}$, und

$\frac{a}{r}$ > $\frac{a}{b}$

Wendet man für die Theilbarkeit von b durch r die Bezeichnung

$b > r$, $r < b$

an, so folgt hieraus:

$\frac{b}{a} > \frac{r}{a}$, $\frac{r}{a} < \frac{b}{a}$

$\frac{a}{b} < \frac{a}{r}$, $\frac{a}{r} > \frac{a}{b}$

Es ist

$r\left(\frac{b}{r}\right) > b$

also

$ra\left(\frac{b}{r}\right) > ab$

also

$a\left(\frac{b}{r}\right) > \frac{ab}{r}$

$a\frac{b}{ar} > \frac{b}{r} > \frac{ab}{ar}$

$\frac{b}{r} > \frac{ab}{ar}$

Satz: $\frac{b}{a} \cdot \frac{b_1}{a_1} > \frac{bb_1}{aa_1}$

Es ist

$br\left(\frac{a}{br}\right) > a$

also

$b\left(\frac{a}{br}\right) > \frac{a}{r}$

also

$\frac{a}{br} > \frac{\left(\frac{a}{r}\right)}{b}$

Umgekehrt ist

$b\left(\frac{\left(\frac{a}{r}\right)}{b}\right) > \frac{a}{r}$

$br\left(\frac{\left(\frac{a}{r}\right)}{b}\right) > r\left(\frac{a}{r}\right) > a$

also

$\frac{\left(\frac{a}{r}\right)}{b} > \frac{a}{br}$

Folglich

$\frac{a}{br} = \frac{\left(\frac{a}{r}\right)}{b}$

Da $b < b \vee r$ und $r < b \vee r$, so ist

$\frac{a}{b} > \frac{a}{b \vee r}$ und $\frac{a}{r} > \frac{a}{b \vee r}$

folglich auch

$\frac{a}{b} + \frac{a}{r} > \frac{a}{b \vee r}$

durch ab, beide also durch a theilbar sind, folgt auch $(b+c)(g+h)$ durch a theilbar, also $g+h$ theilbar durch $\frac{a}{b+c}$. W. z. b. w.

~~38.~~

~~Definition. Basis der Ordnung a^c eines Moduls a ist der Modul $a^c = \frac{a}{a}$ verstanden~~

~~40.~~

39.

Definition: Ein Modul o soll eine Ordnung heißen, wenn

$$\frac{o}{o} = o$$

ist.

40.

Satz: Ist o eine Ordnung, so ist $o^2 = o$.

Beweis. Zufolge des Satzes (32)

$$a\left(\frac{b}{a}\right) > b$$

und aus der Annahme $b = o$ ergibt sich für $a = b = o$ zunächst

$$o^2 > o;$$

~~Definition folgt hieraus nicht~~

~~$\frac{o^2}{o} > \frac{o}{o}$~~

~~also~~

~~$\frac{o^2}{o} > o$~~

~~Andererseits folgt aus dem Satze (32)~~

~~$b > ab$~~

~~für a = b ferner~~

~~$o > \frac{o^2}{o}$~~

~~also~~

~~$\frac{o^2}{o} = o$~~

Da ferner (39.a) $g > o$, so folgt $og > o^2$, und, weil $og = o$ ist,

$$o > o^2.$$

Mithin ist $o^2 = o$. W. z. b. w.

41.

Satz: Ist $o^2 = o$ und $g > o$, so ist o eine Ordnung.

Beweis. Aus $o^2 = o$ folgt ~~[illegible]~~ $o^2 > o$, also (nach 32)

$$o > \frac{o}{o}$$

und aus $g > o$ folgt ferner

$$\frac{o}{g} < \frac{o}{o}$$

d. h.

$$o < \frac{o}{o}$$

Mithin ist $o = \frac{o}{o}$. W. z. b. w.

39.a.

Satz: Jede Ordnung $\frac{o}{o}$ ist ein Theiler von dem aus allen ganzen rationalen Zahlen bestehenden Modul g (während g selbst eine Ordnung ist).

Denn nämlich $og = o$, also auch $og > o$, so folgt aus (29) $g > \frac{o}{o}$, d. h. $g > o$, W. z. b. w.

Oder mit Annahme: $o^2 > o$ und $g > o$

so folgt $o > \frac{o}{o}$ & $\frac{o}{g} < \frac{o}{o}$

also $o = \frac{o}{o}$

42.

