

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

Es existiert eine Zahl α' dann und nur dann unsere Bedingung erfüllen,
wenn es zwei Zahlen ω, ω' gibt, welche die ^{Bedingungen} $\alpha' \equiv$
 $\alpha\omega, \alpha \equiv \alpha'\omega' \pmod{m}$ genügen. Hieraus folgt $\alpha\omega, \alpha \equiv \alpha'\omega'$
 $\pmod{m}$ genügen. Hieraus folgt $\alpha \equiv \alpha'\omega\omega' \pmod{m}$, also nach (16)
nach (17) auf $\omega\omega' \equiv 1 \pmod{b}$, mithin ist ω zu Folge (18) relativ
prim zu b ; umgekehrt, wenn letzteres der Fall ist, und $\alpha' \equiv$
 $\alpha\omega \pmod{m}$ gesetzt wird, so kann man nach (18) eine Zahl ω' so
wählen, daß $\omega\omega' \equiv 1 \pmod{b}$ wird, woraus dann die Möglichkeit
mit α auf $\alpha \equiv \alpha'\omega' \pmod{m}$ folgt. Man erhält also hier alle die
zu einer gegebenen Zahl α mit uns folgende, wenn man $\alpha' \equiv$
 $\alpha\omega \pmod{m}$ setzt, und ω alle relativ

ω irrational

$$\alpha = [ka, a_1 + b\omega], \quad b = [kb_1, b_2 + c\omega], \quad r = [kc, c_1 + a_1\omega]$$

$$\alpha'' = b + r = [kb_1, kb_2 + kc, b_2 + c\omega, c_1 + a_1\omega]$$

$$\left. \begin{array}{l} kb_1, \quad a \\ kb_2, \quad b \\ b_2, \quad ca \\ c_1, \quad ab \end{array} \right\} \begin{array}{l} kaab_1, kab_2, kaac, kabc, a(bb_2 - cc_1) \\ a[kab_2, kab_1, kac, kbc, b(b_2 - cc_1)] \end{array}$$

$$P_3 = 30\omega(30x - 15x_1)$$

$$= 30x - 30x_1$$

$$P_2 = 30 \left\{ 2x - x_1 + 5\omega(3x - 3x_1) \right\}$$

$$= 30[2x - 2x_1 + 15\omega]$$

$$= 30[2x - 2x_1 + 5\omega]$$

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

$$\alpha_3 = 75\alpha'' = \frac{75}{1}\alpha''$$

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

$$b_3 = 50b'' = \frac{50}{1}b''$$

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

$$r_3 = 30r'' = \frac{30}{1}r''$$

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

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

$$\alpha_3 = b - r; \quad 15x + (1 + 10\omega)y = 25x + (1 + 6\omega)y, \quad \# \alpha_3; \quad 15x + y = 25x + y_1; \quad 10y = 6y_1$$

$$y = 3x_1, \quad y_1 = 5x_1; \quad 5(2x - 5x_1) = 2x; \quad x_1 = 5x_1; \quad 3x - 5x_1 = 2x_1$$

$$x - 2x_1 = 2x_1 - x + 2x_1; \quad x_1 = x - 2x_1 + 2x_1; \quad x = x_1 + 2x_1, \quad x_1 = 2x_1 - x_1$$

$$x = x_1 + 2x_1, \quad y = 15(2x - x_1); \quad x_1 = x_1, \quad y_1 = 25(2x - x_1)$$

$$\alpha_3 = 15(x_1 + 2x_1) + (1 + 10\omega)(2x - x_1) = 15[10\omega, 5 + 20\omega] = 75[1, 2\omega] = 75\alpha'''$$

$$b_3 = r - 2; \quad 35x + (1 + 6\omega)y = 10x_1 + (1 + 15\omega)y_1; \quad y = 5x_1; \quad y_1 = 2x_1; \quad \beta_3 = 30\omega x = 25x + 5x = 10x_1 + 2x_1;$$

$$x = 5x_1; \quad \beta_3 = 150\omega x = 5 \cdot 25(x + x_1) = 10(x_1 + x_1) = 50x_1; \quad x + x_1 = 2x_1; \quad x_1 + x_1 = 5x_1$$

