# Calculs sur les modules finis et divisibilité.

### 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

TitreCalculs sur les modules finis et divisibilité.
Date1894 ca.
Sujet

- divisibilité
- modules
- modules finis
- notation3
- théorie des nombres
- trois modules

CoteCod. Ms. Dedekind X 11-1, p. 3-8.
LangueAllemand

## Description & Analyse

DescriptionEnsemble de calculs et petites rédactions autour des opérations et de la divisibilité entre modules.
Mode(s) d'écriture

- Aufgaben
- Calculs phase 1
- Calculs phase 2

Auteur·es de la descriptionHaffner, Emmylou

## Relations

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

Ce document *utilise la même notation que :*

 Théorie des trois modules, divisibilité.

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



Calculs sur les modules et nombres de classes

*a les mêmes calculs que ce document*

Afficher la visualisation des relations de la notice.

## Mots-clefs

divisibilité, modules, modules finis, notation3, théorie des nombres, trois modules
Notice créée par Emmylou Haffner Notice créée le 26/10/2018 Dernière modification le 17/09/2020

---

~~Besitzt eine Zahl $\alpha'$ dann und nur dann unsere Forderung erfüllen, wenn die ganzen Zahlen $\omega, \omega'$ giebt, welche der Congruenz $\alpha' \equiv \alpha\omega, \alpha \equiv \alpha'\omega' \pmod{m}$ genügen. Ferner folgt $\alpha\omega, \alpha \equiv \alpha'\omega'$~~

$\alpha\omega\omega' \equiv \alpha$

~~$\pmod{m}$ genügen. Hieraus folgt $\alpha\omega\omega' \equiv \alpha \pmod{m}$~~, also nach (16) und (17) auch $\omega\omega' \equiv 1 \pmod{b}$, mithin ist $\omega$ zufolge (18) relativ prime zu $b$; umgekehrt, wenn Letzteres der Fall ist, und $\alpha' \equiv \alpha\omega \pmod{m}$ gesetzt wird, so kann man nach (18) eine Zahl $\omega'$ so wählen, daß $\omega\omega' \equiv 1 \pmod{b}$ wird, wonach wegen Multiplication und $\alpha \equiv \alpha'\omega' \pmod{m}$ folgt. Man erhält daher alle, d. h. nur die gesuchten Zahlen $\alpha'$ wie vorhin, wenn man $\alpha' \equiv \alpha\omega \pmod{m}$ setzt, und $\omega$ alle relativen

---

$\omega$ irreduc.

$a = [ha_1, a_2 + b\omega]$, $b = [hb_1, b_2 + ca\omega]$, $r = [hc_1, c_2 + ab\omega]$

$a''' = b + r = [hb_1, hc_1, b_2 + ca\omega, c_2 + ab\omega]$

$hb_1 \cdot a$, $hc_1 \cdot a$, $b_2 \cdot ca$, $c_2 \cdot ab$

$hca b_1, hab b_1, hca c_1, hab c_1, a(bb_2 - cc_2)$

$a[hcb_1, hbb_1, hcc_1, hbc_1, bb_2 - cc_2]$

$r_3 - 30\omega(30z - 15x_1)$
$= 30z - 30x_1$
$r_3 = 30\{z - x_1 + 30(z - 2x_1)\}$
$= 30[1 + 10\omega, 1 + 15\omega]$
$= 30[1 + 10\omega, 5\omega]$

---

$a = [10, 1 + 15\omega]$, $b = [15, 1 + 10\omega]$, $r = [25, 1 + 6\omega]$

$a''' = [15, 1 + 10\omega, 25, 1 + 6\omega] = [5, 4\omega, 1 + 2\omega] = [5, 2, 1 + 4\omega] = [1, 2\omega]$

$b''' = [5, 1 + 6\omega, 1 + 15\omega] = [5, 1 + 6\omega, -1 + 3\omega] = [5, 3, -1 + 3\omega] = [1, 3\omega]$

$r''' = [5, 1 + 10\omega, 1 + 15\omega] = [5, 5\omega, 1 + 10\omega] = [1, 5\omega]$

$\alpha''' = a + b + r = [1, \omega]$

$a_3 = 75\alpha''' = \frac{150}{2}a'''$

$b_3 = 50b''' = \frac{150}{3}b'''$

$r_3 = 30r''' = \frac{150}{5}r'''$

$a_3 = b - r$; $15x + (1 + 10\omega)y = 25x_1 + (1 + 6\omega)y_1 \neq a_3$; $15x + y = 25x_1 + y_1$; $10y = 6y_1$

$y = 3z$; $y_1 = 5z$; $5(3x - 5x_1) = 2z$; $z = 5z_1$; $3x - 5x_1 = 2z_1$;

$x - x_1 = 2(z_1 - x - 2x_1)$; $z_1 = x - 2x_1 + u$; $z = z_1 + 2u$; $z_1 = 3u - x_1$;

$x = x_1 + 2u$, $y = 15(3u - x_1)$, $x_1 = x_1$, $y_1 = 25(3u - x_1)$

$a_3 = 15(x_1 + 2u) + (1 + 10\omega)(3u - x_1)15 = 15[10\omega, 5 + 30\omega] = 75[1, 2\omega] = 75\alpha'''$

$b_3 = r - a$; $25x + (1 + 6\omega)y = 10x_1 + (1 + 15\omega)y_1$; $y = 5z$; $y_1 = 2z$; $\beta_3 - 30\omega z = 25x + 5z = 10z_1 + 2z$;

$x = 5x_1$; $\beta_3 - 150\omega z_1 = \beta 25(x + z_1) = 10(x_1 + z_1) = 50u$; $x + z_1 = 2u$; $x_1 + z_1 = 5u$

$x = 2u - z_1$, $z_1 = 5u - x_1$; $\beta_3 = 50[1, 3\omega] = 50b'''$

$r_3 = a \cdot b$; $\gamma_3 = 10x + (1 + 15\omega)y = 15x_1 + (1 + 10\omega)y_1$; $\gamma_3 - 30\omega z = 10z + 2z = 15x_1 + 3z = 6u$

$30r'''$ $\quad$ $5x + z = 3u$; $5x_1 + z = 2u$; $u = 5(x - x_1)$ $\quad$ $z = 10x - 15x_1$

~~Es sollen nun die Aufgaben~~, die Anzahl aller derjenigen verschiedenen Klassen $\mathfrak{k}+m\mathfrak{g}$ in $\mathfrak{o}+\alpha$ für bestimmte, deren Index $\alpha$ nullsteht, welche also der Bedingung $m+o\alpha=\alpha$ genügen.