Satz. Das Product $o_1 o_2$ von zwei Ordnungen o_1, o_2 ist wieder eine Ordnung.

Beweis. Da $o_1^2 > o_1$, $\mathfrak{z} > o_1$

$o_2^2 > o_2$, $\mathfrak{z} > o_2$

und $\mathfrak{z}^2 = \mathfrak{z}$, so folgt $(o_1 o_2)^2 > o_1 o_2$ und $\mathfrak{z} > o_1 o_2$; folglich (41) ist $o_1 o_2$ eine Ordnung.

43.

Satz: Ist o eine Ordnung, so ist $\mathfrak{a} > \mathfrak{a}o$.

Beweis. Da $\mathfrak{z} > o$, so folgt $\mathfrak{a}\mathfrak{z} > \mathfrak{a}o$, also $\mathfrak{a} > \mathfrak{a}o$.

Aus $\mathfrak{z} > o$ allein folgt $\frac{\mathfrak{a}}{o} > \frac{\mathfrak{a}}{\mathfrak{z}} > \mathfrak{a} > \mathfrak{a}o$

und $\frac{\mathfrak{a}o}{o} = \mathfrak{a}o$ $\left\{\begin{array}{l} \text{weil } \frac{\mathfrak{a}o}{o} > o\frac{\mathfrak{a}o}{o} > \mathfrak{a}o \\ \text{und } \mathfrak{a}o \cdot o = \mathfrak{a}o^2 > \mathfrak{a}o \\ \text{also } \mathfrak{a}o > \frac{\mathfrak{a}o}{o} \end{array}\right.$

44.

Satz: Das kleinste gemeinschaftliche Vielfache $o = o_1 - o_2$ von zwei Ordnungen o_1, o_2 ist wieder eine Ordnung.

Beweis. Aus $o_1^2 > o_1$ und $o > o_1$, ~~[illegible]~~, also auch $o^2 > o_1^2$ folgt $o^2 > o_1$, ebenso $o^2 > o_2$, folglich $o^2 > o$. Ferner folgt aus $\mathfrak{z} > o_1$, und $\mathfrak{z} > o_2$ auch $\mathfrak{z} > o$. W. z. b. w.

45.

Satz: Ist $\mathfrak{a}$ irgend ein Modul, so ist

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}}$$

eine Ordnung, welche die Ordnung von $\mathfrak{a}$ heißen und mit $\mathfrak{a}^0$ bezeichnet werden soll; und es ist $\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a}$.

Beweis. Da $\mathfrak{a}\mathfrak{z} = \mathfrak{a}$, ~~[illegible]~~ also auch $\mathfrak{a}\mathfrak{z} > \mathfrak{a}$, so folgt (20)

$$\mathfrak{z} > \frac{\mathfrak{a}}{\mathfrak{a}}, \text{ also } \mathfrak{z} > \mathfrak{a}^0 \text{ und } \mathfrak{a}\mathfrak{z} = \mathfrak{a} > \mathfrak{a}\mathfrak{a}^0$$

Ferner folgt aus (22)

~~$\mathfrak{a}\left(\frac{\mathfrak{a}}{\mathfrak{a}}\right) = \mathfrak{a}\mathfrak{a}^0 > \mathfrak{a}$~~

~~[illegible] (22)~~

~~$\frac{\mathfrak{a}^0}{\mathfrak{a}^0} = \frac{\left(\frac{\mathfrak{a}}{\mathfrak{a}}\right)}{\mathfrak{a}^0} = \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{a}^0} = \frac{\mathfrak{a}}{\mathfrak{a}}$~~

~~also~~ $\frac{\mathfrak{a}^0}{\mathfrak{a}^0} > \mathfrak{a}^0$

$$\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a}\left(\frac{\mathfrak{a}}{\mathfrak{a}}\right) > \mathfrak{a}$$

folglich ist

$$\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a}.$$

Endlich folgt aus (27)

$$\frac{\mathfrak{a}^0}{\mathfrak{a}^0} = \frac{\left(\frac{\mathfrak{a}}{\mathfrak{a}}\right)}{\mathfrak{a}^0} = \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{a}^0} = \frac{\mathfrak{a}}{\mathfrak{a}} = \mathfrak{a}^0$$

d. h. $(\mathfrak{a}^0)^0 = \mathfrak{a}^0$

W. z. b. w.

46.

