SECTIO QUINTA

DE

FORMIS AEQUATIONIBUSQUE INDETERMINATIS SECUNDI GRADUS.

Disquisitionis propositum: formarum definitio et signum.

153.

In hac sectione imprimis de functionibus duarum indeterminatarum x, y, huius formae

$$axx+2bxy+cyy$$

ubi a, b, c sunt integri dati, tractabimus, quas *formas secundi gradus* sive simpliciter *formas* dicemus. Huic disquisitioni superstructur solutio problematis famosi, invenire omnes solutiones aequationis cuiuscunque indeterminatae secundi gradus duas incognitas implicantis, sive hae incognitae valores integros sive rationales tantum nancisci debeant. Problema hoc quidem iam ab ill. La Grange in omni generalitate est solutum, multaque insuper ad naturam *formarum* pertinentia tum ab hoc ipso magno geometra tum ab ill. Eulero partim primum inventa, partim, a Fermatio olim inventa, demonstrationibus munita. Sed nobis acriter formarum perquisitioni insistentibus tam multa nova se obtulerunt, ut totum argumentum ab integro resumere operae pretium duxerimus, eo magis, quod Virorum illorum inventa, multis locis sparsa, paucis innotuisse experti sumus; porro quod methodus per quam haec tractabimus nobis ad maximam partem est propria; tandem

quod nostra sine nova illorum expositione ne intelligi quidem possent. Nullum vero dubium nobis esse videtur, quin multa eaque egregia in hoc genere adhuc lateant, in quibus alii vires suas exercere possint. Caeterum quae ad veritatum insignium historiam pertinent, loco suo semper trademus.

Formam $axx+2bxy+cyy$, quando de indeterminatis x, y non agitur, ita designabimus, (a, b, c). Haec itaque expressio denotabit indefinite summam trium partium, producti numeri dati a in quadratum indeterminatae cuiuscunque; producti duplicati numeri b in hanc indeterminatam in aliam indeterminatam; producti numeri c in quadratum huius secundae indeterminatae. *Ex. gr.* $(1, 0, 2)$ exprimet summam quadrati et quadrati duplicati. Caeterum, quamvis formae (a, b, c) et (c, b, a) idem designent, si ad *partes ipsas* tantum respicimus, tamen different si insuper ad partium *ordinem* attendimus: quare sedulo eas in posterum distinguemus; quid vero inde lucremur in sequentibus sufficienter patebit.

Numerorum repraesentatio; determinans.

154.

Numerum aliquem datum per formam datam *repraesentari* dicemus, si formae indeterminatis tales valores integri tribuuntur, ut ipsius valor numero dato fiat aequalis. Hic habebimus sequens

THEOREMA. *Si numerus M ita per formam (a, b, c) repraesentari potest, ut indeterminatarum valores, per quos hoc efficitur, inter se sint primi: erit $bb-ac$ residuum quadraticum numeri M.*

Dem. Sint valores indeterminatarum m, n, scilicet

$$amm+2bmn+cnn = M$$

accipianturque numeri μ, ν ita ut sit $\mu m+\nu n = 1$ (art. 40). Tum per evolutionem facile probatur esse

$$(amm+2bmn+cnn)(a\nu\nu-2b\mu\nu+c\mu\mu) = (\mu(mb+nc)-\nu(ma+nb))^2-(bb-ac)(m\mu+n\nu)^2$$

sive

$$M(a\nu\nu-2b\mu\nu+c\mu\mu) = (\mu(mb+nc)-\nu(ma+nb))^2-(bb-ac)$$

Quare erit

$$bb-ac \equiv (\mu(mb+nc)-\nu(ma+nb))^2 \pmod{M}$$

i. e. $bb-ac$ residuum quadraticum ipsius M.

Numerum $bb-ac$, a cuius indole proprietates formae (a,b,c) imprimis pendere in sequentibus docebimus, *determinantem* huius formae vocabimus.

Valores expr. $\sqrt{(bb-ac)}\,(mod.\,M)$ *ad quos repraesentatio numeri* M *per formam* (a,b,c) *pertinet.*

155.

Erit itaque

$$\mu(mb+nc)-\nu(ma+nb)$$

valor expressionis

$$\sqrt{(bb-ac)}\,(\mathrm{mod.}\,M)$$

Constat autem, numeros μ,ν infinitis modis ita determinari posse ut sit $\mu m+\nu n=1$, unde alii aliique valores illius expressionis prodibunt, qui quem nexum inter se habeant videamus. Sit non modo $\mu m+\nu n=1$, sed etiam $\mu' m+\nu' n=1$, ponaturque

$$\mu(mb+nc)-\nu(ma+nb)=v,\quad \mu'(mb+nc)-\nu'(ma+nb)=v'$$

Multiplicando aequationem $\mu m+\nu n=1$ per μ', alteram $\mu' m+\nu' n=1$ per μ, et subtrahendo fit $\mu'-\mu=n(\mu'\nu-\mu\nu')$ similiterque multiplicando illam per ν', hanc per ν, fit subtrahendo $\nu'-\nu=m(\mu\nu'-\mu'\nu)$. Hinc statim prodit

$$v'-v=(\mu'\nu-\mu\nu')(amm+2bmn+cnn)=(\mu'\nu-\mu\nu')M$$

sive $v'\equiv v\,(\mathrm{mod.}\,M)$. Quomodocunque igitur μ,ν determinentur, formula $\mu(mb+nc)-\nu(ma+nb)$ valores *diversos* (*i.e.* incongruos) expressionis $\sqrt{(bb-ac)}$ $(\mathrm{mod.}\,M)$ dare nequit. Si itaque v est valor quicunque illius formulae: repraesentationem numeri M per formam $axx+2bxy+cyy$ eam ubi $x=m$, $y=n$, *pertinere* dicemus *ad valorem* v *expressionis* $\sqrt{(bb-ac)}\,(mod.\,M)$. Ceterum facile ostendi potest, si valor formulae illius aliquis sit v atque $v'\equiv v\,(\mathrm{mod.}\,M)$, loco numerorum μ,ν, qui dant v, alios μ',ν' accipi posse, qui dent v'. Scilicet faciendo

$$\mu'=\mu+\frac{n(v'-v)}{M},\quad \nu'=\nu-\frac{m(v'-v)}{M}$$

fiet

$$\mu' m+\nu' n=\mu m+\nu n=1$$

valor autem formulae ex μ',ν' prodiens superabit valorem ex μ,ν prodeuntem quantitate $(\mu'\nu-\mu\nu')M$, quae fit $=(\mu m+\nu n)(v'-v)=v'-v$, sive valor ille erit $=v'$.

156.

Si duae repraesentationes eiusdem numeri M per eandem formam (a,b,c) habentur, in quibus indeterminatae valores inter se primos habent: hae vel ad eundem valorem expr. $\sqrt{(bb-ac)}\,(\mathrm{mod.}\,M)$ pertinere possunt vel ad diversos. Sit

$$M=amm+2bmn+cnn=am'm'+2bm'n'+cn'n'$$

atque

$$\mu m+\nu n=1,\quad \mu' m'+\nu' n'=1$$

patetque si fuerit

$$\mu(mb+nc)-\nu(ma+nb)\equiv\mu'(m'b+n'c)-\nu'(m'a+n'b)\pmod{M}$$

congruentiam semper manere, quicunque alii valores idonei pro μ,ν; μ',ν' accipiantur, in quo casu utramque repraesentationem ad *eundem* valorem expr. $\sqrt{(bb-ac)}\,(\mathrm{mod.}\,M)$ pertinere dicemus; si vero congruentia pro ullis valoribus ipsorum μ,ν; μ',ν' locum non habet, pro nullis locum habebit, repraesentationesque ad valores *diversos* pertinebunt. Si vero

$$\mu(mb+nc)-\nu(ma+nb)\equiv-(\mu'(m'b+n'c)-\nu'(m'a+n'b))$$

repraesentationes ad valores *oppositos* expr. $\sqrt{(bb-ac)}$ pertinere dicentur. Omnibus hisce denominationibus etiam utemur, quando de pluribus repraesentationibus eiusdem numeri per formas *diversas*, sed quae eundem determinantem habent, agitur.

Ex. Sit forma proposita haec $(3,7,-8)$ cuius determinans $=73$. Per hanc formam habentur repraesentationes numeri 57 hae

$$3.13^2+14.13.25-8.25^2;\quad 3.5^2+14.5.9-8.9^2$$

Pro prima poni potest $\mu=2$, $\nu=-1$, unde prodit valor expr. $\sqrt{73}\,(\mathrm{mod.}\,57)$ ad quam repr. pertinet

$$=2(13.7-25.8)+(13.3+25.7)=-4$$

Simili modo repraesentatio secunda pertinere invenitur, faciendo $\mu = 2$, $\nu = -1$, ad valorem $+4$. Quare ambae repraesentationes ad valores oppositos pertinent.

Antequam ulterius progredimur, observamus, formas quarum determinans $= 0$ ab investigationibus sequentibus prorsus exclusas esse, quippe quae theorematum concinnitatem tantummodo turbarent, adeoque tractationem peculiarem postulent.

Forma aliam implicans, sive sub alia contenta; transformatio, propria et impropria.

157.

Si forma F, cuius indeterminatae sunt x, y, in aliam F', cuius indeterminatae sunt x', y', per substitutiones tales

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

transmutari potest, ita ut $\alpha, \beta, \gamma, \delta$ sint integri: priorem *implicare* posteriorem, sive posteriorem *sub priori contentam esse* dicemus. Sit forma F haec

$$axx + 2bxy + cyy$$

forma F' vero haec

$$a'x'x' + 2b'x'y' + c'y'y'$$

habebunturque sequentes tres aequationes:

$$\begin{aligned} a' &= a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta\beta + 2b\beta\delta + c\delta\delta \end{aligned}$$

Multiplicando aequationem secundam per se ipsam, primam per tertiam, et subtrahendo fit deletis partibus se destruentibus

$$b'b' - a'c' = (bb - ac)(\alpha\delta - \beta\gamma)^2$$

Unde sequitur determinantem formae F' per determinantem formae F divisibilem et quotientem esse quadratum; manifesto igitur hi determinantes *eadem signa* habebunt. Quodsi itaque insuper forma F'' per similem substitutionem in formam F transmutari potest, *i. e.* si tum F' sub F, tum F sub F' contenta est,

formarum determinantes erunt aequales*) atque $(\alpha\delta - \beta\gamma)^2 = 1$. In hoc casu formas *aequivalentes* dicemus. Quare ad formarum aequivalentiam aequalitas determinantium est conditio necessaria, licet illa ex hac sola minime sequatur. — Substitutionem $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ vocabimus *transformationem propriam*, si $\alpha\delta - \beta\gamma$ est numerus positivus, *impropriam*, si $\alpha\delta - \beta\gamma$ est negativus; formam F' *proprie* aut *improprie* sub forma F contentam esse dicemus, si F per transformationem propriam aut impropriam in formam F' transmutari potest. Si itaque formae F, F' sunt aequivalentes, erit $(\alpha\delta - \beta\gamma)^2 = 1$, adeoque si transformatio est propria, $\alpha\delta - \beta\gamma = +1$, si est impropria, $= -1$. — Si plures transformationes simul sunt propriae, aut simul impropriae, *similes* eas dicemus; propriam contra et impropriam *dissimiles*.