Diese Aufgabe lässt sich zunächst auf den besonderen Fall stützen, wo $\alpha=0$ ist; es handelt sich dann um diejenigen Klassen, deren Indices teilerfremd zu $m$ sind, und wir wollen ihre Anzahl im Folgenden immer mit $\varphi(m)$ bezeichnen. Offenbar hat diese Funktion $\varphi$ genau dieselbe Bedeutung für unser Gebiet $o$, wie die Funktion $\varphi$ für das Gebiet $z$ der ganzen rationalen Zahlen (S. 11), und sie geht im Falle $n=1$ in die bekannte über. Ist nun $\alpha$ eine beliebige Zahl von $o$, und setzt man $m=ab$, so ist (nach S. 178 (X)) offenbar die Existenz einer Zahl $\alpha'$ bewiesen, welche der Bedingung $m+o\alpha=o$ genügt, und es kommt dieser Beweis auf (alle) Zahlen $\alpha'$ zu finden, welche die Bedingung $m+o\alpha'=m+o\alpha$ erfüllen. Da nun eine Modulgleichung von der Form $m+\gamma=m+\eta$ nur dann stattfindet, wenn $\gamma$ mit $\eta$ nach $m$ kongruent ist (vergl. nr.), und umgekehrt, so ist ~~in unserem Falle~~ $\alpha\equiv\omega\alpha'$ (mod. $m$), wo $\omega$ eine gewisse Zahl in $o$ bedeutet. Da ferner $\alpha\equiv\alpha'$ (mod. $m$), also $\omega\equiv1$ (mod. $b$), so ist $\omega$ relativ prim zu $b$, und umgekehrt, wenn $\omega$ relativ prim zu $b$ ist, und $\alpha'=\omega\alpha$ (mod. $m$) gesetzt wird, so ist $\alpha'$ ein vollständiges System von Resten nach $m$, wenn $\alpha$ ein solches ist, und $\alpha'\equiv\alpha$ (mod. $m$), dann, wenn $\omega\equiv1$ (mod. $b$) ist, $\omega$ relativ prim zu $b$ ist, und umgekehrt, wenn $\omega$ relativ prim zu $b$ ist, so ist $\omega\alpha$ ein vollständiges System von Resten nach $m$, wenn $\alpha$ ein solches ist, und $\alpha'\equiv\omega\alpha$ (mod. $m$), dann

da nämlich) gerichtet
jeder solche Modul $\underline{b}$ mit Restklassen $\beta'+\tau$ besetzen muß, welche
alle in $\underline{m}$ enthalten sind, und da die Anzahl aller in $m$ ent-
haltenen Restklassen $\alpha'+\tau$ endlich, nämlich $=(a,\tau)$ ist, so ist
auch die Anzahl der Moduln $\underline{b}$ sowohl gleich $\lambda^{m-1}$, womit die
Klasse $\underline{\tau}$ selbst gerichtet in $\underline{b}$ enthalten ist, q. e. d.

Alle Systeme dieser Verknüpfungen über Kongruenzen mit der
folgenden Verallgemeinerung einer in N. 25 bezeichneten Weise,
[III] $\underline{\varrho}$, $\sigma$ gegebene Zahlen, und $\underline{a}$, $\underline{b}$ irgend zwei Moduln, [Abtheil. I
so daß beide Systeme der beiden gleichzeitigen Kongruenzen

$$\omega \equiv \varrho \pmod{\underline{a}}, \quad \omega \equiv \sigma \pmod{\underline{b}} \tag{7}$$

stets und nur eine gemeinschaftliche Klasse $\omega$, deren

$$\varrho \equiv \sigma \pmod{\underline{a}+\underline{b}} \tag{8}$$

ist, mit allen diesen Klassen gleichen eine bestimmte Klasse
in Bezug auf den Modul $\underline{a}-\underline{b}$. In der That, wenn eine Zahl
$\omega$ den Kongruenzen (7) genügt, so sind die Zahlen $\omega-\varrho$, $\omega-\sigma$,
also auch ihre Differenz in $\underline{a}+\underline{b}$ enthalten, d. h. die Bedingung
(8) ist erfüllt. Umgekehrt, wenn dies der Fall ist, so giebt es
zufolge der Definition von $\underline{a}+\underline{b}$ eine Zahl $\alpha$ in $\underline{a}$ und eine Zahl
$\beta$ in $\underline{b}$, für deren Summe $\alpha+\beta=\varrho-\sigma$ ist, und dann erfüllt
die Zahl $\omega=\varrho-\alpha=\sigma+\beta$ die Kongruenzen (7). Genügt
ferner $\omega'$ denselben Kongruenzen (7), so ist $\omega'-\omega$ in $\underline{a}$ und in $\underline{b}$,
also in $\underline{a}-\underline{b}$ enthalten, mithin $\omega' \equiv \omega \pmod{\underline{a}-\underline{b}}$, und umgekehrt leuchtet ein, daß jede Zahl $\omega'$ der Klasse $\omega+(\underline{a}-\underline{b})$
auch den Kongruenzen (7) genügt, q. e. d. x)