Satz: Es ist $\mathfrak{a}^0 \mathfrak{b}^0 > (\mathfrak{a}\mathfrak{b})^0$

Denn es ist $(\mathfrak{a}^0\mathfrak{b}^0)(\mathfrak{a}\mathfrak{b}) = \mathfrak{a}\mathfrak{a}^0 \cdot \mathfrak{b}\mathfrak{b}^0 = \mathfrak{a}\mathfrak{b}$, also auch $(\mathfrak{a}^0\mathfrak{b}^0)(\mathfrak{a}\mathfrak{b}) > \mathfrak{a}\mathfrak{b}$, folglich (20)

$$\mathfrak{a}^0\mathfrak{b}^0 > \frac{\mathfrak{a}\mathfrak{b}}{\mathfrak{a}\mathfrak{b}} \text{ d. h. } \mathfrak{a}^0\mathfrak{b}^0 > (\mathfrak{a}\mathfrak{b})^0$$

W. z. b. w.

47.

Satz. (...)

$$a^0 b^0 > \left(\frac{b}{a}\right)^0.$$

Beweis. Denn es ist (zufolge 37)

$$\left(\frac{b}{a}\right)^0 = \frac{\left(\frac{b}{a}\right)}{\left(\frac{b}{a}\right)} = \frac{b}{a\left(\frac{b}{a}\right)};$$

nun ist (zufolge 45 und 32)

$$a^0 \cdot a\left(\frac{b}{a}\right) = a\left(\frac{b}{a}\right) > b$$

und folglich durch Multiplication mit b^0, und weil (zufolge 40) $bb^0 = b$ ist, auch

$$a^0 b^0 \cdot a\left(\frac{b}{a}\right) > b$$

folglich (43)

$$a^0 b^0 > \frac{b}{a\left(\frac{b}{a}\right)}$$

W. z. b. w.

48.

Definition und Satz. Ein Modul a soll umkehrbar heißen, wenn es einen Modul m der Art giebt, daß $am = a^0$ wird. Ist nun n ebenfalls ein solcher Modul, daß $an = a^0$ wird, so folgt

$$amn = na^0 = ma^0.$$

Dieser, von der speciellen Wahl des Moduls m oder n unabhängige Modul ma^0 soll mit a^{-1} bezeichnet werden und der zu a reciproke oder umgekehrte Modul heißen. Da $a^0a^0 = a^0$ ist, so folgt

$$aa^{-1} = a^0, \quad a^0a^{-1} = a^{-1},$$

und wenn gleichzeitig

$$aa' = a^0, \quad a^0a' = a'$$

ist, so folgt

$$aa^{-1}a' = (aa^{-1})a' = a^0a' = a'$$
$$= (aa')a^{-1} = a^0a^{-1} = a^{-1}$$

also

$$a' = a^{-1}.$$

Ein umkehrbarer Modul ist daher durch die Eigenschaften des einzigen Moduls a^{-1} charakterisirt, für welchen

$$aa^{-1} = a^0, \quad a^0a^{-1} = a^{-1}$$

ist.

49.

Satz. Ist a umkehrbar, so ist $(a^{-1})^0 = a^0$.

Beweis. Aus $a^0a^{-1} = a^{-1}$ folgt zunächst

$$a^0 > (a^{-1})^0,$$

$$a^0 \frac{b}{a} = b^0 \frac{b}{a} = a^0 b^0 \frac{b}{a} = \frac{b}{a}$$

weil

$$a\left\{a^0 b^0 \frac{b}{a}\right\} = aa^0 \frac{b}{a} b^0 = a \frac{b}{a} b^0 > bb^0 > b$$

also $a^0 b^0 \frac{b}{a} > \frac{b}{a}$

und umgekehrt (weil $> a^0$, $> b^0$, $> a^0b^0$)

$$\frac{b}{a} > a^0 b^0 \frac{b}{a}$$

[illegible]

Eigentlich soll umkehrbar.