Aequivalentia, propria et impropria.

158.

Si formarum F, F' determinantes sunt aequales atque F' sub F contenta: etiam F sub F' contenta erit et quidem proprie vel improprie prout F' sub F proprie vel improprie continetur. Transeat F in F' ponendo

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

transibitque F' in F ponendo

$$x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y$$

Patet enim per hanc substitutionem ex F' fieri idem, quod fiat ex F ponendo

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \quad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$$

sive

$$x = (\alpha\delta - \beta\gamma)x, \quad y = (\alpha\delta - \beta\gamma)y$$

Hinc vero manifesto ex F fit $(\alpha\delta - \beta\gamma)^2 F$ *i. e.* rursus F (art. praec.). Perspicuum autem est, transformationem posteriorem esse propriam vel impropriam, prout prior sit propria vel impropria.

Si tum F' sub F, tum F sub F' *proprie* continetur, formas *proprie aequi-*

*) Manifestum est ex analysi praecedente hanc propositionem etiam ad formas quarum determinans $= 0$, patere. Sed aequatio $(\alpha\delta - \beta\gamma)^2 = 1$ ad hunc casum non est extendenda.

valentes, si illae sub invicem improprie, vocabimus *improprie aequivalentes*. — Ceterum usus harum distinctionum mox innotescet.

Exempl. Forma $2xx - 8xy + 3yy$ per substitutiones $x = 2x' + y'$, $y = 3x' + 2y'$ transit in formam $-13x'x' - 12x'y' - 2y'y'$, haec vero in illam factis $x' = 2x - y$, $y' = -3x + 2y$. Quare formae $(2, -4, 3)$, $(-13, -6, -2)$ erunt *proprie aequivalentes*.

Problemata quae tractare iam aggrediemur sunt haec: I. Propositis duabus formis quibuscunque eundem determinantem habentibus, investigare utrum sint aequivalentes necne, utrum proprie aut improprie aut utroque modo, nam etiam hoc fieri potest. Quando vero determinantes inaequales habent, annon saltem altera alteram implicet, proprie vel improprie vel utroque modo. Denique invenire omnes transformationes alterius in alteram, tam proprias quam improprias. II. Proposita forma quacunque, invenire utrum numerus datus per eam repraesentari possit omnesque repraesentationes assignare. Sed quoniam formae determinantis negativi hic aliam methodum requirunt quam formae determinantis positivi, primo trademus ea quae utrisque sunt communia, tum vero formas cuiusvis generis seorsim considerabimus.

Formae oppositae.

159.

Si forma F formam F' implicat, haec vero formam F'', forma F etiam formam F'' implicabit.

Sint indeterminatae formarum F, F', F'' respective x, y; x', y'; x'', y'' transeatque F in F' ponendo

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

F' in F'' ponendo

$$x' = \alpha' x'' + \beta' y'', \quad y' = \gamma' x'' + \delta' y''$$

patetque, F in F'' transmutatum iri ponendo

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y''), \quad y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

sive

$$x = (\alpha\alpha' + \beta\gamma')x'' + (\alpha\beta' + \beta\delta')y'', \quad y = (\gamma\alpha' + \delta\gamma')x'' + (\gamma\beta' + \delta\delta')y''$$

Quare F ipsam F'' implicabit.

Quia

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

adeoque positivus, si tum $\alpha\delta - \beta\gamma$ tum $\alpha'\delta' - \beta'\gamma'$ positivus aut uterque negativus, negativus vero si alter horum numerorum positivus alter negativus: forma F formam F'' *proprie* implicabit, si F ipsam F' et F' ipsam F'' eodem modo implicant, *improprie* si diverso.

Hinc sequitur, si quotcunque formae habeantur F, F', F'', F''' etc., quarum quaevis sequentem implicet, primam implicaturam esse ultimam, et quidem *proprie*, si multitudo formarum, quae sequentem suam improprie implicant, fuerit par, *improprie* si multitudo haec impar.

Si forma F formae F' est aequivalens, formaque F' formae F'': forma F formae F'' aequivalens erit, et quidem proprie, si forma F formae F' eodem modo aequivalet ut forma F' formae F'', improprie, si diverso.

Quia enim formae F, F', his F', F'', respective sunt aequivalentes, tum illae has resp. implicabunt, adeoque F ipsam F'', tum hae illas. Quare F, F'' aequivalentes erunt. Ex praec. vero sequitur, F ipsam F'' proprie vel improprie implicare, prout F ipsi F' et F' ipsi F'' eodem modo vel diverso sint aequivalentes, ut et F'' ipsam F: quare in priori casu F, F'' proprie, in posteriori improprie aequivalentes erunt.

Formae $(a, -b, c)$, (c, b, a), $(c, -b, a)$ formae (a, b, c) aequivalent, et quidem duae priores improprie, ultima proprie.

Nam $axx + 2bxy + cyy$ transit in $ax'x' - 2bx'y' + cy'y'$, ponendo $x = x' + 0.y'$, $y = 0.x' - y'$, quae transformatio est impropria propter $1 \times -1 - 0.0 = -1$; in formam $cx'x' + 2bx'y' + ay'y'$ vero per transformationem impropriam $x = 0.x' + y'$, $y = x' + 0.y'$; et in formam $cx'x' - 2bx'y' + ay'y'$ per propriam $x = 0.x' - y'$, $y = x' + 0.y'$.

Hinc manifestum est, quamvis formam, formae (a, b, c) aequivalentem, vel ipsi, vel formae $(a, -b, c)$ *proprie* aequivalere; similiterque, si quae forma formam (a, b, c) implicet aut sub ipsa contineatur, eam vel formam (a, b, c) vel formam $(a, -b, c)$ *proprie* implicare, aut sub alterutra *proprie* contineri. Formas (a, b, c), $(a, -b, c)$ *oppositas* vocabimus.

Formae contiguae.

160.

Si formae (a, b, c), (a', b', c') eundem determinantem habent, insuperque est $c = a'$ et $b \equiv -b' \pmod{c}$, sive $b + b' \equiv 0 \pmod{c}$, formas has *contiguas* dicemus, et quidem, quando determinatione accuratiori opus est, priorem posteriori *a parte prima*, posteriorem priori *a parte ultima* contiguam dicemus.

Ita *ex. gr.* forma $(7, 3, 2)$ formae $(3, 1, 3)$ a parte ultima contigua, forma $(3, 1, 3)$ oppositae suae $(3, -1, 3)$ ab utraque parte.

Formae contiguae semper sunt proprie aequivalentes. Nam forma $axx + 2bxy + cyy$ transit in formam contiguam $cx'x' + 2b'x'y' + c'y'y'$ per substitutionem $x = -y'$, $y = x' + \frac{b+b'}{c} y'$ (quae est propria ob $0 \times \frac{b+b'}{c} - 1 \times -1 = 1$), uti per evolutionem adiumento aequationis $bb - ac = b'b' - cc'$ facile probatur; $\frac{b+b'}{c}$ vero per hyp. est integer. — Ceterum hae definitiones et conclusiones locum non habent, si $c = a' = 0$. Hic vero casus occurrere nequit, nisi in formis quarum determinans est numerus quadratus.

Formae (a, b, c), (a', b', c') proprie aequivalentes sunt, si $a = a'$, $b \equiv b' \pmod{a}$. Forma enim (a, b, c) formae $(c, -b, a)$ proprie aequivalet (art. praec.), haec vero formae (a', b', c') a parte prima contigua erit.

Divisores communes coefficientium formarum.

161.

Si forma (a, b, c) formam (a', b', c') implicat, quivis divisor communis numerorum a, b, c etiam numeros a', b', c' metietur, et quivis divisor communis numerorum $a, 2b, c$ ipsos $a', 2b', c'$.

Si enim forma $axx + 2bxy + cyy$ per substitutiones $x = \alpha x' + \vec{\alpha} y'$, $y = \gamma x' + \vec{\gamma} y'$ in formam $a'x'x' + 2b'x'y' + c'y'y'$ transit: habebuntur hae aequationes

$$\begin{gathered} a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a' \\ a\alpha\vec{\alpha} + b(\alpha\vec{\gamma} + \vec{\alpha}\gamma) + c\gamma\vec{\gamma} = b' \\ a\vec{\alpha}\vec{\alpha} + 2b\vec{\alpha}\vec{\gamma} + c\vec{\gamma}\vec{\gamma} = c' \end{gathered}$$

unde propositio statim sequitur (pro parte secunda propos. loco aequationis secundae hanc adhibendo $2a\alpha\vec{\alpha} + 2b(\alpha\vec{\gamma} + \vec{\alpha}\gamma) + 2c\gamma\vec{\gamma} = 2b'$).

Hinc sequitur maximum divisorem communem numerorum $a, b\,(2b), c$ simul metiri divisorem communem maximum numerorum $a', b'\,(2b'), c'$. Quodsi igitur insuper forma (a', b', c') formam (a, b, c) implicat, *i. e.* formae sunt aequivalentes, divisor communis maximus numerorum $a, b\,(2b), c$, divisori communi maximo numerorum $a', b'\,(2b'), c'$ aequalis erit, quoniam tum ille hunc metiri debet, tum hic illum. Si itaque in hoc casu $a, b\,(2b), c$ divisorem communem non habent, *i. e.* si maximus $= 1$, etiam $a', b'\,(2b'), c'$ divisorem communem non habebunt.

Nexus omnium transformationum similium formae datae in formam datam.

162.

Problema. *Si forma* $AXX + 2BXY + CYY \ldots F$

formam $axx + 2bxy + cyy \ldots f$

implicat, atque transformatio aliqua illius in hanc est data: ex hac omnes reliquas transformationes ipsi similes deducere.