[d. h. alle der beiden Klassen $\varrho+\underline{a}$, $\sigma+\underline{b}$ gemeinsamen Zahlen $\omega$ [Abtheil. I

4

---

x) Demgemäß gestaltet sich die Erledigung, für drei
oder mehre gegebene Kongruenzen, den Inhalt (7) betreffend, Restklassen
$\varrho+\underline{a}$, $\sigma+\underline{b}$, $\tau+\underline{c}$ ... gemeinsame Zahlen besitzen oder nicht;
im ersteren Falle kann man sie einig nennen, und es bezeichnet
sie, deren Gemeinheit, d. h. der Inbegriff aller jener gemeinsamen Zahlen, nach dem Modul $\underline{a}-\underline{b}-\underline{c}$... bezügliche
Klasse ist.

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

$$\mathfrak{a}_0 = \mathfrak{a}_1 + \mathfrak{a}_2 = a\mathfrak{a}' + hbc\,\mathfrak{a}'' = [ha, a+abc\omega, hbc, habc\omega]$$
$$= [h, a+abc\omega, habc\omega] = [h, a+abc\omega]$$
$$\mathfrak{a}_0 = \mathfrak{a}' - \mathfrak{a}''' = (\mathfrak{a}', \mathfrak{a}''')\mathfrak{a}' + (\mathfrak{a}'', \mathfrak{a}')\mathfrak{a}'' = (\mathfrak{d}''', \mathfrak{a}'')\mathfrak{a}' + (\mathfrak{d}''', \mathfrak{a}')\mathfrak{a}'''$$
$$= a\,\mathfrak{a}' + hbc\,\mathfrak{a}'''$$

$$\mathfrak{a}' + \mathfrak{a}''' = [h, 1+bc\omega, 1, a\omega] = \mathfrak{d}'''$$

Also

$$\mathfrak{a}_0 = [h, a+abc\omega], \quad \mathfrak{b}_0 = [h, b+abc\omega], \quad \mathfrak{r}_0 = [h, c+abc\omega]$$

---

$$\mathfrak{d}' = \mathfrak{a}'' - \mathfrak{b}''' - \mathfrak{r}''' = \mathfrak{a}'' - \mathfrak{a}'' = (\mathfrak{a}'', \mathfrak{a}''')\mathfrak{a}''' + (\mathfrak{a}'', \mathfrak{a}''')\mathfrak{a}''$$

$$\mathfrak{a}'' + \mathfrak{a}''' = [1, bc\omega, 1, a\omega] = [1, \omega] = \mathfrak{d}''''$$

$$\mathfrak{d}' = (\mathfrak{d}''', \mathfrak{a}'')\mathfrak{a}''' + (\mathfrak{d}''', \mathfrak{a}''')\mathfrak{a}'' = bc\,\mathfrak{a}''' + a\,\mathfrak{a}'' = [bc, abc\omega, a, abc\omega]$$
$$= [1, abc\omega]$$

---

$$\mathfrak{d}_1 = \mathfrak{a}_2 + \mathfrak{b}_2 + \mathfrak{r}_2 = h\{bc\,\mathfrak{a}''' + ca\,\mathfrak{b}''' + ab\mathfrak{r}'''\} = h[1, abc\omega] = h\,\mathfrak{d}'$$

---

$\mathfrak{a}_3 = hbc \cdot \mathfrak{a}'''$
$\mathfrak{a}_2 = ha \cdot \mathfrak{a}''$
$\mathfrak{a}_1 = a \cdot \mathfrak{a}'$
$\mathfrak{d}_1 = h \cdot \mathfrak{d}'$

---

Beispiel I.

$a = 3, \quad b = 4, \quad c = 5$

$(b-c)(c-a)(a-b) = 2$

$h = 3$

$\mathfrak{a} = [9, 1+20\omega]$
$\mathfrak{b} = [12, 1+15\omega]$
$\mathfrak{r} = [15, 1+12\omega]$

Summe der Coeff. $= 86$

Beispiel II.

$a = 2, \quad b = 3, \quad c = 5$

$(b-c)(c-a)(a-b) = 6$

$h = 5$

$\mathfrak{a} = [10, 1+15\omega]$
$\mathfrak{b} = [15, 1+10\omega]$
$\mathfrak{r} = [25, 1+6\omega]$

Summe der Coeff. $= 84$

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

Bei einander zweigliedrigen Modulen gilt die Zahl

$$\alpha - \beta = (\alpha, \beta)\alpha + (\beta, \alpha)\beta$$

also auch

$$\alpha - \beta - \gamma = (\alpha, \beta-\gamma)\alpha + (\beta-\gamma, \alpha)(\beta-\gamma)$$
$$= (\alpha, \beta-\gamma)\alpha + (\beta-\gamma, \alpha)\{(\beta,\gamma)\beta + (\gamma,\beta)\gamma\}$$
$$= (\alpha, \beta-\gamma)\alpha + (\beta,\gamma)(\beta-\gamma, \alpha)\beta + (\gamma,\beta)(\beta-\gamma, \alpha)\gamma$$
$$= (\alpha, \beta-\gamma)\alpha + (\beta, \gamma-\alpha)\beta + (\gamma, \alpha-\beta)\gamma$$

---

Drei Moduln $\alpha, \beta, \gamma$, $\omega$ irrational

$\alpha = [h a, 1 + bc\omega]$, $\beta = [h b, 1 + ca\omega]$, $\gamma = [h c, 1 + ab\omega]$

$a, b, c$ relative Primzahlen und $> 1$

$h \neq 1$ und relative Primzahl zu $(b-c)(c-a)(a-b)$

$\alpha''' = \beta + \gamma = [\underline{h b}, \underline{h c}, 1 + ca\omega, 1 + ab\omega, b(1+ca\omega) - c(1+ab\omega) = \underline{b-c}]$
$= [1, ca\omega, ab\omega] = [1, a\omega]$