Nach der allgemeinen Definition:

$$a^{-1} = \frac{a^0}{a} \quad \boxed{= \frac{a}{a^2} \quad (\text{nach } 37)}$$

$$aa^{-1} > a^0 \quad (\text{nach } 32)$$

~~$a^0 > (a^{-1})^0$ (nach 47, 47)~~

$$a a^0 a^{-1} = aa^{-1} > a^0; \quad a^0a^{-1} > a^{-1}$$
$$> a^0 \qquad\qquad a^{-1} > a^0a^{-1}$$

$$a^0a^{-1} = a^{-1}$$
$$a^0 > (a^{-1})^0$$

Also immer

$$\begin{cases} aa^{-1} > a^0 & ; \quad aa^{-1} > a^0 > (a^{-1})^0 \\ a^0a^{-1} = a^{-1} & ; \quad a > (a^{-1})^{-1} \\ a^0 > (a^{-1})^0 & ; \quad a^0 (a^{-1})^0 = (a^{-1})^0 \end{cases}$$

Giebt es einen Modul m, für welchen

$$am = a^0$$

wird, so ist

$$\begin{cases} m a^0 = a^{-1} \\ aa^{-1} = a^0 \\ (a^{-1})^0 = a^0 \\ (a^{-1})^{-1} = a \end{cases}$$

Ebenso: Wenn $\mathfrak{z} > aa^{-1}$, [illegible] so ist $aa^{-1} = a^0$ u. s. w.

Immer ist

$$a = aa^{-1}a ?$$

eine (Ausnahme a^0 [illegible]) Ordnung. Denn aus $aa^{-1} > a^0$ und $aa^0 = a$ folgt $(aa^{-1})^2 > a^0aa^{-1}$ [illegible], also $(aa^{-1})^2 > aa^{-1}$

folglich

$$a^2 = (aa^{-1})^2 + aa^{-1} + \ldots = aa^{-1} + \ldots = a$$

und da $\mathfrak{z} > a$, bildet a eine Ordnung.

aus $aa^{-1} = a^0$ und $a^{-1}(a^{-1})^0 = a^{-1}$ folgt

$$a^0(a^{-1})^0 = (aa^{-1})(a^{-1})^0 = a(a^{-1}(a^{-1})^0) = aa^{-1} = a^0$$

also, da a^0 eine Ordnung ist (nach 43)

$$(a^{-1})^0 > (a^{-1})^0 a^0$$

also

$$(a^{-1})^0 > a^0$$

mithin

$$(a^{-1})^0 = a^0.$$

50.

Satz. Ist a umkehrbar, so ist auch a^{-1} umkehrbar, und es ist

$$(a^{-1})^{-1} = a.$$

Beweis. Denn aus

$$aa^{-1} = a^0 \text{ und } a^0 a^{-1} = a^{-1}$$

und aus

$$(a^{-1})^0 = a^0$$

folgt

$$a^{-1}a = (a^{-1})^0 \text{ und } (a^{-1})^0 a = a$$

W. z. b. w.

51.

Satz. Ist a umkehrbar, so ist

$$\frac{ba^0}{a} = ba^{-1}.$$

Beweis. Da

$$(ba^{-1})a = ba^0 \text{ also auch } > ba^0$$

ist, so folgt aus (33)

$$ba^{-1} > \frac{ba^0}{a}; \quad \text{I.}$$

ferner folgt aus (22)

$$a\left(\frac{ba^0}{a}\right) > ba^0$$

und hieraus durch Multiplication mit a^{-1}

$$a^0\left(\frac{ba^0}{a}\right) > ba^{-1},$$

da ferner a^0 eine Ordnung ist, so folgt aus (43)

$$\frac{ba^0}{a} > a^0\left(\frac{ba^0}{a}\right) > ba^{-1}. \quad \text{II.}$$

W. z. b. w.

Und da $b > ba^0$, so ist

$$\frac{b}{a} > \frac{ba^0}{a}, \text{ also}$$

$$\frac{b}{a} > ba^{-1}$$

Ferner (ohne Voraussetzung): nach 36 ist allgemein

$$b\frac{a^0}{a} > \frac{ba^0}{a} \quad \text{allgemein: } ba^{-1} > \frac{ba^0}{a}$$

Satz: Ist $a^0 > b^0$, und $aa^{-1} = a^0$, so ist

$$\frac{b}{a} = ba^{-1}$$

52.