Solutio. Sit transformatio data haec $X = \alpha x + \vec{\alpha} y$, $Y = \gamma x + \vec{\gamma} y$, ponamusque primo aliam huic similem datam esse $X = \alpha' x + \vec{\alpha}' y$, $Y = \gamma' x + \vec{\gamma}' y$, ut quid inde sequatur investigemus. Tum positis determinantibus formarum $F, f, = D, d$, atque $\alpha\vec{\gamma} - \vec{\alpha}\gamma = e$, $\alpha'\vec{\gamma}' - \vec{\alpha}'\gamma' = e'$, erit (art. 157) $d = Dee = De'e'$, et quum ex hyp. e, e' eadem signa habeant, $e = e'$. Habebuntur autem sequentes sex aequationes:

$$\begin{gathered} A\alpha\alpha + 2B\alpha\gamma + C\gamma\gamma = a \quad \ldots\ldots [1] \\ A\alpha'\alpha' + 2B\alpha'\gamma' + C\gamma'\gamma' = a \quad \ldots\ldots [2] \\ A\alpha\vec{\alpha} + B(\alpha\vec{\gamma} + \vec{\alpha}\gamma) + C\gamma\vec{\gamma} = b \quad \ldots\ldots [3] \\ A\alpha'\vec{\alpha}' + B(\alpha'\vec{\gamma}' + \vec{\alpha}'\gamma') + C\gamma'\vec{\gamma}' = b \quad \ldots\ldots [4] \\ A\vec{\alpha}\vec{\alpha} + 2B\vec{\alpha}\vec{\gamma} + C\vec{\gamma}\vec{\gamma} = c \quad \ldots\ldots [5] \\ A\vec{\alpha}'\vec{\alpha}' + 2B\vec{\alpha}'\vec{\gamma}' + C\vec{\gamma}'\vec{\gamma}' = c \quad \ldots\ldots [6] \end{gathered}$$

Si brevitatis gratia numeros

$$\begin{gathered} A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma' \\ A(\alpha\vec{\alpha}' + \vec{\alpha}\alpha') + B(\alpha\vec{\gamma}' + \vec{\alpha}\gamma' + \gamma\vec{\alpha}' + \vec{\gamma}\alpha') + C(\gamma\vec{\gamma}' + \vec{\gamma}\gamma') \\ A\vec{\alpha}\vec{\alpha}' + B(\vec{\alpha}\vec{\gamma}' + \vec{\gamma}\vec{\alpha}') + C\vec{\gamma}\vec{\gamma}' \end{gathered}$$

per $a', 2b', c'$ designamus, ex aequ. praecc. sequentes novas deducemus *):

$$a'a' - D(\alpha\gamma' - \gamma\alpha')^2 = aa \quad [7]$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab \quad [8]$$
$$4b'b' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee') = 2bb + 2ac$$

unde fit, addendo $2Dee' = 2d = 2bb - 2ac$,

$$4b'b' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4bb \quad [9]$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = bb$$

unde subtrahendo $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = bb - ac$ fit

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac \quad [10]$$
$$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc \quad [11]$$
$$c'c' - D(\beta\delta' - \delta\beta')^2 = cc \quad [12]$$

Ponamus iam, divisorem communem maximum numerorum $a, 2b, c$ esse m numerosque $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ita determinatos, ut fiat

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$$

(art. 40); multiplicentur aequationes 7, 8, 9, 10, 11, 12 resp. per $\mathfrak{AA}, 2\mathfrak{AB}, \mathfrak{BB}, 2\mathfrak{AC}, 2\mathfrak{BC}, \mathfrak{CC}$ summenturque producta. Quodsi iam brevitatis caussa ponimus

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T \quad [13]$$
$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') + \mathfrak{C}(\beta\delta' - \delta\beta') = U \quad [14]$$

ubi T, U manifesto erunt integri, prodibit

$$TT - DUU = mm$$

Deducti itaque sumus ad hanc conclusionem elegantem, *ex binis quibuscunque transformationibus similibus formae F in f sequi solutionem aequationis indeterminatae $tt - Duu = mm$, in integris*, scilicet $t = T$, $u = U$. Ceterum quum in

*) Origo harum aequationum haec est: 7 fit ex 1.2 (*i. e.* si aequatio (1) in aequationem (2) multiplicatur, sive potius, si illius pars prior in partem priorem huius multiplicatur, illiusque pars posterior in posteriorem huius, productaque aequalia ponuntur); 8 ex $1.4 + 2.3$; sequens quae non est numerata ex $1.6 + 2.5 + 3.4 + 3.4$; sequens non numerata ex 3.4; 11 ex $3.6 + 4.5$; 12 ex 5.6. Simili designatione etiam in sequentibus semper utemur. Evolutionem vero lectoribus relinquere debemus.

ratiociniis nostris non supposuerimus, transformationes esse *diversas: una* adeo transformatio bis considerata solutionem praebere debet. Tum vero fit propter $\alpha' = \alpha$, $\beta' = \beta$ etc. $a' = a$, $b' = b$, $c' = c$, adeoque $T = m$, $U = 0$, quae solutio per se est obvia.

Iam primam transformationem solutionemque aequationis indeterminatae tanquam cognitas consideremus, et quomodo hinc altera transformatio deduci possit, sive quomodo $\alpha', \beta', \gamma', \delta'$, ab his $\alpha, \beta, \gamma, \delta$, T, U pendeant, investigemus. Ad hunc finem multiplicamus primo aequationem [1] per $\delta\alpha' - \beta\gamma'$, [2] per $\alpha\delta' - \gamma\beta'$, [3] per $\alpha\gamma' - \gamma\alpha'$, [4] per $\gamma\alpha' - \alpha\gamma'$, addimusque producta, unde prodibit

$$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a \quad [15]$$

Simili modo fit ex

$$(\delta\beta' - \beta\delta')([1] - [2]) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')([3] + [4]) + (\alpha\gamma' - \gamma\alpha')([5] + [6])$$

$$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b \quad [16]$$

Denique ex $(\delta\beta' - \beta\delta')([3] - [4]) + (\alpha\delta' - \gamma\beta')[5] + (\delta\alpha' - \beta\gamma')[6]$ prodit:

$$(e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c \quad [17]$$

Substituendo hos valores (15, 16, 17) in 13 fit

$$(e + e')T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)$$

sive

$$2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')m \quad [18]$$

unde T multo facilius deduci potest, quam ex [13]. — Combinando hanc aequationem cum 15, 16, 17 obtinetur $ma' = Ta$, $2mb' = 2Tb$, $mc' = Tc$. Quos valores ipsorum $a', 2b', c'$ in aequ. 7—12 substituendo et loco ipsius TT scribendo $mm + DUU$, transeunt illae post mutationes debitas in has

$$(\alpha\gamma' - \gamma\alpha')^2 mm = aaUU$$
$$(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')mm = 2abUU$$

$$(\alpha\delta' + \delta\gamma' - \gamma\delta' - \delta\alpha')^2 mm = 4bbUU$$
$$(\alpha\gamma' - \gamma\alpha')(\delta\delta' - \delta\delta')mm = acUU$$
$$(\alpha\delta' + \delta\gamma' - \gamma\delta' - \delta\alpha')(\delta\delta' - \delta\delta')mm = 2beUU$$
$$(\delta\delta' - \delta\delta')^2 mm = ccUU$$

Hinc adiumento aequationis [14] et huius $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, facile deducitur (multiplicando primam, secundam, quartam; secundam, tertiam, quintam; quartam, quintam, sextam, resp. per $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ addendoque producta):

$$(\alpha\gamma' - \gamma\alpha')Umm = maUU$$
$$(\alpha\delta' + \delta\gamma' - \gamma\delta' - \delta\alpha')Umm = 2mbUU$$
$$(\delta\delta' - \delta\delta')Umm = mcUU$$

atque hinc, dividendo per mU *)

$$aU = (\alpha\gamma' - \gamma\alpha')m \quad \ldots\ldots\ldots\ldots [19]$$
$$2bU = (\alpha\delta' + \delta\gamma' - \gamma\delta - \delta\alpha')m \quad \ldots\ldots [20]$$
$$cU = (\delta\delta' - \delta\delta')m \quad \ldots\ldots\ldots\ldots [21]$$

ex quarum aequationum aliqua U multo facilius quam ex [14] deduci potest. — Simul hinc colligitur, quomodocunque $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ determinentur (quod infinitis modis diversis fieri potest), tum T tum U eundem valorem adipisci.

Iam si aequatio 18 multiplicatur per α, 19 per 2δ, 20 per $-\alpha$, fit per additionem

$$2\alpha eT + 2(\delta a - \alpha b)U = 2(\alpha\delta - \delta\gamma)\alpha' m = 2e\alpha' m$$

Simili modo fit ex δ [18] $+ \delta$ [20] $- 2\alpha$ [21]

$$2\delta eT + 2(\delta b - \alpha c)U = 2(\alpha\delta - \delta\gamma)\delta' m = 2e\delta' m$$

Porro ex γ [18] $+ 2\delta$ [19] $- \gamma$ [20] fit

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \delta\gamma)\gamma' m = 2e\gamma' m$$

Tandem ex δ [18] $+ \delta$ [20] $- 2\gamma$ [21] prodit

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \delta\gamma)\delta' m = 2e\delta' m$$

*) Hoc non liceret, si esset $U = 0$: tunc vero aequationum 19, 20, 21 veritas statim ex prima, tertia et sexta praecedentium sequeretur.

In quibus formulis, si pro a, b, c valores ex 1, 3, 5 substituuntur, fit

$$\alpha' m = \alpha T - (\alpha B + \gamma C)U$$
$$\delta' m = \delta T - (\delta B + \delta C)U$$
$$\gamma' m = \gamma T + (\alpha A + \gamma B)U$$
$$\delta' m = \delta T + (\delta A + \delta B)U \text{ *)}$$

Ex analysi praec. sequitur, nullam transformationem formae F in f propositae similem dari, quae non sit contenta sub formula

$$X = \tfrac{1}{m}(\alpha t - (\alpha B + \gamma C)u)x + \tfrac{1}{m}(\delta t - (\delta B + \delta C)u)y$$
$$Y = \tfrac{1}{m}(\gamma t + (\alpha A + \gamma B)u)x + \tfrac{1}{m}(\delta t + (\delta A + \delta B)u)y \quad \ldots\ldots (1)$$

designantibus t, u indefinite omnes numeros integros aequationi $tt - Duu = mm$ satisfacientes. Hinc vero concludere nondum possumus, omnes valores ipsorum t, u, aequationi illi satisfacientes, in formula (1) substitutos, transformationes idoneas praebere. At

1. Formam F per substitutionem, e quibusvis ipsorum t, u valoribus ortam, semper in formam f transmutari, per evolutionem confirmari facile potest adiumento aequationum 1, 3, 5 et huius $tt - Duu = mm$. Calculum prolixiorem quam difficiliorem brevitatis gratia supprimimus.