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

$$r_3 = \alpha \cdot b; \quad y_3 = 10x + (1 + 15\omega)y = 15x_1 + (1 + 10\omega)y_1; \quad y_3 = 30\omega x = 10x + 2x = 15x_1 + 3x_1 = 6x_1$$

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

$$\alpha_0 = \alpha_1 + \alpha_2 = a\alpha' + hbc\alpha''' = [ha, a + abc\omega, hbc, habc\omega] \\ = [h, a + abc\omega, habc\omega] = [h, a + abc\omega]$$

$$\alpha_0 = \alpha' - \alpha''' = (\alpha', \alpha''')\alpha' + (\alpha'', \alpha')\alpha'' = (\delta''', \alpha''')\alpha' + (\delta''', \alpha')\alpha'' \\ = a\alpha' + hbc\alpha''$$

$$\alpha' + \alpha''' = [h, 1 + bc\omega, 1, a\omega] = \delta''''$$

Also

$$\alpha_0 = [h, a + abc\omega], \quad b_0 = [h, b + abc\omega], \quad r_0 = [h, c + abc\omega]$$

$$\delta' = \alpha''' - b''' - r''' = \alpha''' - \alpha'' = (\alpha''', \alpha'')\alpha''' + (\alpha'', \alpha''')\alpha''$$

$$\alpha'' + \alpha''' = [1, bc\omega, 1, a\omega] = [1, \omega] = \delta''''$$

$$\delta' = (\delta''', \alpha'')\alpha''' + (\delta''', \alpha''')\alpha'' = bc\alpha''' + a\alpha'' = [bc, abc\omega, a, abc\omega] \\ = [1, abc\omega]$$

$$\delta_1 = \alpha_0 + b_0 + r_0 = h\{bca''' + cab''' + abr'''\} = h[1, abc\omega] = h\delta'$$

$$\begin{aligned} \alpha_3 &= hbc \cdot \alpha''' \\ \alpha_2 &= ha \cdot \alpha'' \\ \alpha_1 &= a \cdot \alpha' \\ \alpha_0 &= h \cdot \alpha' \end{aligned}$$

Beispiel I.

$$a = 2, \quad b = 4, \quad c = 5$$

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

$$h = 3$$

$$a = [9, 1 + 20\omega]$$

$$b = [12, 1 + 15\omega]$$

$$r = [15, 1 + 12\omega]$$

$$\text{Summe der Expp.} = 86$$

Beispiel II.

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

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

$$h = 5$$

$$a = [10, 1 + 15\omega]$$

$$b = [15, 1 + 10\omega]$$

$$r = [25, 1 + 6\omega]$$

$$\text{Summe der Expp.} = 84$$

Bei einander zueingliedigen Moduln gilt der Satz

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

also auch

$$\begin{aligned} a - b - r &= (a, b-r) a + (b-r, a) (b-r) \\ &= (a, b-r) a + (b-r, a) \{ (b, r) b + (r, b) r \} \\ &= (a, b-r) a + (b, r) (b-r, a) b + (r, b) (b-r, a) r \\ &= (a, b-r) a + (b, r-a) b + (r, a-b) r \end{aligned}$$

Drei Moduln a, b, r , ω irrational

$$a = [ha, 1+b\omega], b = [hb, 1+c\omega], r = [hc, 1+a\omega]$$

a, b, c relative Primzahlen und > 1

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

$$\begin{aligned} a''' = b+r &= [h', hc, 1+c\omega, 1+a\omega, b(1+c\omega) - c(1+a\omega) = b-c] \\ &= [1, c\omega, ab\omega] = [1, a\omega] \end{aligned}$$