$\alpha''' = [1, a\omega]$, $\beta''' = [1, b\omega]$, $\gamma''' = [1, c\omega]$; $\vartheta''' = \alpha''' + \beta''' + \gamma''' = [1, \omega]$

$(\beta, \gamma) = (\alpha''', \gamma) = hbc$; $(\gamma, \beta) = (\alpha''', \beta) = hbc$

$(\gamma, \alpha) = (\alpha, \gamma) = hca$; $(\alpha, \beta) = (\beta, \alpha) = hab$

---

$\alpha_3 = \beta - \gamma = (\beta, \gamma)\beta + (\gamma, \beta)\gamma = hbc(\beta+\gamma) = hbc\,\alpha'''$

$\beta_3 = \gamma - \alpha = hca\beta'''$; $\gamma_3 = \alpha - \beta = hab\gamma'''$

$\vartheta_4 = \alpha - \beta - \gamma = \alpha - \alpha_3$
$= (\alpha, \alpha_3)\alpha + (\alpha_3, \alpha)\alpha_3$
$= (\alpha', \alpha_3)\alpha + (\alpha', \alpha)\alpha_3$
$= habc\,\alpha + aa_3$
$= habc\,\alpha + habc\,\alpha'''$
$= habc(\alpha + \alpha''') = habc\vartheta''''$

---

$\alpha'' = \beta''' - \gamma''' = (\beta'', \gamma''')\beta''' + (\gamma''', \beta''')\gamma''' = (\vartheta'''', \gamma''')\beta''' + (\vartheta'''', \beta''')\gamma'''$
$= c\beta''' + b\gamma''' = [c, bc\omega] + [b, bc\omega] = [1, bc\omega]$

$\alpha'' = [1, bc\omega]$, $\beta'' = [1, ca\omega]$, $\gamma'' = [1, ab\omega]$

---

$\alpha_2 = \beta_3 + \gamma_3 = ha\{c\beta''' + b\gamma'''\} = ha\,\alpha'' = ha[1, bc\omega]$

$\beta_2 = \gamma_3 + \alpha_3 = hb\beta'' = hb[1, ca\omega]$, $\gamma_2 = \alpha_3 + \beta_3 = hc\gamma'' = hc[1, ab\omega]$

---

$\alpha' = \alpha + \alpha_2 = [ha, 1 + bc\omega, hbc, habc\omega] = [h, 1 + bc\omega, habc\omega] = [h, 1 + bc\omega]$

$\beta' = \beta + \beta_2 = [h, 1 + ca\omega]$, $\gamma' = \gamma + \gamma_2 = [h, 1 + ab\omega]$

---

$\alpha_1 = \alpha - \alpha''' = (\alpha, \alpha''')\alpha + (\alpha''', \alpha)\alpha''' = (\vartheta'''', \alpha''')\alpha + (\vartheta'''', \alpha)\alpha''' = aa + habc\,\alpha'''$
$= a(\alpha + hbc\,\alpha''') = a(\alpha + \alpha_3) = a\alpha' = a[h, 1 + bc\omega]$

$\beta_1 = b\beta' = b[h, 1 + ca\omega]$; $\gamma_1 = c\gamma' = c[h, 1 + ab\omega]$

---

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

IX. Ist $(\mathfrak{A}, m) > 0$, und $\mathfrak{A} - m$ theilbar durch jeden der $\varphi$ Moduln $m$, so ist die Anzahl aller derjenigen nach $m$ incongruenten Zahlen $\xi$ im $\mathfrak{A}$, die in keinem Modul $m$ sind, falls sie nicht gleich der Summen-Differenz

$$\Sigma(m', m) - \Sigma(m'', m), \qquad (g)$$

wo für $m'$ der Modul $\mathfrak{M}$ und jeder aus $\mathfrak{A}$ mit einer geraden Anzahl, für $m''$ jeder aus $\mathfrak{A}$ mit einer ungeraden Anzahl von Moduln $m$ gebildete kleinste Vielfache zu setzen ist.

Denn wenn $\mathfrak{A}$ irgend eine Zahl in $\mathfrak{D}$ bedeutet, so ist nach dem Obigen die Klasse $(\mathfrak{D} - m) + \mathfrak{A}$ der Inbegriff aller der Zahlen in $\mathfrak{D}$, welche $\equiv \omega \pmod{m}$ sind, und $\mathfrak{A}$ besteht aus $(\mathfrak{D}, m)$ solchen Klassen. Ist nun $\mathfrak{D} - m > m$, und $\omega$ in $m$, also auch in $\mathfrak{D} - m$ enthalten, so gilt dasselbe von allen Zahlen der Klasse $(\mathfrak{D} - m) + \omega$, und da $\mathfrak{D} - m$ aus $(\mathfrak{D} - m, m)$ solchen Klassen besteht, so ist $(\mathfrak{D}, m) - (\mathfrak{D} - m, m)$ die Anzahl derjenigen nach $m$ incongruenten Zahlen in $\mathfrak{D}$, welche nicht in $m$ enthalten sind. Mithin gilt unser Satz für den Fall $\varphi = 1$, weil es dann nur einen Modul $m' = \mathfrak{D}$, und nur einen Modul $m'' = \mathfrak{D} - m$ giebt. Nehmen wir an, es sei für eine bestimmte Anzahl $\varphi$ von Moduln $m$ allgemein bewiesen, und der Modul $\chi$ gehe ebenfalls in $\mathfrak{D} - m$ auf, so darf man $\mathfrak{D}$ auch durch $\mathfrak{D} - \chi$ ersetzen, weil $(\mathfrak{D} - \chi, m) > 0$, und weil der Modul $(\mathfrak{D} - \chi) - m = \mathfrak{D} - m$, also durch jeden Modul $m$ theilbar ist; so folgt $(g)$ ist daher die Differenz

$$\Sigma(m' - \chi, m) - \Sigma(m'' - \chi, m)$$

die Anzahl derjenigen, im Falle mit $\varphi$ bezeichneten Zahlen, welche in $\chi$ enthalten sind, giebt man dieselbe von der in $(g)$ angegebenen Anzahl aller Zahlen $\xi$ ab, so erhält man die Differenz

Fortsetzung auf der nächsten Seite 85. b.