2. Quaevis transformatio ex formula deducta propositae erit similis. Namque

$$\tfrac{1}{m}(\alpha t - (\alpha B + \gamma C)u) \times \tfrac{1}{m}(\delta t + (\delta A + \delta B)u)$$
$$- \tfrac{1}{m}(\delta t - (\delta B + \delta C)u) \times \tfrac{1}{m}(\gamma t + (\alpha A + \gamma B)u)$$
$$= \tfrac{1}{mm}(\alpha\delta - \delta\gamma)(tt - Duu) = \alpha\delta - \delta\gamma$$

3. Si formae F, f determinantes inaequales habent, fieri potest, ut formula (1) pro quibusdam valoribus ipsorum t, u praebeat substitutiones, quae *fractiones* implicent, adeoque reiici debeant. Omnes vero reliquae erunt transformationes idoneae, aliaeque praeter ipsas non dabuntur.

4. Si vero formae F, f eundem determinantem habent adeoque sunt *aequivalentes*, formula (1) nullas transformationes quae fractiones implicent praebe-

*) Hinc facile deducitur
$$AeU = (\delta\gamma' - \gamma\delta')m$$
$$2BeU = (\alpha\delta' - \delta\alpha' + \gamma\delta' - \delta\gamma')m$$
$$CeU = (\delta\alpha' - \alpha\delta')m$$

bit, adeoque in hoc casu solutionem completam problematis exhibebit. Illud vero ita demonstramus.

Ex theoremate art. praec. sequitur in hocce casu, m simul fore divisorem communem numerorum $A, 2B, C$. Quoniam $tt - Duu = mm$, fit $tt - BBuu = mm - ACuu$, quare $tt - BBuu$ per mm divisibilis erit: hinc etiam a potiori $4tt - 4BBuu$ adeoque (quia $2B$ per m divisibilis) etiam $4tt$ per mm et proin $2t$ per m. Hinc $\frac{1}{m}(t + Bu)$, $\frac{1}{m}(t - Bu)$ erunt integri, et quidem (quoniam differentia inter ipsos $\frac{1}{m}Bu$ est par) aut uterque par aut uterque impar. Si uterque impar esset, etiam productum impar foret, quod tanquam quadruplum numeri $\frac{1}{mm}(tt - BBuu)$, quem integrum esse modo ostendimus, necessario par: quare hic casus est impossibilis, adeoque $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$ semper pares, unde $\frac{1}{m}(t + Bu)$, $\frac{1}{m}(t - Bu)$ erunt integri. Hinc vero nullo negotio deducitur, omnes quatuor coefficientes in (I) semper esse integros. *Q. E. D.*

Ex praecedentibus colligitur, si omnes solutiones aequationis $tt - Duu = mm$ habeantur, omnes transformationes formae (A, B, C) in (a, b, c) transf. datae similes inde derivari. Illas vero in sequentibus invenire docebimus. Hic tantummodo observamus multitudinem solutionum semper esse finitam, quando D sit negativus, aut positivus simulque quadratus: quando vero D positivus non quadratus, infinitam. Quando hic casus locum habet, simulque D non $= d$ (supra 3^0), disquiri insuper deberet, quomodo ii valores ipsorum t, u, qui substitutiones a fractionibus liberas, ab iis, qui fractas producunt, a priori dignosci possint. Sed pro hocce casu infra aliam methodum ab hoc incommodo liberam exponemus (art. 214).

Exempl. Forma $xx + 2yy$ per substitutionem propriam $x = 2x' + 7y'$, $y = x' + 5y'$ transit in formam $(6, 24, 99)$: desiderantur *omnes* transformationes propriae formae illius in hanc. Hic $D = -2$, $m = 3$, adeoque aequatio solvenda haec: $tt + 2uu = 9$. Huic sex modis diversis satisfit ponendo scilicet $t = 3, -3, 1, -1, 1, -1$; $u = 0, 0, 2, 2, -2, -2$ resp. Solutio tertia et sexta dant substitutiones in fractis, adeoque sunt reiiciendae; ex reliquis sequuntur quatuor substitutiones:

$$x = \begin{cases} 2x' + 7y' \\ -2x' - 7y' \\ -2x' - 9y' \\ 2x' + 9y' \end{cases} \qquad y = \begin{cases} x' + 5y' \\ -x' - 5y' \\ x' + 3y' \\ -x' - 3y' \end{cases}$$

(quarum prima est proposita).

Formae ancipites.

163.

Iam supra obiter diximus fieri posse ut forma aliqua, F, aliam, F', tam proprie quam improprie implicet. Perspicuum est hoc evenire, si inter formas F, F' alia G interponi possit, ita ut F ipsam G, G ipsam F' implicet, formaque G ita sit comparata, ut sibi ipsa sit improprie aequivalens. Si enim F ipsam G proprie vel improprie implicare supponitur: quum G ipsam G improprie implicet, F ipsam G improprie vel proprie (resp.) implicabit, adeoque in utroque casu, tam proprie quam improprie (art. 159). Eodem modo hinc deducitur, quomodocunque G ipsam F' implicare supponatur, F semper ipsam F' tum proprie tum improprie implicare debere. — Tales vero formas dari, quae sibi ipsae sint improprie aequivalentes, videtur in casu maxime obvio, ubi formae terminus medius $= 0$. Talis enim forma sibi ipsa erit opposita (art. 159) adeoque improprie aequivalens. Generalius quaevis forma (a, b, c) hac proprietate est praedita, in qua $2b$ per a est divisibilis. Huic enim forma (c, b, a) a parte prima erit contigua (art. 160) adeoque proprie aequivalens: sed (c, b, a) per art. 159 formae (a, b, c) improprie aequivalet: quare (a, b, c) sibi ipsa improprie aequivalebit. Tales formas (a, b, c) in quibus $2b$ per a est divisibilis, *ancipites* vocabimus. Habebimus itaque theorema hoc:

Forma F, aliam formam F' tum proprie tum improprie implicabit, si forma anceps inveniri potest sub F contenta ipsam F' vero implicans. Sed haec propositio etiam converti potest: scilicet

Theorema circa casum ubi forma sub alia simul proprie et improprie contenta est.

164.

THEOREMA. *Si forma* $Axx + 2Bxy + Cyy \quad \ldots \quad (F)$

formam $A'x'x' + 2B'x'y' + C'y'y' \quad \ldots \quad (F')$

tum proprie tum improprie implicat: forma anceps inveniri potest, sub F contenta formamque F' implicans.

Ponamus, formam F transire in formam F' tum per substitutionem

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

tum per hanc illi dissimilem

$$x = \alpha' x' + \vec{\alpha}' x', \quad y = \gamma' x' + \vec{\gamma}' y'$$

Tum designatis numeris $\alpha\vec{\delta} - \vec{\alpha}\gamma$, $\alpha'\vec{\delta}' - \vec{\alpha}'\gamma'$ per e, e', erit $BB' - AC = ee'(BB - AC) = e\acute{e}'(BB - AC)$; hinc $ee = e'\acute{e}'$, et, quia per hyp. e, e' signa opposita habent, $e = -e'$ sive $e + e' = 0$. Iam patet si in F' pro x' substituatur $\vec{\delta}' x'' - \vec{\alpha}' y''$, et pro y', $-\gamma' x'' + \alpha' y''$, eandem formam esse prodituram ac si in F scribatur

aut 1) pro x $\quad \alpha(\vec{\delta}' x'' - \vec{\alpha}' y'') + \vec{\alpha}(-\gamma' x'' + \alpha' y'')$

i. e. $\quad (\alpha\vec{\delta}' - \vec{\alpha}'\gamma') x'' + (\vec{\alpha}'\alpha - \alpha\vec{\alpha}') y''$

et pro y $\quad \gamma(\vec{\delta}' x'' - \vec{\alpha}' y'') + \vec{\delta}(-\gamma' x'' + \alpha' y'')$

i. e. $\quad (\gamma\vec{\delta}' - \vec{\delta}\gamma') x'' + (\vec{\delta}\alpha' - \gamma\vec{\alpha}') y''$

aut 2) pro x $\quad \alpha'(\vec{\delta}' x'' - \vec{\alpha}' y'') + \vec{\alpha}'(-\gamma' x'' + \alpha' y'')$ *i. e.* $e' x''$

et pro y $\quad \gamma'(\vec{\delta}' x'' - \vec{\alpha}' y'') + \vec{\delta}'(-\gamma' x'' + \alpha' y'')$ *i. e.* $\acute{e} y''$

Designatis itaque numeris $\alpha\vec{\delta}' + \vec{\alpha}\gamma'$, $\vec{\alpha}\alpha' - \alpha\vec{\alpha}'$, $\gamma\vec{\delta}' - \vec{\delta}\gamma'$, $\vec{\delta}\alpha' - \gamma\vec{\alpha}'$ per a, b, c, d: forma F per duas substitutiones

$$x = ax'' + by'', \quad y = cx'' + dy''; \quad x = \acute{e}x'', \; y = \acute{e}y''$$

in eandem formam transmutabitur, unde obtinemus tres aequationes sequentes:

$$Aaa + 2Bac + Ccc = A\acute{e}\acute{e} \quad \ldots\ldots\ldots [1]$$
$$Aab + B(ad + bc) + Ccd = B\acute{e}\acute{e} \quad \ldots\ldots [2]$$
$$Abb + 2Bbd + Cdd = C\acute{e}\acute{e} \quad \ldots\ldots\ldots [3]$$

Ex valoribus ipsorum a, b, c, d autem invenitur

$$ad - bc = ee' = -ee = -\acute{e}\acute{e} \quad \ldots\ldots [4]$$

Hinc fit ex $d[1] - c[2]$

$$(Aa + Bc)(ad - bc) = (Ad - Bc)\acute{e}\acute{e}$$

adeoque

$$A(a + d) = 0$$

Porro ex $(a+d)[2] - b[1] - c[3]$ fit

$$(Ab + B(a+d) + Cc)(ad - bc) = (-Ab + B(a+d) - Cc)\acute{e}\acute{e}$$

adeoque

$$B(a+d) = 0$$

Denique ex $a[3] - b[2]$ fit

$$(Bb + Cd)(ad - bc) = (-Bb + Ca)\acute{e}\acute{e}$$

adeoque

$$C(a+d) = 0$$

Quare quum omnes A, B, C nequeant esse $= 0$, necessario erit $a + d = 0$ sive $a = -d$.