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

$$(b, r) = (a''', r) = hbc; (r, b) = (a''', b) = hbc$$

$$(a, a) = (a, r) = hca; (a, b) = (b, a) = hab$$

$$a_2 = b - r = (b, r) b + (r, b) r = hbc(b+r) = hbc a''' \quad \delta_4 = a - b - r = a - a_2$$

$$b_2 = b - a = hca b''', r_2 = a - b = hab r'''$$

$$\begin{aligned} a'' = b''' - r''' &= (b''', r''') b''' + (r''', b''') r''' = (\delta''', r''') b''' + (\delta''', b''') r''' \\ &= c b''' + b r''' = [c, b\omega] + [b, b\omega] = [1, b\omega] \\ a'' = [1, b\omega], b'' = [1, c\omega], r'' = [1, ab\omega] \end{aligned}$$

$$\begin{aligned} &= (a, a_2) a + (a_2, a) a_2 \\ &= (a', a_2) a + (a', a) a_2 \\ &= habca + aa_2 \\ &= habca + habca''' \\ &= habca(a+a''') = habca'' \end{aligned}$$

$$a_2 = b_2 + r_2 = ha \{ c b''' + b r''' \} = ha a'' = ha [1, b\omega]$$

$$b_2 = r_2 + a_2 = hb b'' = hb [1, c\omega], r_2 = a_2 + b_2 = hc r'' = hc [1, ab\omega]$$

$$a' = a + a_2 = [ha, 1+b\omega, hbc, hab\omega] = [h, 1+b\omega, hab\omega] = [h, 1+b\omega]$$

$$b' = b + b_2 = [h, 1+c\omega], r' = r + r_2 = [h, 1+ab\omega]$$

$$\begin{aligned} a_1 = a - a'' &= (a, a'') a + (a'', a) a'' = (\delta''', a'') a + (\delta''', a) a'' = a a + habca''' \\ &= a(a + habca''') = a(a + a_2) = a a' = a [h, 1+b\omega] \end{aligned}$$

$$b_1 = b - b' = b [h, 1+c\omega], r_1 = a - r' = hc [h, 1+ab\omega]$$

IV. Ist $(\mathfrak{P}, m) > 0$, und $\mathfrak{P}-m$ heißt das jeden des Moduln m , so ist die Aussage aller diejenigen nach m un-
vergleichbaren Teilen $\mathfrak{Q}$ in $\mathfrak{P}$, die in keinem Modul m ent-
fallen hinein gleich der Trümmer, Differenz

$$\Sigma (u', m) - \Sigma (u'', m), \quad (9)$$

wo für u' der Modul $\mathfrak{P}$ und jeder auf $\mathfrak{P}$ mit einer geraden
Aussage, für u'' jeder auf $\mathfrak{P}$ mit einer un-geraden Aussage
von Modulen m gebildet kleinsten Teilen zu folgen ist.

Denn wenn $\mathfrak{P}$ irgend eine Teil in $\mathfrak{P}$ bedeutet, so ist nach
dem Obigen die Klasse $(\mathfrak{P}-m) + \mathfrak{P}$ der Subjekt aller der
Teile in $\mathfrak{P}$, welche $\equiv \mathfrak{P} \pmod{m}$ sind, und $\mathfrak{P}$ besteht aus
 $(\mathfrak{P}, m)$ solchen Klassen. Ist nun $\mathfrak{P}-m > m$, und $\mathfrak{P}$ in m ,
also auch in $\mathfrak{P}-m$ enthalten, so gilt dasselbe von allen Teilen
der Klasse $(\mathfrak{P}-m) + \mathfrak{P}$, und da $\mathfrak{P}-m$ mit $(\mathfrak{P}-m, m)$ solchen
Klassen besteht, so ist $(\mathfrak{P}, m) - (\mathfrak{P}-m, m)$ die Anzahl derje-
nigen nach m unvergleichbaren Teilen in $\mathfrak{P}$, welche nicht in m
enthalten sind. Müßte gilt unser Satz für den Fall $\tau = 1$,
wird es dann mit einem Modul $u' = \mathfrak{P}$, und mit einem Modul
 $u'' = \mathfrak{P}-m$ geben. Nimmt man an, es sei für eine bestimmte
Aussage τ zum Modul m allgemein bezeugt, und der Modul
 y ganz ebenfalls in $\mathfrak{P}-m$ auf, so darf man $\mathfrak{P}$ auf $\mathfrak{P}-y$
setzen, weil $(\mathfrak{P}-y, m) > 0$, und weil der Modul $(\mathfrak{P}-y) - m$
 $= \mathfrak{P}-m$, also dass jeder Modul m heilbar ist, zu folgen (9)
ist daher die Differenz