Satz. Sind a und b umkehrbar, so ist auch ab umkehrbar, und es ist

$$(ab)^0 = a^0 b^0, \quad (ab)^{-1} = a^{-1}b^{-1}.$$

Ferner ist $ba^0 > \frac{ab}{a}$
Specieller Fall von 36: $b\frac{a}{r} > \frac{ab}{r}$

Beweis. Da a umkehrbar ist, so ist (nach 51)

$$\frac{ab}{a} = \frac{aba^0}{a} = aba^{-1} = ba^0, \quad \text{— Besonderer Satz!}$$

und da b umkehrbar ist (nach 51)

$$\frac{ab}{ab} = (ab)^0 = \frac{\left(\frac{ab}{a}\right)}{b} = \frac{ba^0}{b} = \frac{ba^0b^0}{b} = ba^0 b^{-1} = a^0 b^0;$$

ferner ist

$$(ab)(a^{-1}b^{-1}) = aa^{-1}bb^{-1} = a^0 b^0 = (ab)^0$$

und

$$(ab)^0(a^{-1}b^{-1}) = a^0 b^0 a^{-1}b^{-1} = a^{-1}b^{-1}$$

folglich

$$(ab)^{-1} = a^{-1}b^{-1}$$

w.z.b.w.

53.

Satz: Ist a ein Körper, und setzt man

$$a^{-n} = \frac{a^0}{a^n} \quad , \text{wenn } n > 0 \, ,$$

so gelten für beliebige ganze rationale Exponenten τ, δ die Gesetze

$$a^\tau a^\delta = a^{\tau+\delta} \, , \quad \frac{a^\tau}{a^\delta} = a^{\tau-\delta} \, , \quad (a^\tau)^\delta = a^{\tau\delta} \, .$$

Beweis: zunächst folgt aus Def., daß a^n ein Körper ist, denn

$$(a^n)^0 = (a^0)^n = a^0$$

$$(a^n)^{-1} = (a^{-1})^n$$

Da $a^n \cdot (a^n)^{-1} = a^0 = (a^{-1})^0$; $a^0 \cdot (a^n)^{-1} = (a^{-1})^0 (a^{-1})^n = (a^{-1})^n = (a^n)^{-1}$

ist, so muß

$$(a^n)^{-1} = a^{-n} \, .$$

Da ferner

$$a^n a^{-n} = a^n \left(\frac{a^0}{a^n}\right) = a^0$$

ist, so folgt durch Multiplikation mit $(a^n)^{-1}$

$$a^0 a^{-n} = a^0 (a^n)^{-1}$$

oder da

$$a^{-n} = a^0 a^{-n} \, , \quad a^0 (a^n)^{-1} = (a^{-1})^0 (a^{-1})^n = (a^{-1})^n = (a^n)^{-1}$$

so ist

$$a^{-n} = (a^n)^{-1} \, ,$$

weiterhin

$$a^{-n} = (a^n)^{-1} = (a^{-1})^n \, .$$

also auch

$$a^n \cdot a^{-n} = a^0 \quad , \quad n > 0$$

also auch

$$a^\tau \cdot a^{-\tau} = a^0 \quad , \quad \tau \text{ beliebig}$$

Der Satz

$$a^\tau a^\delta = a^{\tau+\delta}$$

gilt zunächst, wenn $\tau \geq 0$, $\delta \geq 0$; ist ferner $\tau < 0$, $\delta < 0$, so ist

$$a^\tau a^\delta = (a^{-1})^{-\tau} (a^{-1})^{-\delta} = (a^{-1})^{-(\tau+\delta)} = a^{\tau+\delta} \, ,$$