Ex $a[2] - b[1]$ fit

$$(Ba + Cc)(ad - bc) = (Ba - Ab)\acute{e}\acute{e}$$

unde

$$Ab - 2Ba - Cc = 0 \quad \ldots\ldots\ldots [5]$$

Ex aequationibus $e + e' = 0$, $a + d = 0$ sive

$$\alpha\vec{\delta} - \vec{\alpha}\gamma + \alpha'\vec{\delta}' - \vec{\alpha}'\gamma' = 0, \quad \alpha\vec{\delta}' - \vec{\alpha}\gamma' - \gamma\vec{\alpha}' + \vec{\delta}\alpha' = 0$$

sequitur $(\alpha + \alpha')(\vec{\delta} + \vec{\delta}') = (\vec{\alpha} + \vec{\alpha}')(\gamma + \gamma')$ sive

$$(\alpha + \alpha') : (\gamma + \gamma') = (\vec{\alpha} + \vec{\alpha}') : (\vec{\delta} + \vec{\delta}')$$

Sit rationi huic*) in numeris minimis aequalis ratio $m : n$, ita ut m, n inter se primi sint, accipianturque μ, ν ita ut fiat $\mu m + \nu n = 1$. Porro sit r div. comm. max. numerorum a, b, c; cuius quadratum propterea metietur ipsum $aa + bc$ sive $bc - ad$ sive ee; quare r etiam ipsum e metietur. His ita factis, si forma F per substitutionem

$$x = mt + \tfrac{\nu e}{r} u, \quad y = nt - \tfrac{\mu e}{r} u$$

in formam $Mtt + 2Ntu + Puu$ (G) transire supponitur, haec anceps erit formamque F' implicabit.

*) Si omnes $\alpha + \alpha'$, $\gamma + \gamma'$, $\vec{\alpha} + \vec{\alpha}'$, $\vec{\delta} + \vec{\delta}'$ essent $= 0$, ratio indeterminata foret, adeoque methodus non applicabilis. Sed exigua attentio docet, hoc cum suppositionibus nostris consistere non posse. Foret enim $\alpha\vec{\delta} - \vec{\alpha}\gamma = \alpha'\vec{\delta}' - \vec{\alpha}'\gamma'$ *i. e.* $e = e'$ adeoque, quia $e = -e'$, $e = e' = 0$. Hinc vero etiam $BB' - AC$ *i. e.* determinans formae F' fieret $= 0$, quales formas omnino exclusimus.

Dem. I. Quo pateat, formam G esse ancipitem, ostendemus esse

$$M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr$$

unde quia r ipsos a, b, c metitur $\frac{1}{r}(b\mu\mu - 2a\mu\nu - c\nu\nu)$ integer erit, adeoque $2N$ multiplum ipsius M. Erit autem

$$M = Amm + 2Bmn + Cnn, \quad Nr = (Am\nu - B(m\mu - n\nu) - Cn\mu)e \quad . \quad [6]$$

Porro per evolutionem facile confirmatur esse

$$2e + 2a = e - e' + a - d = (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma')$$

$$2b = (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta')$$

Hinc quoniam $m(\gamma + \gamma') = n(\alpha + \alpha')$, $m(\delta + \delta') = n(\beta + \beta')$ erit

$$m(2e + 2a) = -2nb \quad \text{sive}$$

$$me + ma + nb = 0 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad [7]$$

Eodem modo erit

$$2e - 2a = e - e' - a + d = (\alpha + \alpha')(\delta - \delta') - (\beta + \beta')(\gamma - \gamma')$$

$$2c = (\gamma - \gamma')(\delta + \delta') - (\gamma + \gamma')(\delta - \delta')$$

atque hinc $n(2e - 2a) = -2mc$ sive

$$ne - na + mc = 0 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad [8]$$

Iam si ad $mm(b\mu\mu - 2a\mu\nu - c\nu\nu)$ additur

$$(1 - m\mu - n\nu)(m\nu(e - a) + (m\mu + 1)b)$$
$$+ (me + ma + nb)(m\mu\nu + \nu) + (ne - na + mc)m\nu\nu$$

quod manifesto $= 0$, propter

$$1 - \mu m - \nu u = 0, \quad me + ma + nb = 0, \quad ne - na + mc = 0$$

prodit productis rite evolutis partibusque se destruentibus deletis, $2m\nu e + b$. Quare erit

$$mm(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2m\nu e + b \quad . \quad . \quad . \quad . \quad . \quad [9]$$

Eodem modo addendo ad $mn(b\mu\mu - 2a\mu\nu - c\nu\nu)$ haec:

$$(1 - m\mu - n\nu)((n\nu - m\mu)e - (1 + m\mu + n\nu)a)$$
$$- (me + ma + nb)m\mu\mu + (ne - na + mc)n\nu\nu$$

invenitur

$$mn(b\mu\mu - 2a\mu\nu - c\nu\nu) = (n\nu - m\mu)e - a \quad . \quad . \quad . \quad . \quad [10]$$

Denique addendo ad $nn(b\mu\mu - 2a\mu\nu - c\nu\nu)$ haec:

$$(m\mu + n\nu - 1)(n\mu(e + a) + (n\nu + 1)c)$$
$$- (me + ma + nb)n\mu\mu - (ne - na + mc)(n\mu\nu + \mu)$$

fit

$$nn(b\mu\mu - 2a\mu\nu - c\nu\nu) = -2n\mu e - c \quad . \quad . \quad . \quad . \quad [11]$$

Iam ex 9, 10, 11, deducitur

$$(Amm + 2Bmn + Cnn)(b\mu\mu - 2a\mu\nu - c\nu\nu)$$
$$= 2e(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc$$

sive propter [6],

$$M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr. \quad Q.\ E.\ D.$$

II. Ut probetur, formam G implicare formam F', demonstrabimus, *primo* G transire in F' ponendo

$$t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y', \quad u = \tfrac{r}{g}(n\alpha - m\gamma)x' + \tfrac{r}{e}(n\beta - m\delta)y' \quad . \quad . \quad (S)$$

secundo $\frac{r}{g}(n\alpha - m\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ esse integros.

1. Quoniam F transit in G ponendo

$$x = mt + \tfrac{\nu e}{r}u, \quad y = nt - \tfrac{\mu e}{r}u$$

forma G per substitutionem (S) transmutabitur in eandem formam in quam F transformatur ponendo

$$x = m((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') + \nu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$
i. e. $$= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y' \quad \text{sive} \quad = \alpha x' + \beta y'$$
et $$y = n((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') - \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$
i. e. $$= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y' \quad \text{sive} \quad = \gamma x' + \delta y'$$

Per hanc vero substitutionem F transit in F': quare per substitutionem (S) etiam G transibit in F'.

2. Ex valoribus ipsorum e, b, d invenitur $\alpha' e + \gamma b - \alpha d = 0$, sive propter $d = -a$, $n\alpha' e + n\alpha a + n\gamma b = 0$; hinc ex [7], $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$ sive

$$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e \quad \ldots\ldots\ldots [12]$$

Porro fit $anb = -am(e+a)$, $\gamma mb = -m(\alpha' e + \alpha a)$ adeoque

$$(n\alpha - m\gamma)b = (\alpha' - \alpha)me \quad \ldots\ldots\ldots [13]$$

Denique fit $\gamma' e - \gamma a + \alpha c = 0$: hinc multiplicando per n, et pro na substituendo valorem ex [8] fit

$$(n\alpha - m\gamma)c = (\gamma - \gamma')ne \quad \ldots\ldots\ldots [14]$$

Simili modo eruitur $\mathfrak{G}' e + \delta b - \mathfrak{G} d = 0$, sive $n\mathfrak{G}' e + n\delta b + n\mathfrak{G} a = 0$, adeoque per [7], $n\mathfrak{G}' e + n\mathfrak{G} a = m\delta e + m\delta a$ sive

$$(n\mathfrak{G} - m\delta)a = (m\delta - n\mathfrak{G}')e \quad \ldots\ldots\ldots [15]$$

Porro fit $\mathfrak{G} nb = -\mathfrak{G} m(e+a)$, $\delta mb = -m(\mathfrak{G}' e + \mathfrak{G} a)$ adeoque

$$(n\mathfrak{G} - m\delta)b = (\mathfrak{G}' - \mathfrak{G})me \quad \ldots\ldots\ldots [16]$$

Tandem $\delta e - \delta a + \mathfrak{G} c = 0$: hinc multiplicando per n et substituendo pro na valorem ex [8] fit

$$(n\mathfrak{G} - m\delta)c = (\delta - \delta')ne \quad \ldots\ldots\ldots [17]$$

Iam quum divisor communis maximus numerorum a, b, c sit r, integri $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ita accipi possunt, ut fiat

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$$

Quo facto erit ex 12, 13, 14; 15, 16, 17

$$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n = \tfrac{r}{e}(n\alpha - m\gamma)$$
$$\mathfrak{A}(m\delta - n\mathfrak{G}') + \mathfrak{B}(\mathfrak{G}' - \mathfrak{G})m + \mathfrak{C}(\delta - \delta')n = \tfrac{r}{e}(n\mathfrak{G} - m\delta)$$

adeoque $\frac{r}{e}(n\alpha - n\gamma)$, $\frac{r}{e}(n\mathfrak{G} - m\delta)$ integri. *Q. E. D.*

165.

Ex. Forma $3xx + 14xy - 4yy$ in formam $-12x'x' - 18x'y' + 39y'y'$ transmutatur, tum proprie, ponendo

$$x = 4x' + 11y', \quad y = -x' - 2y'$$

tum improprie, ponendo

$$x = -74x' + 89y', \quad y = 15x' - 18y'$$

Hic igitur $\alpha + \alpha'$, $\mathfrak{G} + \mathfrak{G}'$, $\gamma + \gamma'$, $\delta + \delta'$ sunt $-70, 100, 14, -20$; est autem $-70 : 14 = 100 : -20 = 5 : -1$. Faciemus itaque $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. Numeri autem a, b, c inveniuntur $-237, -1170, 48$, quorum divisor communis maximus $= 3 = r$; denique fit $e = 3$. Hinc transformatio (S) haec erit, $x = 5t - u$, $y = -t$. Per quam forma $(3, 7, -4)$ transit in formam ancipitem $tt - 16tu + 3uu$.

Si formae F, F' sunt aequivalentes: forma G, sub F' contenta, etiam sub F' contenta erit. Sed quoniam eandem formam etiam implicat, ipsi aequivalens erit, et proin etiam formae F. In hoc igitur casu theorema ita enunciabitur:

Si F, F' tam proprie, quam improprie sunt aequivalentes: forma anceps utrique aequivalens inveniri poterit. — Ceterum in hoc casu $e = \pm 1$, adeoque etiam r. ipsum e metiens, $= 1$ erit.

Haec de formarum transformatione in genere sufficiant: transimus itaque ad considerationem *repraesentationum*.

Generalia de repraesentationibus numerorum per formas, earumque nexu cum transformationibus.

166.

Si forma F formam F' implicat: quicunque numerus per F' repraesentari potest, etiam per F poterit.