$$\Sigma (u'-y, m) - \Sigma (u''-y, m)$$

die Aussage derjenigen, im Satz mit $\mathfrak{Q}$ bezeichneten Teilen,
welche in y enthalten sind, gibt man dieselbe von der
in (9) angegebenen Aussage aller Teilen $\mathfrak{Q}$ ab, so resultiert
man die Differenz

Korrespondenz
auf dem
nächsten Blatt
85. b

$$\{\Sigma(u', u) + \Sigma(u'' - y, u)\} - \{\Sigma(u'', u) + \Sigma(u' - y, u)\}$$

als Klasse aller in y aufzählbaren Systeme $\mathcal{C}$, d. h. alle nach u in $\mathcal{R}$ aufzählbaren Systeme in $\mathcal{H}$, welche in einem der $(r+1)$ Module α , β aufzählbar sind. Vergleicht man diese mit $\mathcal{C}$ mit (9), so ergibt sich, daß unser Satz auch für die nächstfolgende Klasse $(r+1)$, nämlich allgemein gilt, s. g. b. 17.

Wird die vollständige Induktion angewandt (wie in S. 11), kann man unseren Satz auch unmittelbar auf folgende Art beweisen (vergl. S. 138). Wir fixieren die Bemerkung voraus, daß die Klasse der Module u' immer gleich der der Module u'' , nämlich $= 2^{r-1}$ ist, sondern man wählt einen bestimmten Modul u aus, und bezeichnet mit α' , α'' resp. alle die, zu u' , u'' , u in Beziehung stehenden u nicht eindeutig, so besteht das System aller Module u' aus den Modulen α' , $\alpha'' - u$, ebenso das System aller Module u'' aus den Modulen $\alpha' - u$, α'' , wobei unsere Festsetzung angewandt ist. Bedeutet nun $\mathcal{H}$ irgend eine Zahl in $\mathcal{H}$, so bezeichnet wir mit $\mathcal{H}'$, $\mathcal{H}''$ resp. die Klasse der Module u' , u'' , denen $\mathcal{H}$ zugehört, läßt man $\mathcal{H}$ ein Restsystem von $\mathcal{H}$ nach u durchlaufen, so ist offenbar $\Sigma \alpha' = \Sigma(u', u)$, $\Sigma \alpha'' = \Sigma(u'', u)$, also die in (9) angegebene Differenz $= \Sigma(\alpha' - \alpha'')$. Da nun die Klasse der Systeme offenbar $= \Sigma(\mathcal{H}' - \mathcal{H}'')$ ist, weil $\mathcal{H}' = 1$, $\mathcal{H}'' = 0$, so ist unser Satz bewiesen, wenn wir zeigen, daß für jede andere Zahl $\mathcal{H}$ die Differenz $\alpha' - \alpha'' = 0$, also $\alpha' = \alpha''$ ist. Bezeichnet man mit y alle diejenigen Module u , denen $\mathcal{H}$ zugehört, und mit y' , y'' resp. alle diejenigen Module u' , u'' , welche aus $\mathcal{H}$ und aus diesen Modulen y gebildet sind, so gehört $\mathcal{H}$ allen diesen Modulen y' , y'' und einem anderen Modul u' , u'' an; mithin ist α' die Klasse der y' , ebenso α'' die Klasse der y'' , und folglich nach der obigen Bemerkung $\alpha' = \alpha''$, s. g. b. 17.

*] [Vgl. Anhang 85. c.]