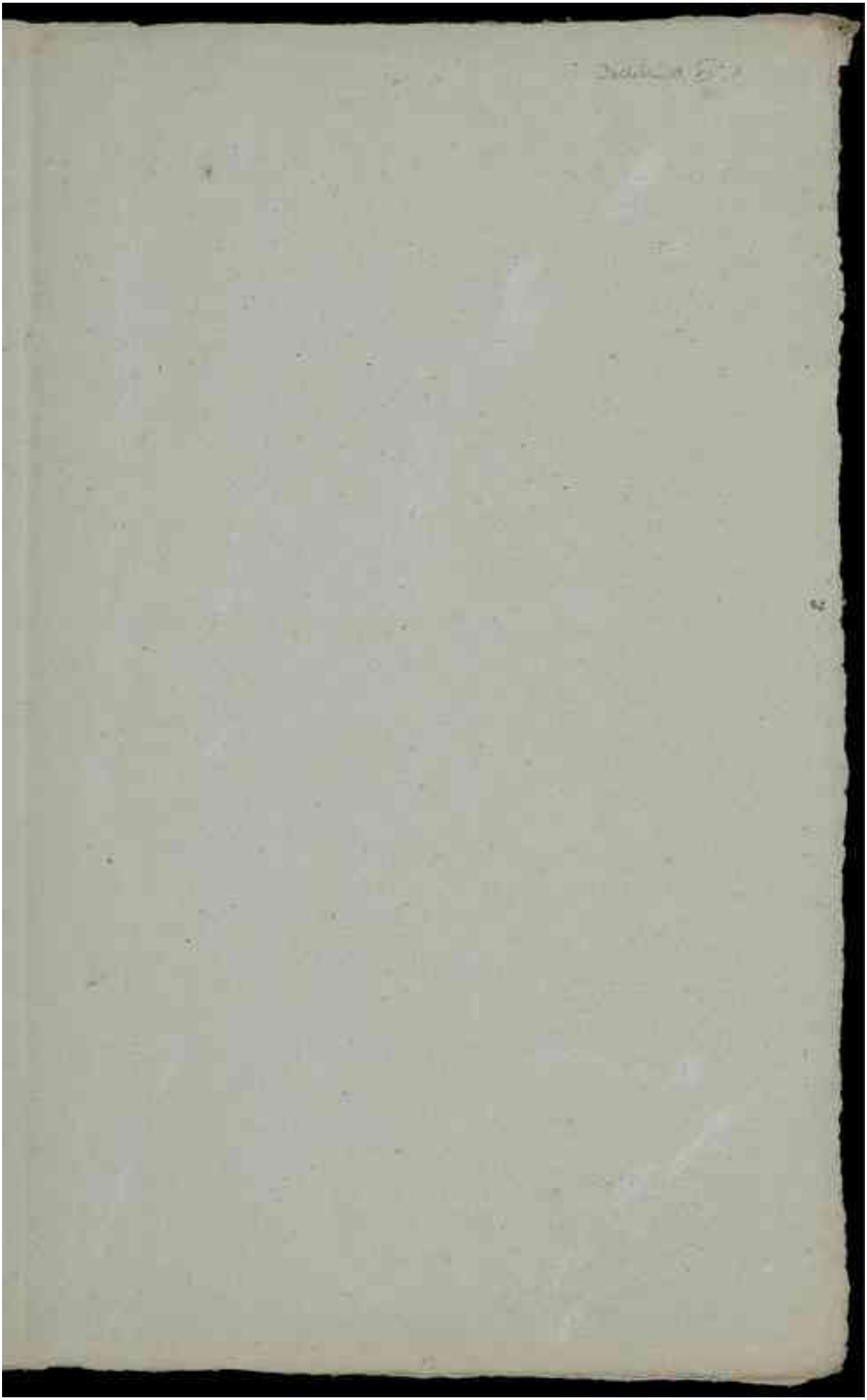
und derselbe muß für $\tau = 0$, $\delta = -n$ (auf dem Obigen)