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

$$\{\Sigma(n',m)+\Sigma(n''-\mathfrak{y},m)\}-\{\Sigma(n'',m)+\Sigma(n'-\mathfrak{y},m)\}$$

wo Summe alles mit in $\mathfrak{y}$ aufgehenden Faktor $\xi$, d. h. alles mal $m$ in $\mathfrak{o}$ ganzen Faktoren in $\mathfrak{o}$, welche in keinem der $(r+1)$ Moduln $\mathfrak{y}$ aufgehen sind. Vergleicht man diesen Ausdruck mit $(\mathfrak{Q})$, so ergibt sich, daß unser Satz auch für die nächst folgende Anzahl $(r+1)$, wofür allgemein gilt, ev. z. b. ev.

Statt die vollständige Induktion anzuwenden (wie in S. 11), kann man unseren Satz auch so mittelbar auf folgende Art beweisen (vergl. S. 128). Wir setzen die Bemerkung voraus, daß die Anzahl des Moduls $n'$ einmal der des Moduls $n''$, nämlich $=2^{r-1}$ ist; sondert man nämlich einen bestimmten Modul $n$ aus, und bezeichnet mit $\alpha'$, $\alpha''$ resp. alle die, zu $n'$, $n''$, so deren Teilung $n$ nicht unterstellt, so besteht das System aller Moduln $n'$ aus den Moduln $n'$, $\alpha''-n$, ebenso das System aller Moduln $n''$ aus den Moduln $\alpha'-n$, $\alpha''$, womit unsere Behauptung erwiesen ist.*) Bedeutet nun $\mathfrak{M}$ irgend eine Faktorenmenge in $\mathfrak{o}$, so bezeichnen wir mit $\mathfrak{M}\alpha'$, $\mathfrak{M}\alpha''$ resp. die Anzahl der Moduln $n'$, $n''$, denen $\mathfrak{M}$ angehört; faßt man $\mathfrak{M}$ ein Restsystem von $\mathfrak{o}$ nach $\mathfrak{y}$ laufen, so ist offenbar $\Sigma\alpha'=\Sigma(n',m)$, $\Sigma\alpha''=\Sigma(n'',m)$, also die in $(\mathfrak{Q})$ angegebene Differenz $=\Sigma(\alpha'-\alpha'')$. Da nun die Anzahl des Faktums $\xi$ offenbar $=\Sigma(\xi'-\xi'')$ ist, weil $\xi'=1$, $\xi''=0$, so wird unser Satz bewiesen sein, wenn wir zeigen, daß für jede andere Faktorenmenge $\mathfrak{M}$ die Differenz $\alpha'-\alpha''=0$, also $\alpha'=\alpha''$ ist. Bezeichnet man mit $\mathfrak{y}$ alle diejenigen Moduln $n$, denen $\mathfrak{M}$ angehört, und mit $\mathfrak{y}'$, $\mathfrak{y}''$ resp. alle diejenigen Moduln $n'$, $n''$, welche auf $\mathfrak{M}$ und nicht auf diesen Moduln $\mathfrak{y}$ gebildet sind, so gehört $\mathfrak{M}$ allemal den Moduln $\mathfrak{y}'$, $\mathfrak{y}''$ und keinem anderen Modul $n'$, $n''$ an; mithin ist $\alpha'$ die Anzahl der $\mathfrak{y}'$, ebenso $\alpha''$ die Anzahl der $\mathfrak{y}''$, woraus folgt nach der obigen Bemerkung $\alpha'=\alpha''$, ev. z. b. w.

*) [Siehe Rückseite 85. c.!]

~~85. c~~ $hca(y+bwy_1) = hab(z+cwz_1)$ ; $\frac{a}{b} = \frac{z}{c} = u$ ; $y = cz_1$

~~Hieraus ergiebt sich sogleich, dass gemeinschaftliche Theiler der Moduln a, b, c~~ aufgefasst ~~der System der mit dem~~, müssen $a'' - u = u''$, $a' - u = a'$ ist; das System der Moduln $u'$ mit dem der $w'$ zusammenfällt, und folglich die ~~einfache~~ Differenz (4) verschwindet, was damit übereinstimmt, dass in diesem Falle ~~gar kein~~ ausschliesslich kein Satz $\xi$ gilt. Aber man darf nicht ausgehen auf die bekannte Thatsache schliessen, dass gemeinschaftlichen der Moduln u bis v aufgefasst (vergl. S. 178. X).