85.c.

$$hca(y+by_1) = hab(x+cz_1); \frac{x}{b} = \frac{z}{c} = u; y_1 = c;$$

~~Es ist anzunehmen, dass, wenn man die Module u in $\mathcal{O}$ aufstellt, das System der mit dem, mit $\alpha' - u = u''$, $\alpha' - u = \alpha'$ ist, das System der Module u' mit dem der u'' zusammenfällt, und folglich die einzige Differenz (9) verschwindet, was damit übereinstimmt, dass in diesem Falle gar kein selbstständiges System $\mathcal{O}$ existiert. Aber man darf nicht übersehen, dass das letztere Theorem folgendermaßen, dass man die Module u in $\mathcal{O}$ aufstellt (vergl. S. 178. IX).~~

$$\begin{aligned} \alpha &= [ha, 1+b\omega], \beta = [hb, 1+c\omega], \tau = [hc, 1+a\omega] \\ a, b, c \text{ rel. Pr. } > 1; a, b, c \text{ rel. Pr. } > 1 & \left| \begin{array}{l} ka \pmod{a_1} \\ b \pmod{b_1} \\ c \pmod{c_1} \end{array} \right. \\ k \text{ rel. Pr. zu } (b-c)(c-a)(a-b) & \\ \alpha''' &= [h, 1+c\omega, 1+ab\omega] = [h, 1+c\omega, a(b-c)\omega] = [h, 1+c\omega, 1+ab\omega, b'+c'+a\omega] \\ &= [h, b'+c'+a\omega, c(b-c), h(b+c')] = [h, b'+c'+a\omega, (b-c)b', (b-c)c'] \\ &= [1, a\omega], \beta''' = [1, b\omega] \end{aligned}$$

$$\begin{aligned} \alpha &= [ha, 1+b\omega], \beta = [hb, 1+c\omega], \tau = [hc, 1+a\omega] \\ a, b, c \text{ rel. Pr. } > 1; k \text{ rel. Pr. zu } (b-c)(c-a)(a-b) \text{ und } > 1 \\ \alpha''' &= [h, 1+c\omega, 1+ab\omega] = [h, 1+c\omega, 1+ab\omega, b'+c'+a\omega] = [h, b'+c'+a\omega, 1-c(b-c), 1-b(b-c)] \\ &= [h, (b-c)b', (b-c)c', b'+c'+a\omega] = [1, a\omega] \\ \beta''' &= [1, b\omega], \tau''' = [1, c\omega], \gamma''' = [1, \omega] \end{aligned}$$

$$\begin{aligned} \alpha_2 &= b-r; \alpha_3 = hby + (1+c\omega)y_1 = hcx + (1+ab\omega)z_1; \beta_1 = bu, \tau_1 = cu \\ \alpha_2 - ab\omega u &= hby + bu = hcx + cu = b\omega u_1; hby + cu = hcx + cu = b\omega u_1 \\ h(y-x) &= (c-b)u = h(b-c)u_1; y-x = (b-c)u_1; u_1 = hu_2 \\ h(by-cx) &= (c-b)u = h(b-c)u_1; u = -hu_1; by-cx = (b-c)u_1 \\ b(y-u_1) &= c(x-u_1) = b\omega u_2; y = u_1 + cu_2, z = u_1 + bu_2 \\ b(by+u) &= b(hu_1 + hc u_2 - hu_1) = hbc u_2 \\ c(hx+u) &= c(hu_1 + hb u_2 - hu_1) = hbc u_2 \\ \alpha_2 &= hbc u_2 - hbc \omega u_2; \alpha_3 = hbc[1, a\omega] = hbc \alpha''', \beta_2 = hcb''', \tau_2 = hab'''' \\ \alpha'' &= b'' + \tau'' = [1, b\omega] - [1, c\omega], y+by_1 = z+c\omega z, y=x, by_1 = cz_1 = bc\omega \\ \alpha'' &= [1, b\omega], \beta'' = [1, c\omega], \tau'' = [1, ab\omega] \\ \alpha_2 &= \beta_2 + \tau_2 = [hca, hcb\omega, hab, hab\omega] = ha[1, b\omega] = ha\alpha'', \beta_2 = hab'', \tau_2 = hct''. \end{aligned}$$

Definition
 Zwei Moduln a und b heißen gleichwertig oder äquivalent, wenn es ein Modul δ gibt, so dass $a = \delta + b$ gilt. Dies ist der Fall, wenn a und b denselben Restklassenmodul δ enthalten. Sind zwei Moduln a und b gegeben, so sind sie äquivalent, wenn $a = \delta + b$ gilt.