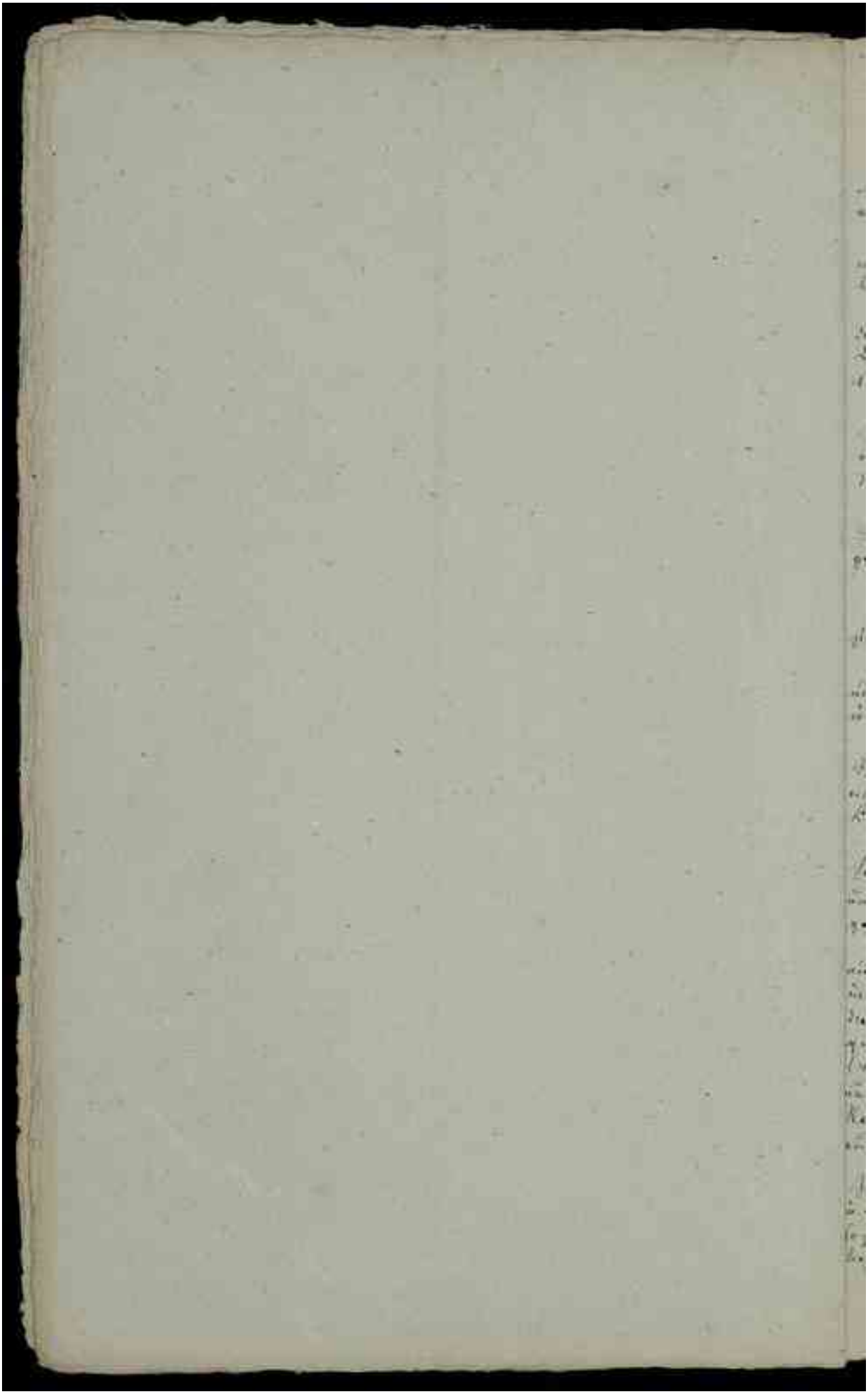
ist ferner $m > 0$, so ist

$$a^{m-n} \cdot a^{-m} = a^m \cdot a^{-n} \cdot a^{-m} = a^{-n} a^0 = a^{-n}$$

$$a^m \cdot a^{-(m+n)} = a^m \cdot a^{-n} \cdot a^{-m} = a^{-n} a^0 = a^{-n}$$

womit der Beweis für die andern Fälle klar ist, w.z.b.w.





und so ist

$\nu = a + d = (c \vee a) + b$;

[illegible] $a + b$ und durch $a + c$, [illegible] durch $(a+b) \vee (a+c)$; [illegible]

$a \vee (b \vee (a+c))$ theilbar durch $(c+a) \vee (a+b)$ [illegible] sind beide Moduln identisch, q. e. d.

Durch Vertauschung von b, c ergiebt sich die andere Identität. [illegible] durch [illegible]

14.

Definition der Zahlklassen (mod. a) oder a-Klassen, und der Congruenz der Zahlen (mod. a) (D. § 161, 1)

15.

Satz. Sind a, b gegebene Moduln, λ, μ gegebene Zahlen, so sind die Congruenzen

$$\left.\begin{array}{l} \omega \equiv \lambda \ (\text{mod. } a) \\ \omega \equiv \mu \ (\text{mod. } b) \end{array}\right\}$$

stets und nur dann gleichzeitig möglich, wenn

$$\lambda \equiv \mu \ (\text{mod. } a + b)$$

und dann bilden alle Zahlen ω eine Klasse in Bezug auf den Modul $(a \vee b)$.