$a = [ha_1, 1+bcw]$, $b = [hb_1, 1+caw]$, $r = [hc_1, 1+abw]$ | $bb'+cc' = 1$

$a, b, c$ rel. Nz. $> 1$ ; $a_1, b_1, c_1$ rel. Nz. $> 1$ | $k \equiv a \pmod{a_1}$ $\equiv b \pmod{b_1}$ $\equiv c \pmod{c_1}$

$k$ rel. Nz. zu $(b-c)(c-a)(a-b)$ | $b(b+c') = 1 - cc' + bc'$ $a_1 + c'(b-c)$ $c(b'+c') = cb' + 1 - bb'$ $a_1 - b'(b-c)$

$a''' = [k, 1+caw, 1+abw] = [k, 1+caw, a(b-c)w] = [k, 1+caw, 1+abw, b'+c'+aw]$

$= [k, b'+c'+aw, c(b'+c'), b(b'+c')] = [k, b'+c'+aw, (b-c)b', (b-c)c']$

$= [1, aw]$ ; $b''' = [1, bw]$

---

$a = [ha, 1+bcw]$, $b = [hb, 1+caw]$, $r = [hc, 1+abw]$

$a, b, c$ rel. Nz. $> 1$ ; $k$ rel. Nz. zu $(b-c)(c-a)(a-b)$ und $> 1$

$a''' = [k, 1+caw, 1+abw] = [k, 1+caw, 1+abw, b'+c'+aw] = [k, b'+c'+aw, 1-c(bc'), 1-b(bc')]$

$= [k, (b-c)b', (b-c)c', b'+c'+aw] = [1, aw]$

$b''' = [1, bw]$, $r''' = [1, cw]$ ; $s''' = [1, w]$

$a_2 = b - r$ ; $a_2 = hby + (1+caw)y_1 = hcz + (1+abw)z_1$ ; $y_1 = bu$, $z_1 = cu$

$a_2 - abcwu = hby + bu = hcz + cu$ ~~$= bcwu$~~ ; ~~$by + u = cwu$~~, ~~$hz + u = bcu$~~,

~~$h(y-z) = (c-b)u = h(b-c)u_2$~~ ; $y - z = (b-c)u_2$ ; $u_2 z = hu_2$

$h(by - cz) = (c-b)u = h(b-c)u_1$ ; $u = -hu_1$ ; $by - cz = (b-c)u_1$

$b(y - u_1) = c(z - u_2) = bcu_2$ ; $y = u_1 + cu_2$ , $z = u_1 + bu_2$

$b(by + u) = b(bu_1 + hcu_2 - hu_1) = hbcu_2$ | $\vartheta_2 = a - b - r = habz[1, w] + hab\vartheta'''$

$c(hz + u) = c(hu_1 + hbu_2 - hu_1) = hbcu_2$

$a_2 = hbcu_2 - habzwu_2$ ; $a_2 = hbc[1, aw] = hbca'''$, $b_2 = hcab'''$, $r_2 = habr'''$

---

$a'' = b''' - r''' = [1, bw] - [1, cw]$ ; $y + bwy_1 = z + cwz_1$ ; $y = z$ , $by_1 = cz_1 = bcu$ |

$a'' = [1, bcw]$, $b'' = [1, caw]$, $r'' = [1, abw]$

$a_2 = b_2''' + r_2 = [hca, habcw, hab, habcw] = ha[1, bcw] = haa''$, $b_2 = hab''$, $r_2 = hcr''$.

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

~~Einfachheit~~

~~Einfachheit eines Begriffes~~

~~Ähnlichkeit und Abhängigkeit von diesem Begriffe der Kette~~

~~Ähnlichkeit der Moduln, ein Modul a heißt theilbar durch den Modul b, wenn alle Zahlen des Moduls a auch in b enthalten sind, dann ist auch a theilbar durch jeden Modul b, der in a aufgeht, und jeder Modul c, durch welchen a und b theilbar sind, geht auch in a, b gegenseitig theilbar sind, wenn sie für identisch, und dann a = b~~

Theilbarkeit der Moduln ($>$, $<$, $+$, $-$)

I. $m > \mathfrak{d}$ gleichwerthig mit $\mathfrak{d} < m$,

II. mit $m + \mathfrak{d} = \mathfrak{v}$, mit $m - \mathfrak{d} = m$

III. $a + a = a$ ; $a - a = o$

$a + b = b + a$ ; $a - b = b - a$

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

---

Satz: Aus $a > a'$, und $a' > a''$ folgt $a > a''$

Beweis: Denn $a + a' = a'$ ; $a' + a'' = a''$; folglich

$a + a'' = a + (a' + a'') = (a + a') + a'' = a' + a' = a''$, w. z. b. w.

Oder $a - a' = a$ ; $a' - a'' = a'$; folglich

$a - a'' = (a - a') - a'' = a - (a' - a'') = a - a' = a$, w. z. b. w.

---

Satz: Aus $m > \mathfrak{d}$ und $\mathfrak{d} > m$ folgt $m = \mathfrak{d}$

Beweis: Denn $m + \mathfrak{d} = \mathfrak{d}$ und $\mathfrak{d} + m = m$, folglich $m = \mathfrak{d}$.

Oder $m - \mathfrak{d} = m$ und $\mathfrak{d} - m = \mathfrak{d}$, folglich $m = \mathfrak{d}$.

---

Satz: Aus $a > a'$ und $b > b'$ folgt $a + b > a' + b'$, $a - b > a' - b'$

Beweis: Denn $a + a' = a'$, $b + b' = b'$, folglich $(a + b) + (a' + b') = (a + a') + (b + b') = a' + b'$

$a - a' = a$, $b - b' = b$, folglich $(a - b) - (a' - b') = (a - a') - (b - b') = a - b$, w. z. b. w.

---

Satz: Aus $a > \mathfrak{d}$, $b > \mathfrak{d}$ folgt $a + b > \mathfrak{d}$

" $m > a$, $m > b$ " $m > a - b$

---

Satz: $a > a + b$, $a - b > a$

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

$(a - b) - a = (a - a) - b = a - b$

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

$c_0 x^k + c_1 x^{k-1} + \cdots = (x-\omega)(a_0 x^{k-1} + a_1 x^{k-2} + \cdots + a_{\tau} x^{k-1-\tau} + \cdots + a_{k-1})$

$c_0 = a_0 \; ; \; c_1 = a_1 - \omega a_0 \; \ldots \; c_\tau = a_\tau - \omega a_{\tau-1} \; \ldots \; c_{k-1} = a_{k-1} - \omega a_{k-2} \; ; \; c_k = -\omega a_{k-1}$

$c_\tau = (c_0 b^\tau + \cdots + c_\tau)$

$- \omega (c_0 \omega^{\tau-1} + \cdots + c_{\tau-1})$

$c_k = -\omega (c_0 \omega^{k-1} + \cdots + c_{k-1})$

IV. Sind alle Coefficienten $\alpha$ der Function $A$ und alle Coefficienten $b$ der Function $B$ rational ganze Zahlen, und sind alle Coefficienten $c$ des Products $AB$ ganze Zahlen, so sind auch alle Producte $ab$ ganze Zahlen.