Sint indeterminatae formarum F, F' respective x, y; x', y', ponamusque numerum M per F' repraesentari faciendo $x' = m$, $y' = n$, formam F vero in F' transire per substitutionem

$$x = \alpha x' + \mathfrak{G} y', \quad y = \gamma x' + \delta y'$$

Tum manifestum est, si ponatur

$$x = \alpha m + \beta n, \quad y = \gamma m + \delta n$$

F transire in M.

Si M pluribus modis per formam F' repraesentari potest, e.g. etiam faciendo $x' = m'$, $y' = n'$: plures repraesentationes ipsius M per F inde sequentur. Si enim esset tum

$$\alpha m + \beta n = \alpha m' + \beta n' \quad \text{tum} \quad \gamma m + \delta n = \gamma m' + \delta n'$$

foret aut $\alpha\delta - \beta\gamma = 0$, adeoque etiam determinans formae $F = 0$ contra hyp., aut $m = m'$, $n = n'$. Hinc sequitur M ad minimum totidem modis diversis per F repraesentari posse quot per F'.

Si igitur tum F ipsam F', tum F' ipsam F implicat *i. e.* si F, F' sunt aequivalentes, numerusque M per alterutram repraesentari potest: etiam per alteram repraesentari poterit, et quidem totidem modis diversis per alteram, quot per alteram.

Denique observamus, in hocce casu divisorem communem maximum numerorum m, n aequalem esse divisori comm. max. numerorum $\alpha m + \beta n$, $\gamma m + \delta n$. Sit ille $= \Delta$, numerique μ, ν ita accepti, ut fiat $\mu m + \nu n = \Delta$. Tum erit

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm\Delta$$

Hinc div. comm. max. numerorum $\alpha m + \beta n$, $\gamma m + \delta n$ metietur ipsum Δ, Δ vero etiam illum metietur, quia manifesto ipsos $\alpha m + \beta n$, $\gamma m + \delta n$ metitur. Quare necessario ille erit $= \Delta$. — Quando igitur m, n inter se primi sunt, etiam $\alpha m + \beta n$, $\gamma m + \delta n$ inter se primi erunt.

167.

THEOREMA. *Si formae*

$$axx + 2bxy + cyy \quad \ldots\ldots\ldots \quad (F)$$
$$a'x'x' + 2b'x'y' + c'y'y' \quad \ldots\ldots\ldots \quad (F')$$

sunt aequivalentes, ipsarum determinans $= D$, posteriorque in priorem transit ponendo

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y$$

porro numerus M per F repraesentatur, faciendo $x = m$, $y = n$, adeoque per F' faciendo

$$x' = \alpha m + \beta n = m', \quad y' = \gamma m + \delta n = n'$$

et quidem ita ut m ad n eoque ipso etiam m' ad n' sit primus: ambae repraesentationes aut ad eundem valorem expressionis $\sqrt{D} (\mathrm{mod.}\, M)$ pertinebunt, aut ad oppositos, prout transformatio formae F' in F propria est vel impropria.

Dem. Determinentur numeri μ, ν ita ut fiat $\mu m + \nu n = 1$, ponaturque

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \quad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

(qui erunt integri propter $\alpha\delta - \gamma\beta = \pm 1$). Tum erit

$$\mu' m' + \nu' n' = 1. \quad \text{(Cf. art. praec. fin.)}$$

Porro sit

$$\mu(bm + cn) - \nu(am + bn) = V, \quad \mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$$

eruntque V, V' valores expr. $\sqrt{D} (\mathrm{mod.}\, M)$ ad quos repraesentatio prima et secunda pertinent. Si in V' pro μ', ν', m', n' valores ipsorum substituuntur, in V vero

$$\text{pro } a, \; a'\alpha\alpha + 2b'\alpha\gamma + c'\gamma\gamma$$
$$\text{pro } b, \; a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta$$
$$\text{pro } c, \; a'\beta\beta + 2b'\beta\delta + c'\delta\delta$$

invenietur evolutione facta $V = V'(\alpha\delta - \beta\gamma)$.

Quare erit aut $V = V'$, aut $V = -V'$, prout $\alpha\delta - \beta\gamma = +1$ aut $= -1$, *i. e.* repraesentationes pertinebunt ad eundem valorem expr. $\sqrt{D} (\mathrm{mod.}\, M)$ vel ad oppositos, prout transformatio formae F' in F est propria vel impropria. *Q. E. D.*

Si itaque plures repraesentationes numeri M per formam (a, b, c), ope valorum inter se primorum indeterminatarum x, y, habentur ad valores *diversos* expr. $\sqrt{D} (\mathrm{mod.}\, M)$ pertinentes: repraesentationes respondentes per formam (a', b', c') ad eosdem resp. valores pertinebunt, et si nulla repraesentatio numeri M per formam aliquam ad valorem quendam determinatum pertinens datur, nulla quoque dabitur ad hunc valorem pertinens per formam illi aequivalentem.

168.

THEOREMA. *Si numerus M per formam $axx+2bxy+cyy$ repraesentatur tribuendo ipsis x,y valores inter se primos m,n, valorque expressionis $\sqrt{D}(\mathrm{mod.}\,M)$, ad quem haec repraesentatio pertinet, est N: formae (a,b,c), $(M, N, \frac{NN-D}{M})$ proprie aequivalentes erunt.*

Demonstr. Ex art. 155 patet, numeros integros μ,ν inveniri posse ita ut sit

$$m\mu+n\nu=1; \quad \mu(bm+cn)-\nu(am+bn)=N$$

Quo facto forma (a,b,c) per substitutionem $x=mx'-\nu y'$, $y=nx'+\mu y'$, quae manifesto est propria, transit in formam cuius determinans $=D(m\mu+n\nu)^2$ *i. e.* $=D$, sive in formam aequivalentem: quae forma si ponitur $=(M', N', \frac{N'N'-D}{M'})$, erit

$$M'=amm+2bmn+cnn=M, \quad N'=-m\nu a+(m\mu-n\nu)b+n\mu c=N$$

Quare forma in quam (a,b,c) per transformationem illam mutatur, erit $(M, N, \frac{NN-D}{M})$. *Q. E. D.*

Ceterum ex aequationibus

$$m\mu+n\nu=1, \quad \mu(mb+nc)-\nu(ma+nb)=N$$

deducitur

$$\mu=\frac{nN+ma+nb}{amm+2bmn+cnn}=\frac{nN+ma+nb}{M}, \quad \nu=\frac{mb+nc-mN}{M}$$

qui numeri itaque erunt integri.

Porro observandum, hanc propositionem locum non habere, si $M=0$; tum enim terminus $\frac{NN-D}{M}$ fit indeterminatus*).

169.

Si plures repraesentationes numeri M per (a,b,c) habentur, ad eundem valorem expr. $\sqrt{D}(\mathrm{mod.}\,M)$, N, pertinentes (ubi valores ipsorum x,y semper inter se primos supponimus): plures etiam transformationes propriae formae $(a,b,c)\ldots(F)$, in $(M, N, \frac{NN-D}{M})\ldots(G)$ inde deducentur. Scilicet si etiam per hos valores $x=m', y=n'$ talis repraesentatio provenit, (F) etiam per substitutionem

*) In hoc enim casu, si ad ipsum phrasin extendere volumus, haec: N esse valorem expr. $\sqrt{D}(\mathrm{mod.}\,M)$, sive $NN\equiv D(\mathrm{mod.}\,M)$ significabit, $NN-D$ esse multiplum ipsius M, adeoque $=0$.

$$x=m'x'+\frac{m'N-m'b-n'c}{M}y', \quad y=n'x'+\frac{n'N+m'a+n'b}{M}y'$$

in (G) transit. Vice versa, ex quavis transformatione propria formae (F) in (G) sequetur repraesentatio numeri M per formam (F), ad valorem N pertinens. Scilicet si (F) transit in (G) positis $x=mx'-\nu y'$, $y=nx'+\mu y'$, M repraesentatur per (F) ponendo $x=m$, $y=n$, et quoniam hic $m\mu+n\nu=1$, valor expr. $\sqrt{D}(\mathrm{mod.}\,M)$ ad quem repraesentatio pertinet erit $\mu(bm+cn)-\nu(am+bn)$ *i. e.* N. Ex pluribus vero transformationibus propriis diversis, sequentur totidem repraesentationes diversae ad N pertinentes*). — Hinc facile colligitur, si omnes transformationes propriae formae (F) in (G) habeantur, ex his omnes repraesentationes ipsius M per (F) ad valorem N pertinentes sequi. Unde quaestio de repraesentationibus numeri dati per formam datam (in quibus indeterminatae valores inter se primos nanciscuntur) investigandis, reducta est ad quaestionem de inveniendis omnibus transformationibus propriis formae illius in datam aequivalentem.

Applicando iam ad haec ea quae in art. 162 docuimus, facile concluditur: Si repraesentatio aliqua numeri M per formam (F) ad valorem N pertinens sit haec: $x=\alpha$, $y=\gamma$: formulam generalem omnes repraesentationes eiusdem numeri per formam (F), ad valorem N pertinentes, comprehendentem fore hanc:

$$x=\frac{\alpha t-(\alpha b+\gamma c)u}{m}, \quad y=\frac{\gamma t+(\alpha a+\gamma b)u}{m}$$

ubi m divisor communis maximus numerorum $a, 2b, c$; et t, u omnes numeri, indefinite, aequationi $tt-Duu=mm$ satisfacientes.

170.

Si forma (a,b,c) ancipiti alicui aequivalens, adeoque formae $(M, N, \frac{NN-D}{M})$ tam proprie, quam improprie, sive tam formae $(M, N, \frac{NN-D}{M})$, quam huic $(M, -N, \frac{NN-D}{M})$ proprie: repraesentationes numeri M habebuntur per formam

*) Si ex duabus transformationibus propriis diversis eadem repraesentatio defluere supponitur, illae ita se habere debebunt:

1) $x=mx'-\nu y'$, $y=nx'+\mu y'$: 2) $x=mx'-\nu' y'$, $y=nx'+\mu' x'$.

Sed ex duabus aequationibus

$$m\mu+n\nu=m\mu'+n\nu', \quad \mu(mb+nc)-\nu(ma+nb)=\mu'(mb+nc)-\nu'(ma+nb),$$

facile deducitur esse aut $M=0$ aut $\mu=\mu'$, $\nu=\nu'$. At $M=0$ iam exclusimus.

(F), tam ad valorem N, quam ad valorem $-N$, pertinentes. Et vice versa si plures repraesentationes numeri M per eandem formam (F), ad valores *oppositos* expr. $\sqrt{D} \pmod{M}$, $N, -N$, pertinentes habentur: forma (F) formae (G) tam proprie quam improprie aequivalens erit, formaque anceps assignari poterit, cui (F) aequivaleat.