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

I. $m > \delta$ gleichwertig mit $\delta < m$,

mit $m + \delta = \delta$, mit $m - \delta = m$

II. $a + a = a$; $a - a = a$

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

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

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

Beweis: Dem $a + a' = a'$; $a' + a'' = a''$; 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 $m > \delta$ und $\delta > m$ folgt $m = \delta$

Beweis: Dem $m + \delta = \delta$ und $\delta + m = m$; folglich $m = \delta$.

Oder $m - \delta = m$ und $\delta - m = \delta$; folglich $m = \delta$.

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

Beweis: Dem $a + a' = a'$; $b + b' = b'$; 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 $a > \delta$; $b > \delta$ folgt $a + b > \delta$

oder $m > a$; $m > b$; $m > a + b$

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

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

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

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

$$c_0 = a_0, c_1 = a_1 - \omega a_0, \dots, c_{k-1} = a_{k-1} - \omega a_{k-2}, \dots, c_k = -\omega a_{k-1}$$

IV. Sind alle Koeffizienten a der Funktion A und alle Koeffizienten b der Funktion B rationale Zahlen, und sind alle Koeffizienten des Produktes AB ganze Zahlen, so sind auch alle Produkte a b ganze Zahlen.

Dieses Satz aus dem Satz II. folgt in dem Sinne gleich, nämlich, daß man sich vorstellen kann, ohne auf den Weg der Beweis von Gauss, also auf die Zusammensetzung der Koeffizienten c aus den Koeffizienten a und b zurückzuführen. Setzt man $A = xA'$, $B = \beta B'$, so ist A' und B' ein ganzzahliges Polynom, und α, β ganzzahlige rationale Zahlen. Da nun die Funktion $AB = \alpha\beta A'B'$ laut dem Annahme 1) lauter ganze Koeffizienten c hat, und die Funktion $A'B'$ (nach III) unzerlegbar ist, so ist $\alpha\beta$ der größte gemeinsame Theiler der Koeffizienten c eine ganze Zahl. Da lassen die Koeffizienten a, b die Form $\alpha a', \beta b'$ haben, wo a', b' Koeffizienten der Funktionen A', B' , die ganze Zahlen sind, so ist jedes Produkt a, b genau Koeffizienten a, b von der Form $\alpha\beta a' b'$, also ebenfalls eine ganze Zahl, u. s. w.

Umgekehrt ist bekanntlich, daß, wie aus dem Satz II und dem Satz III, ~~unmittelbar~~ aus II und III ~~abgeleitet~~ werden kann, ohne auf irgendwelchen Weg der Beweis von Gauss, also auf die Zusammensetzung der Koeffizienten c aus den Koeffizienten a und b zurückzuführen.

Das ist zu sehen, nämlich, vorausgesetzt, daß a, b die Funktionen $A = \alpha A'$, $B = \beta B'$ sind mit α, β neuen Koeffizienten der unzerlegbaren Funktionen A', B' , jedes Produkt a, b ist dann von der Form $\alpha\beta a' b'$, was folgt, da a, b (nach II oder III) die Theiler der Funktionen AB sind, diese aber (nach Annahme 1) lauter ganze Koeffizienten c hat, so ist $\alpha\beta$ ein Faktor von jedem Produkt a, b und daher ist es, nach dem Satz III, unzerlegbar. Das ist also II oder III abgeleitet.