16.

Ist a theilbar durch b, so besteht b aus einer endlichen oder unendlichen Anzahl von Klassen (mod. a). (D. § 161, 2.)

17.

Satz. Sind a, b irgend zwei Moduln, und bildet man ein vollständiges System von Zahlen

$\kappa_1, \kappa_2, \kappa_3, \ldots$

welche alle in a enthalten und zugleich incongruent (mod. b) sind, so bilden dieselben zugleich ein vollständiges System von Repräsentanten aller der Klassen (mod. b), aus welchen $a + b$ besteht, und zugleich ein vollständiges System von Repräsentanten aller der Klassen (mod. $a \vee b$), aus welchen a besteht.

18.

Ist die Anzahl der in a enthaltenen, in Bezug auf b incongruenten Zahlen endlich, so soll sie — Definition — durch (a, b) bezeichnet werden; ist sie aber unendlich, [illegible]

13. a.

Satz:

$$(c \vee a) + (a \vee b) = a \vee ((c \vee a) + b)$$
$$= a \vee ((a \vee b) + c)$$

[illegible] (13. 1.) [illegible] durch $(c \vee a)$, so folgt [illegible] $(c \vee a) + c$ [illegible]

$$c \vee ((c \vee a) + b) = (c \vee a) + (b \vee c)$$

q. e. d.

Dieser Satz ist charakteristisch für das Zeichen +, [illegible] $a \vee b$ [illegible]

$$a + b = b + a$$
$$(a + b) \vee b = b$$

[illegible] $c \vee a = c$, $a \vee b = b$, so folgt $b + c = a \vee (b + c)$, [illegible] (in Bezug auf a).

[illegible]

Dualität: + und ∨.

Repräsentanten von a nach b oder: von a (mod. b)

gesetzt $(a, b) = c$ (nicht $= 0$) zu schreiben.

59.

Die Theilbarkeit von a durch b kann daher durch die Gleichung $(a, b) = 1$ ausgedrückt werden.

60.

Ferner ist (zufolge 57.)

$(a + b, b) = (a, b) = (a, a \vee b)$

61.

Bilden die Zahlen

$x_1, x_2, x_3 \ldots$

ein vollständiges System von Repräsentanten der in a enthaltenen Zahlen (mod. b), und bilden die Zahlen

$\beta'_1, \beta'_2, \beta'_3 \ldots$ — besser $\beta'_1, \beta'_2, \beta'_3 \ldots$

ein vollständiges System von Repräsentanten der in ~~b~~ enthaltenen Zahlen (mod. c), — $(a \vee b)$ — so bilden die allen Combinationen r, s entsprechenden Zahlen

$x_r + \beta'_s$

ein vollständiges System von Repräsentanten der in ~~a~~ enthaltenen Zahlen (mod. $b \vee c$), und es ist folglich

$(a, b \vee c) = (a, b)(a \vee b, c)$

Beweis. Ist erstens

$x_r + \beta'_s \equiv x_{r'} + \beta'_{s'}$ (mod. $b \vee c$),

so findet diese Congruenz auch mod. b statt, und da $\beta'_s \equiv \beta'_{s'} \equiv 0$ (mod. b), so folgt $x_r \equiv x_{r'}$ (mod. b), woraus $r = r'$, also auch $x_r = x_{r'}$. Die angenommene Congruenz ergiebt daher $\beta'_s \equiv \beta'_{s'}$ (mod. $b \vee c$), also auch $\beta'_s \equiv \beta'_{s'}$ (mod. c), folglich $s = s'$, $\beta'_s = \beta'_{s'}$. Also sind alle Zahlen $x_r + \beta'_s$ incongruent (mod. $b \vee c$), und alle sind in a enthalten. Ist umgekehrt α eine Zahl in a, so giebt es eine (und nur eine) Zahl x_r der Art, daß $\alpha \equiv x_r$ (mod. b); dann ist $\alpha - x_r$ in a und b, also in $a \vee b$ enthalten, folglich einer (und nur einer) Zahl β'_s congruent (mod. c) und folglich auch (mod. $b \vee c$) (ja auch mod. $a \vee b \vee c$).

Hieraus folgt die obige Gleichung, mögen (a, b) und $(a \vee b, c)$ von Null verschieden sein oder nicht.