Haec generalia de repraesentationibus hic sufficiant: de repraesentationibus, in quibus indeterminatae valores inter se non primos habent, infra dicemus. Respectu aliarum proprietatum, formae quarum determinans est negativus prorsus alio modo sunt tractandae, quam formae determinantis positivi: quare iam utrasque seorsim considerabimus. Ab illis tamquam facilioribus initium facimus.

De formis determinantis negativi.

171.

Problema. *Proposita forma quacunque, (a, b, a''), cuius determinans negativus, $= -D$, designante D numerum positivum, invenire formam huic proprie aequivalentem, (A, B, C), in qua A nec maior quam $\sqrt{\frac{4}{3}D}$, C, nec minor quam $2B$.*

Solutio. Supponimus in forma proposita non omnes tres conditiones simul locum habere: alioquin enim aliam formam quaerere opus non esset. Sit b' residuum abs. min. numeri $-b$ secundum modulum a' *), atque $a'' = \frac{b'b'+D}{a'}$, qui erit integer quia $b'b' \equiv bb, b'b'+D \equiv bb+D \equiv aa' \equiv 0 \pmod{a'}$. Iam si $a'' < a'$, fiat denuo b'' resid. abs. min. ipsius $-b'$ secundum mod. a'', atque $a''' = \frac{b''b''+D}{a''}$. Si hic iterum $a''' < a''$, sit rursus b''' res. abs. min. ipsius $-b''$ secundum mod. a'' atque $a'''' = \frac{b'''b'''+D}{a'''}$. Haec operatio continuetur donec in progressione a', a'', a''', a'''' etc. ad terminum a^{m+1} perveniatur, qui praecedente suo a^m non sit minor, quod tandem evenire debet, quia alias progressio infinita numerorum integrorum continuo decrescentium haberetur. Tum forma (a^m, b^m, a^{m+1}) omnibus conditionibus satisfaciet.

Dem. I. In progressione formarum (a, b, a'), (a', b', a''), (a'', b'', a''') etc. quaevis praecedenti est contigua, quare ultima primae proprie aequivalens erit (artt. 159, 160).

*) Observare convenit, si formae alicuius (a, b, a') terminus primus vel ultimus a vel a' sit $= 0$, ipsius determinantem esse quadratum positivum: quare illud in casu praesenti evenire nequit. — Ex simili ratione termini exteri a, a' formae determinantis negativi, signa opposita habere non possunt.

II. Quum b^m sit residuum absolute minimum ipsius $-b^{m-1}$ secundum mod. a^m, maior quam $\frac{1}{2}a^m$ non erit (art. 4).

III. Quia $a^m a^{m+1} = D + b^m b^m$, atque a^{m+1} non $< a^m$, $a^m a^m$ non erit $> D + b^m b^m$, et quum b^m non $> \frac{1}{2}a^m$, $a^m a^m$ non erit $> D + \frac{1}{4}a^m a^m$ et $\frac{3}{4}a^m a^m$ non $> D$, tandemque a^m non $> \sqrt{\frac{4}{3}D}$.

Exempl. Proposita sit forma $(304, 217, 155)$, cuius determinans $= -31$. Hic invenitur progressio formarum:

$$(304, 217, 155), (155, -62, 25), (25, 12, 7), (7, 2, 5), (5, -2, 7).$$

Ultima est quaesita. — Eodem modo formae $(121, 49, 20)$, cuius determinans $= -19$, aequivalentes inveniuntur: $(20, -9, 5)$, $(5, -1, 4)$, $(4, 1, 5)$: quare $(4, 1, 5)$ erit forma quaesita.

Tales formas (A, B, C), quarum determinans est negativus et in quibus A nec maior quam $\sqrt{\frac{4}{3}D}$, C, nec minor quam $2B$, *formas reductas* vocabimus. Quare cuivis formae determinantis negativi, forma reducta proprie aequivalens inveniri poterit.

172.

Problema. *Invenire conditiones, sub quibus duae formae reductae non identicae, eiusdem determinantis $-D$, (a, b, c), (a', b', c') proprie aequivalentes esse possint.*

Solutio. Supponamus, id quod licet, a' esse non $> a$, formamque $axx + 2bxy + cyy$ transire in $a'x'x' + 2b'x'y' + c'y'y'$ per substitutionem propriam $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Tum habebuntur aequationes

$$a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a' \quad \ldots\ldots\ldots [1]$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b' \quad \ldots\ldots\ldots [2]$$
$$\alpha\delta - \beta\gamma = 1 \quad \ldots\ldots\ldots [3]$$

Ex [1] sequitur $aa' = (a\alpha + b\gamma)^2 + D\gamma\gamma$; quare aa' erit positivus; et quum $ac = D + bb$, $a'c' = D + b'b'$, etiam ac, $a'c'$ positivi erunt: quare a, a', c, c' omnes eadem signa habebunt. Sed tum a tum a' non $> \sqrt{\frac{4}{3}D}$, adeoque aa' non $> \sqrt{\frac{4}{3}D}$; quare multo minus $D\gamma\gamma$ $(= aa' - (a\alpha + b\gamma)^2)$ maior quam $\frac{4}{3}D$ esse poterit. Hinc γ erit aut $= 0$, aut $= \pm 1$.

I. Si $\gamma = 0$, ex [3] sequitur esse aut $\alpha = 1, \delta = 1$, aut $\alpha = -1, \delta = -1$.

In utroque casu fit ex [1] $a' = a$, et ex [2] $b' - b = \pm \vartheta a$. Sed b non $> \frac{1}{2}a$, et b' non $> \frac{1}{2}a'$; proin etiam non $> \frac{1}{2}a$. Quare aequatio $b' - b = \pm \vartheta a$ consistere nequit, nisi fuerit

aut $b = b'$, unde sequeretur $c' = \frac{b'b' + D}{a'} = \frac{bb + D}{a} = c$, quare formae (a, b, c), (a', b', c') identicae essent contra hyp.

aut $b = -b' = \pm \frac{1}{2}a$. In hoc etiam casu erit $c' = c$ formaque (a', b', c') erit $(a, -b, c)$ *i. e.* formae (a, b, c) opposita. Simul patet formas has esse ancipites propter $2b = \pm a$.

II. Si $\gamma = \pm 1$, fit ex [1] $a\alpha\alpha + c - a' = \pm 2b\alpha$. Sed c non minor quam a, adeoque non minor quam a': hinc $a\alpha\alpha + c - a'$ sive $2b\alpha$ certo non minor quam $a\alpha\alpha$. Quare quum $2b$ non sit maior quam a, erit α non minor quam $\alpha\alpha$; unde necessario aut $\alpha = 0$, aut $= \pm 1$.

1) Si $\alpha = 0$, fit ex [1] $a' = c$, et quoniam a neque maior quam c, neque minor quam a', erit necessario $a' = a = c$. Porro ex [3] fit $\vartheta\gamma = -1$, unde ex [2] $b + b' = \pm \delta c = \pm \delta a$. Hinc simili modo ut in (I) sequitur esse

aut $b = b'$, in quo casu formae (a, b, c), (a', b', c') forent identicae, contra hyp.

aut $b = -b'$, in quo casu formae (a, b, c), (a', b', c') erunt oppositae.

2) Si $\alpha = \pm 1$, ex [1] sequitur $\pm 2b = a + c - a'$. Quare quum neque a, neque $c < a'$, erit $2b$ non $< a$, et non $< c$. Sed $2b$ etiam non $> a$, neque $> c$; unde necessario $\pm 2b = a = c$, et hinc ex aequ. $\pm 2b = a + c - a'$, etiam $= a'$. Fit igitur ex [2]

$$b' = a(\alpha\vartheta + \gamma\delta) + b(\alpha\delta + \vartheta\gamma)$$

sive, propter $\alpha\delta - \vartheta\gamma = 1$,

$$b' - b = a(\alpha\vartheta + \gamma\delta) + 2b\vartheta\gamma = a(\alpha\vartheta + \gamma\delta \pm \vartheta\gamma)$$

quare necessario, ut ante

aut $b = b'$, unde formae (a, b, c), (a', b', c') identicae, contra hyp.

aut $b = -b'$, adeoque formae illae oppositae. Simul in hoc casu propter $a = \pm 2b$, formae erunt ancipites.

Ex his omnibus colligitur, formas (a, b, c), (a', b', c') proprie aequivalentes esse non posse nisi fuerint oppositae, simulque *aut* ancipites, *aut* $a = c = a' = c'$.

In hisce casibus formas (a, b, c), (a', b', c') proprie aequivalere, vel a priori facile praevideri potuit; si enim formae sunt oppositae, improprie, et si insuper ancipites, etiam proprie aequivalentes esse debent; si vero $a = c$, forma $(\frac{D + (a-b)^2}{a}, a - b, a)$ formae (a, b, c) contigua et proin aequivalens erit; sed propter $D + bb = ac = aa$ fit $\frac{D + (a-b)^2}{a} = 2a - 2b$, forma vero $(2a - 2b, a - b, a)$ est anceps; quare (a, b, c) oppositae suae etiam proprie aequivalebit.

Aeque facile iam diiudicari potest, quando duae formae reductae (a, b, c), (a', b', c') non oppositae improprie aequivalentes esse possint. Erunt enim impr. aequivalentes, si (a, b, c), $(a', -b', c')$, quae non identicae erunt, proprie sunt aequivalentes, et contra. Hinc patet, conditionem, sub qua *illae* improprie sint aequivalentes, esse, ut sint identicae, insuperque aut ancipites aut $a = c$. — Formae vero reductae quae neque identicae sunt neque oppositae, neque proprie neque improprie aequivalentes esse possunt.

173.

Problema. *Propositis duabus formis eiusdem determinantis negativi, F et F', investigare utrum sint aequivalentes.*

Solutio. Quaerantur duae formae reductae f, f' formis F, F' resp. proprie aequivalentes: si formae f, f' sunt proprie, vel improprie vel utroque modo aequivalentes, etiam F, F' erunt; si vero f, f' nullo modo aequivalentes sunt, etiam F, F' non erunt.

Ex art. praec. dari possunt quatuor casus:

1) Si f, f' neque identicae neque oppositae, F, F' nullo modo aequivalentes erunt.

2) Si f, f' sunt *primo* vel identicae vel oppositae, et *secundo* vel ancipites, vel terminos suos extremos aequales habent: F, F' tum proprie, tum improprie aequivalentes erunt.

3) Si f, f' sunt identicae, neque vero ancipites neque terminos extremos aequales habent: F, F' proprie tantum aequivalebunt.