Dieser Satz und der Satz II sind in ihrem Inhalt gleichwerthig, dasjenige sei vorausgesetzt, der eines aus dem andern ableiten kann, ohne nochmals auf den Kern der Beweise von Gauß, also auf die Zusammensetzung der Coefficienten $c$ aus den Coefficienten $a$ und $b$ zurückzugehen. Zu der Voraussetzung $A = \alpha A'$, $B = \beta B'$, wo $A'$, $B'$ ursprüngliche Functionen, und $\alpha$, $\beta$ gewisse rationale ganze Zahlen bedeuten, da wenn die Function $AB = \alpha\beta A'B'$ lauter ganze Coefficienten $c$ hat, auch die Function $A'B'$ (nach III) ursprünglich ist, gleich $\alpha\beta$ der größten gemeinsamen Theiler der Coefficienten $c$ eine ganze Zahl, da keines die Coefficienten $a$, $b$ also der Form $\alpha A'$, $\beta B'$ haben, wo $A'$, $B'$ Coefficienten der Functionen $A'$, $B'$, alle ganze Zahlen sind, so ist jedes Product von gewissen Coefficienten $a$, $b$ von der Form $\alpha\beta \cdot a'b'$ also ebenfalls eine ganze Zahl, q. e. d.

Umgekehrt heißt dieser Satz, wie aber der Satz IV aus dem Satze III, so folgt auch III aus IV abgeleitet werden kann, ohne daß nochmals auf den Kern des Beweises von Gauß, also auf die Zusammensetzung Bildung der Coefficienten eines Productes aus denen der Factoren zurückgegangen

Um dies zu beweisen, bezeichne ich mit $\alpha$, $\beta$ die größten Theiler der Functionen $A = \alpha A'$, $B = \beta B'$, wo mit $a'$, $b'$ alle Coefficienten der ursprünglichen Functionen $A'$, $B'$, jedes Product $ab$ ist dann von der Form $\alpha\beta \cdot a'b'$, wo folglich ganze Zahl und $\alpha\beta$ (nach II oder III) der Theiler der Function $AB$ ist, diese aber (nach Annahme) lauter ganze Coefficienten $c$ hat, so ist $\alpha\beta$ auch folglich auch jedes Product $ab$ eine ganze Zahl

Hieraus schließt sich, daß dieser Satz III eine gekehrt die Sätze II oder III abzuleiten

$\alpha'$ in $a$, nicht $b$, nicht $\tau$ | nicht $a$, in $b$, in $\tau$ : $\varkappa_0$
$\beta'$ nicht $a$, in $b$, nicht $\tau$ | in $a$, nicht $b$, in $\tau$ : $\beta_0$ } unmöglich
$\gamma'$ nicht $a$, nicht $b$, in $\tau$ | in $a$, in $b$, nicht $\tau$ : $\gamma_0$
in $a$, in $b$, in $\tau$

$o - b - \tau = o - \tau - a = o - a - b = o - a - b - \tau$
$o > a + b + \tau$

$\alpha' - \alpha''$ in $a$
$\beta' - \alpha'$ nicht in $a$, nicht in $b$, also in $\tau$
$\alpha'' \equiv \alpha' \pmod a$
$\alpha' \equiv \gamma' \pmod b$
$\alpha'' \equiv \beta' \pmod \tau$

Wäre $2\alpha'$ nicht in $b$ enthalten, so wäre
$2\alpha' - \beta'$
$\beta' + \gamma'$ und $\beta' - \gamma'$ beide in $a$ enthalten,
also auch $2\beta'$, $2\gamma'$
also
$2o > o - b - \tau$

$o = (o - a) + [\beta'] \; A = (o - a) + [\gamma']$
$=$

---

Aufgabe: Alle Systeme von vier Moduln $a, b, \tau, \delta$ zu finden, welche die Eigenschaften haben:

1) $\delta$ ist durch keinen der drei Moduln $a, b, \tau$ theilbar

2) Jede Zahl in $\delta$ ist in mindestens einem der Moduln $a, b, \tau$ enthalten.

Lösung: Da $\delta$ weder durch $b$, noch durch $\tau$ theilbar ist (1), so giebt es (vorher leicht zu beweisen) in $\delta$ eine Zahl $\alpha$, welche weder in $b$, noch in $\tau$, mithin (2) in $a$ enthalten ist. Man bezeichne mit
$\alpha$ alle Zahlen in $\delta$, welche so in $a$, nicht in $b$, nicht in $\tau$
$\beta$ " " " " " " nicht in $a$, in $b$, nicht in $\tau$ } enthalten sind
$\gamma$ " " " " " " nicht in $a$, nicht in $b$, in $\tau$

Da $\beta + \gamma$ weder in $b$, noch in $\tau$ enthalten, ~~ist~~ also in $a$ enthalten, so ist $\alpha + \beta + \gamma$ in $a$, ebenso in $b$, ebenso in $\tau$ enthalten, also

$\alpha + \beta + \gamma \equiv 0 \pmod m$ wo $m = a - b - \tau$. Ebenso $\pm\alpha \pm \beta \pm \gamma$, also $2\alpha, 2\beta, 2\gamma$

Eine Zahl in $\delta$, welche in zweien der 3 Moduln $a, b, \tau$ enthalten ist, ist auch in der dritten, also in $m$ enthalten, denn wenn $\delta$ in $b, \tau$ enthalten, so ist $\alpha + \delta$ nicht in $b$, nicht in $\tau$, mithin in $a$ enthalten, also auch $\delta$ in $a$ enthalten.