$$\left. \begin{array}{l} \sqrt[1]{\text{in } a, \text{ nicht } b, \text{ nicht } c} \\ \sqrt[2]{\text{nicht } a, \text{ in } b, \text{ nicht } c} \\ \sqrt[3]{\text{nicht } a, \text{ nicht } b, \text{ in } c} \\ \sqrt[4]{\text{in } a, \text{ in } b, \text{ in } c} \end{array} \right\} \begin{array}{l} \text{nicht } a, \text{ in } b, \text{ in } c : \alpha_0 \\ \text{in } a, \text{ nicht } b, \text{ in } c : \beta_0 \\ \text{in } a, \text{ in } b, \text{ nicht } c : \gamma_0 \end{array} \left. \vphantom{\begin{array}{l} \sqrt[1]{\text{in } a, \text{ nicht } b, \text{ nicht } c} \\ \sqrt[2]{\text{nicht } a, \text{ in } b, \text{ nicht } c} \\ \sqrt[3]{\text{nicht } a, \text{ nicht } b, \text{ in } c} \\ \sqrt[4]{\text{in } a, \text{ in } b, \text{ in } c} \end{array}} \right\} \text{unmöglich}$$

$$\sigma - \beta - \epsilon = \sigma - \gamma - \alpha = \sigma - \alpha - \beta = \sigma - \alpha - \beta - \gamma$$

$$K^p - K^q \leq 0, \quad p < q$$

$\beta^1 = \alpha^1$ nicht in α , nicht in β , also in τ

$$x^b \equiv x^t \pmod{n}$$

$$y' = y^2 \quad (\text{not } e)$$

$$\alpha' \equiv \beta' \pmod{\tau}$$

Wäre α^1 nicht in b enthalten, so wäre

207-51.

$\beta^1 + \gamma^1$ and $\beta^1 - \gamma^1$ binds in a subplate.

also aus z, z', z''

207. $\pi = 6 - \pi$

$$y = (y - \alpha) + E[\beta' | \mathcal{A}] = (y - \alpha) + \bar{\beta}' \mathcal{I}$$

88

Aufgabe: Alle Systeme von vier Modulen a, b, c, d zu finden, welche die Eigenschaften haben:

1) $\bar{z}$ ist durch Keinen der drei Module $n, 6, 7$ theilbar

2) Jede Zahl in I ist ein mindestens eines der obigen a, b, c teilt.
Bew. Für I wieder durch 6, und durch 11. $11 \mid 1001$ und $11 \mid 10001$.

Lösung: Für δ wieder durch b , auch durch τ theilbar ist (1), so gibt es (vorher leicht zu beweisen) in δ eine Zahl x , welche auch in b , auch in τ , theilbar (2) ist. Man beschreibe mit

alle Fehler, ^{in a} ~~welche~~, welche ~~in a~~, nicht in b, nicht in T

β — — — — —, — — — — —, nicht in T
 γ — — — — —, — — — — —, in T
 δ — — — — —, — — — — —, in T

enthalten sind

$\alpha + \beta + \gamma$ under in b , with in t sublates, ~~is~~ also in α sublates, so is $\alpha + \beta + \gamma$ in α , shows in b , shows in t sublates, also

$\alpha + \beta + \gamma \equiv 0 \pmod{m} = a - b - c$ (Es sei $\pm \alpha \pm \beta \pm \gamma$, also $2a, 2b, 2c$),

Die Zahl in $\mathfrak{d}$, welche in zweien der 3 Moduln α, β, γ enthalten ist, ist auch in dritten, also in $\mathfrak{a}$ enthalten; denn wenn δ in β, γ enthält, so ist $\alpha + \delta$ nicht in β , nicht in γ , mithin in α enthalten, also auch δ in α enthalten.

Alle Zahlen α bilden eine Klasse mod. $(0-n)$

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

$$\text{oder } \alpha=1, \alpha\beta\gamma=0$$

$$\text{oder } \alpha>1, \alpha=0 \text{ oder } \alpha=1$$

$$II. a=2; a=b=c=1; a_1=b_1=c_1=1$$

$$(a, a_1) = a$$

$$(a_1, a_2) = h$$

$$(a_2, a_3) = b_1$$

$$(a_3, a_4) = c_1$$

~~Liegt nun ein System der Gruppe Π ebenfalls eine Gruppe Π' , welche aus p Permutationen π' besteht, so ist das zu Π' gehörige Körper Π' ein System von M und Mächtigkeit von A , weil jede zu Π zugehörige Permutation auch eine Permutation zu Π' ist, und zugleich ist $\pi = \pi q$, wo $p = (A, A')$, $q = (A', A)$.
 Macht man jedoch, wenn der Körper A' ein System von M und Mächtigkeit von A ist, so bilden diejenigen Permutationen von A , welche Mächtigkeit von A und diejenigen Permutationen von A' sind, eine in Π enthaltene Gruppe Π' , und A' ist der zu Π' gehörige Körper. Ist ferner A'' ebenfalls ein solches System, welches zu Π enthaltene Gruppe Π'' gehört, so gehört das Produkt $A'A''$ zu Π und ist ferner Π'' ebenfalls eine in Π enthaltene Gruppe, und A'' der zu Π'' gehörige Körper, so bilden alle die drei Körper Π' , Π'' gemeinsamen Permutationen wieder eine Gruppe, und das zu ihr gehörige Körper ist das Produkt $A'A''$.~~

1) wie man leicht sieht,

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

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

$$+ 4abc = (a+b+c)^2$$

$$h^2(pq+q+1+p+q+1)$$

$$+ 2 - h(p+1) - h(q+1) - h^2pq$$

$$= h^2(pq+q+1+p+q+1)$$

$$+ (h-1)hp + (h-1)hq +$$

$$(h-1)h^2$$

$$+ h^2 - 2h + 2$$

$$= h^2(pq+q+1+p+q+1)$$

$$+ (h-1)(p+q+1)$$

$$+ (h-1)(h-2)$$

Gehen wir nun, daß die vollständige Definition aller dieser Körper A' , A'' ... und die Aufeinanderfolge ihrer gegenseitigen Beziehungen vollständig

$$d''', a_1, b_1, c_1; a_2, b_2, c_2; a_3, b_3, c_3; a_4, b_4, c_4; (d''', a) = a_1, h, b, c$$

$$h^2abc, h^2c, + a, + b, + c, - h^2ab, c, - h^2bc, a, - h^2ca, b, - 1 = \Delta$$

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

$$\Delta = (a_1-1)(b_1-1)(c_1-1) = (h^2abc - 1)a_1b_1c_1 - \{h^2a-1\}b_1c_1 + \{h^2b-1\}c_1a_1 + \{h^2c-1\}a_1b_1\}$$

$$\Delta = h^2abc(\alpha\beta\gamma + \beta\gamma + \gamma\alpha + \alpha\beta + \alpha + \beta + \gamma + 1) + \alpha + \beta + \gamma + 3 - h^2a(\beta\gamma + \beta + \gamma + 1) - h^2b(\gamma\alpha + \gamma + \alpha + 1) - h^2c(\alpha\beta + \alpha + \beta + 1) - 1$$

$$= h^2abc\alpha\beta\gamma + (h^2abc - h^2a)\beta\gamma + (h^2abc - h^2b)\gamma\alpha + (h^2abc - h^2c)\alpha\beta + (h^2abc + 1 - h^2b - h^2c)\alpha + (h^2abc + 1 - h^2a - h^2c)\beta + (h^2abc + 1 - h^2a - h^2b)\gamma + (h^2abc + 2 - h^2a - h^2b - h^2c)$$

$$= h^2abc\alpha\beta\gamma + h^2a(h^2b-1)\beta\gamma + h^2b(h^2c-1)\gamma\alpha + h^2c(h^2a-1)\alpha\beta + (h^2bc(a-1) + (h^2b-1)(h^2c-1))\alpha + (h^2ca(b-1) + (h^2c-1)(h^2a-1))\beta + (h^2ab(c-1) + (h^2a-1)(h^2b-1))\gamma +$$