Alle Zahlen $\alpha$ bilden eine Klasse $\pmod{o - m}$.

Fichier issu d'une page EMAN : http://eman-archives.org/Dedekind/items/show/178?context=pdf

I. $h=1$; $b=1$; $c=1$; $\sigma = \alpha x\beta y + (\alpha-1)x + (\alpha-1)\beta + (\alpha-1)\gamma$

entw. $\alpha=1$, $\alpha\beta y = 0$

od. $\alpha>1$; $x=0$ d.h. $a_1=1$

II. $n=2$; $a=bc=1$; $a_1=b_1=c_1=1$.

$(\alpha_1, a_1) = a$

$(\alpha_1, a_2) = h$

$(\alpha_2, \alpha_3) = b_1$

$(\alpha_3, \alpha_4) = c_1$

Liebe nun ein Theil der Gruppe $\Pi$ abermals eine Gruppe $\Pi'$, welche auf $p$ fernere Relationen $\pi'$ besteht, so ist der zu $\Pi'$ gehörige Körper $A'$ Divisor von $M$ und Multiplum von $A$, und jede zu $\Pi$ conjugirte Gruppe auch eine conjugirte zu $\Pi'$ ist, eine zugleich ist $n = pq$, wo $p = (M, A')$, $q = (A', \Omega)$.

Ist umgekehrt, wenn der Körper $A'$ Divisor von $M$ und Multiplum von $A$ ist, so bilden die $q$ einzigen Fernen Relationen von $M$, welche Multiplen von den $q$ linearen Fernen Relationen von $A'$ sind, mit in $\Pi$ enthaltenen Gruppe $\Pi'$, und $A'$ ist der zu $\Pi'$ gehörige Körper. Ist ferner $A''$ abermals ein solcher Körper, welcher zu der in $\Pi$ enthaltenen Gruppe $\Pi''$ gehört, so gehört der Product $A'A''$ zu derjenigen Ist ferner $\Pi''$ abermals eine in $\Pi$ enthaltene Gruppe, und $A''$ der zu gehörige Körper, so bilden die den beiden Gruppen $\Pi'$, $\Pi''$ gemeinsamen Fernen Relationen wieder eine Gruppe, und der zu ihr gehörige Körper ist der Product $A'A''$.

Hieraus erhellt man, daß die vollständige Definition aller dieser Körper $A'$, $A''$... und die Aufstellung ihrer gegenseitigen Beziehungen gänzlich

$\Delta'''', a_3, b_3, r_3$; $a, b, r$, $\delta_4 \mid (\delta'''', a) = a_1 h bc$

$h^2abc\,a_1b_1c_1 + a_1 + b_1 + c_1 - hab_1c_1 - hbc_1a_1 - hca_1b_1 - 1 = \Delta$

$(a_1-1)(b_1-1)(c_1-1) = a_1b_1c_1 - (b_1c_1 + c_1a_1 + a_1b_1) + (a_1 + b_1 + c_1) - 1$

$\Delta - (a_1-1)(b_1-1)(c_1-1) = (h^2abc - 1)a_1b_1c_1 - \{(ha-1)b_1c_1 + (hb-1)c_1a_1 + (hc-1)a_1b_1\}$

$\Delta = h^2abc(\alpha\beta\gamma + \beta\gamma + \gamma\alpha + \alpha\beta + \alpha + \beta + \gamma + 1) + \alpha + \beta + \gamma + 3 - ha(\beta\gamma + \beta + \gamma + 1) - hb(\gamma\alpha + \gamma + \alpha + 1)$
$- hc(\alpha\beta + \alpha + \beta + 1) - 1$

$= h^2abc\,\alpha\beta\gamma + (h^2abc - ha)\beta\gamma + (h^2abc - hb)\gamma\alpha + (h^2abc - hc)\alpha\beta + (h^2abc + 1 - hb - hc)\alpha$
$+ (h^2abc + 1 - hc - ha)\beta + (h^2abc + 1 - ha - hb)\gamma + (h^2abc + 2 - ha - hb - hc)$

$= h^2abc\,\alpha\beta\gamma + ha(hbc - 1)\beta\gamma + hb(hca - 1)\gamma\alpha + hc(hab - 1)\alpha\beta + (h^2bc(a-1) + (hb-1)(hc-1))\alpha$
$+ (h^2ca(b-1) + (hc-1)(ha-1))\beta + (h^2ab(c-1) + (ha-1)(hb-1))\gamma +$

$\Gamma$, wie man leicht findet:

$4abc(h^2abc - h(a+b+c) + 1)$

$= (2abch - a - b - c)^2$

$+ 8abc - (a+b+c)^2$

$h^2(\gamma\alpha + \alpha\gamma + \gamma\beta + \beta\gamma + \alpha\beta + \beta\alpha)$
$+ \gamma + \alpha + \beta + 1$

$+ 2 - h(\beta+1) - h(\gamma+1) - h(\alpha+1)$

$= h^2(\beta\gamma + \gamma\alpha + \alpha\beta)$
$+ (h-1)h\beta + (h-1)h\gamma +$
$(h-1)h\alpha$
$+ h^2 - 3h + 2$

$= h^2(\beta\gamma + \gamma\alpha + \alpha\beta + \alpha + \beta + \gamma + 1)$
$- (h^2 - h)(\alpha + \beta + \gamma + 1)$
$+ (h-1)(h-2)$