4) Si f, f' sunt oppositae, neque vero ancipites, neque terminos extremos aequales habent: F, F' improprie tantum aequivalentes erunt.

Ex. Formis $(41, 35, 30)$, $(7, 18, 47)$ quarum determinans $= -5$, reductae $(1, 0, 5)$, $(2, 1, 3)$ aequivalentes inveniuntur, quare illae nullo modo aequivalentes erunt. — Formis vero $(23, 38, 63)$, $(15, 20, 27)$ aequivalet eadem

reducta $(2, 1, 3)$, quae quum simul sit anceps, formae $(23, 38, 63)$, $(15, 20, 27)$ tum proprie tum improprie aequivalebunt. — Formis $(37, 53, 78)$, $(53, 73, 102)$, aequivalent reductae $(9, 2, 9)$, $(9, -2, 9)$ quae quum sint oppositae, ipsarumque termini extremi aequales: formae propositae tam proprie quam improprie erunt aequivalentes.

174.

Multitudo omnium formarum reductarum, determinantem datum $-D$ habentium, semper est finita, et, respectu numeri D, satis modica: formae hae ipsae vero duplici modo inveniri possunt. Designemus formas reductas determinantis $-D$ indefinite per (a, b, c), ubi itaque omnes valores ipsorum a, b, c determinari debent.

Methodus prima. Accipiantur pro a omnes numeri, tum positivi tum negativi non maiores quam $\sqrt{\frac{1}{3}D}$, quorum residuum quadraticum $-D$, et pro singulis a, fiat b successive aequalis omnibus valoribus expr. $\sqrt{-D}\,(\mathrm{mod.}\,a)$, non maioribus quam $\frac{1}{2}a$, tum positive tum negative acceptis; c vero pro singulis valoribus determinatis ipsorum a, b, ponatur $=\frac{D+bb}{a}$. Si quae formae hoc modo oriuntur in quibus $c<a$, hae erunt reiiciendae, reliquae autem manifesto erunt reductae.

Methodus secunda. Accipiantur pro b omnes numeri, tum positivi tum negativi, non maiores quam $\frac{1}{2}\sqrt{\frac{1}{3}D}$, sive $\sqrt{\frac{1}{12}D}$; pro singulis b resolvatur $bb+D$ omnibus quibus fieri potest modis in binos factores (etiam signorum diversitatis ratione habita) ambos ipso $2b$ non minores ponaturque alter factor $=a$, alter $=c$. Quum a non erit $>\sqrt{\frac{1}{3}D}$, omnes formae quae hoc modo prodeunt, manifesto erunt reductae. — Denique patet, nullam formam reductam dari posse quae non per utramque methodum inveniatur.

Ex. Sit $D=85$. Hic limes valorum ipsius a est $\sqrt{\frac{340}{3}}$ qui iacet inter 10 et 11. Numeri vero inter 1 et 10 (incl.) quorum residuum -85, sunt 1, 2, 5, 10. Unde habentur formae duodecim:

$(1, 0, 85)$, $(2, 1, 43)$, $(2, -1, 43)$, $(5, 0, 17)$, $(10, 5, 11)$, $(10, -5, 11)$; $(-1, 0, -85)$, $(-2, 1, -43)$, $(-2, -1, -43)$, $(-5, 0, -17)$, $(-10, 5, -11)$, $(-10, -5, -11)$.

Per methodum alteram limes valorum ipsius b habetur $\sqrt{\frac{85}{3}}$, qui situs est inter 5 et 6. Pro $b=0$, prodeunt formae

$$(1, 0, 85),\ (-1, 0, -85),\ (5, 0, 17),\ (-5, 0, -17),$$

pro $b=\pm 1$ hae $(2, \pm 1, 43)$, $(-2, \pm 1, -43)$.

Pro $b=\pm 2$ nullae habentur, quia 89 in duos factores, qui ambo non <4, resolvi nequit. Idem valet de $\pm 3, \pm 4$. Tandem pro $b=\pm 5$, proveniunt

$$(10, \pm 5, 11),\ (-10, \pm 5, -11).$$

175.

Si ex omnibus formis reductis determinantis dati, formarum binarum, quae, licet non identicae, tamen proprie sunt aequivalentes, alterutra reiicitur: formae remanentes hac insigni proprietate erunt praeditae, ut, quaevis forma eiusdem determinantis alicui ex ipsis proprie sit aequivalens, et quidem unicae tantum (alias enim inter ipsas aliquae proprie aequivalentes forent). Unde patet, *omnes formas eiusdem determinantis in totidem classes distribui posse quot formae remanserint*, referendo scilicet formas eidem reductae proprie aequivalentes in eandem classem. Ita pro $D=85$, remanent formae

$$(1, 0, 85),\ (2, 1, 43),\ (5, 0, 17),\ (10, 5, 11),$$
$$(-1, 0, -84),\ (-2, 1, -43),\ (-5, 0, -17),\ (-10, 5, -11)$$

quare omnes formae determinantis -85 in octo classes distribui poterunt, prout formae primae, aut secundae etc. proprie aequivalent. Perspicuum vero est, formas in eadem classe locatas proprie aequivalentes fore, formas ex diversis classibus proprie aequivalentes esse non posse. Sed hoc argumentum de classificatione formarum infra multo fusius exsequemur. Hic unicam observationem adiicimus. Iam supra ostendimus, si determinans formae (a, b, c) fuerit negativus $=-D$, a et c eadem signa habere (quia scilicet $ac=bb+D$ adeoque positivus); eadem ratione facile perspicitur, si formae (a, b, c), (a', b', c') sint aequivalentes, omnes a, c, a', c' eadem signa habituros. Si enim prior in posteriorem per substitut. $x=\alpha x'+\vec{o}y'$, $y=\gamma x'+\delta y'$ transit: erit $aa\alpha\alpha+2ba\gamma+c\gamma\gamma=a'$, hinc $aa'=(a\alpha+b\vec{o})^2+D\gamma\gamma$, adeoque certo non negativus; quoniam vero neque a neque $a'=0$ esse potest, erit aa' positivus et proin signa ipsorum a, a' eadem.

Hinc manifestum est, formas quarum termini exteri sint positivi, ab iis quarum termini exteri sint negativi, prorsus esse separatas, sufficitque ex formis reductis eas tantum considerare quae terminos suos exteros positivos habent, nam

reliquae totidem sunt multitudine et ex illis oriuntur, tribuendo terminis exteris signa opposita; idemque valet de formis ex reductis reiiciendis et remanentibus.

176.

Ecce itaque pro determinantibus quibusdam negativis tabulam formarum, secundum quas omnes reliquae eiusdem determinantis in classes distingui possunt; apponimus autem, ad annotat. art. praec., semissem tantum, scilicet eas quarum termini exteri positivi.

D	
1	$(1, 0, 1)$.
2	$(1, 0, 2)$.
3	$(1, 0, 3)$, $(2, 1, 2)$.
4	$(1, 0, 4)$, $(2, 0, 2)$.
5	$(1, 0, 5)$, $(2, 1, 3)$.
6	$(1, 0, 6)$, $(2, 0, 3)$.
7	$(1, 0, 7)$, $(2, 1, 4)$.
8	$(1, 0, 8)$, $(2, 0, 4)$, $(3, 1, 3)$.
9	$(1, 0, 9)$, $(2, 1, 5)$, $(3, 0, 3)$.
10	$(1, 0, 10)$, $(2, 0, 5)$.
11	$(1, 0, 11)$, $(2, 1, 6)$, $(3, 1, 4)$, $(3, -1, 4)$.
12	$(1, 0, 12)$, $(2, 0, 6)$, $(3, 0, 4)$, $(4, 2, 4)$.

Superfluum foret hanc tabulam hic ulterius continuare, quippe quam infra multo aptius disponere docebimus.

Patet itaque, quamvis formam determinantis -1, formae $xx+yy$ proprie aequivalere, si ipsius termini exteri sint positivi, vel huic $-xx-yy$, si sint negativi; quamvis formam determinantis -2, cuius termini exteri positivi, formae $xx+2yy$ etc.; quamvis formam determinantis -11, cuius termini exteri positivi, alicui ex his $xx+11yy$, $2xx+2xy+6yy$, $3xx+2xy+4yy$, $3xx-2xy+4yy$ etc.

177.

Problema. *Habetur series formarum, quarum quaevis praecedenti a parte posteriori contigua: desideratur transformatio aliqua propria primae in formam quamcumque seriei.*

Solutio. Sint formae $(a, b, a') = F$; $(a', b', a'') = F'$; $(a'', b'', a''') = F''$; $(a''', b''', a'''') = F'''$ etc. Designentur $\frac{b+b'}{a}$, $\frac{b'+b''}{a'}$, $\frac{b''+b'''}{a''}$ etc. respective per h', h'', h''' etc. Sint indeterminatae formarum F, F', F'' etc. x, y; x', y'; x'', y'' etc. Ponatur F transmutari

in F positis $x = \alpha' x' + \delta' y'$, $y = \gamma' x' + \varepsilon' y'$
F' . . . $x = \alpha'' x'' + \delta'' y''$, $y = \gamma'' x'' + \varepsilon'' y''$
F'' . . . $x = \alpha''' x''' + \delta''' y'''$, $y = \gamma''' x''' + \varepsilon''' y'''$
etc.

Tum quia F transit in F' positis $x = -y'$, $y = x' + h'y'$
F' in F'' positis $x' = -y''$, $y' = x'' + h''y''$
F'' in F''' positis $x'' = -y'''$, $y'' = x''' + h'''y'''$ etc. (art. 160)

facile eruetur sequens algorithmus (art. 159):

$$\begin{array}{llll}
\alpha' = 0 & \delta' = -1 & \gamma' = 1 & \varepsilon' = h' \\
\alpha'' = \delta' & \delta'' = h''\delta' - \alpha' & \gamma'' = \varepsilon' & \varepsilon'' = h''\varepsilon' - \gamma' \\
\alpha''' = \delta'' & \delta''' = h'''\delta'' - \alpha'' & \gamma''' = \varepsilon'' & \varepsilon''' = h'''\varepsilon'' - \gamma'' \\
\alpha'''' = \delta''' & \delta'''' = h''''\delta''' - \alpha''' & \gamma'''' = \varepsilon''' & \varepsilon'''' = h''''\varepsilon''' - \gamma''' \\
\multicolumn{4}{c}{\text{etc.}}
\end{array}$$

sive

$$\begin{array}{llll}
\alpha' = 0 & \delta' = -1 & \gamma' = 1 & \varepsilon' = h' \\
\alpha'' = \delta' & \delta'' = h''\delta' & \gamma'' = \varepsilon' & \varepsilon'' = h''\varepsilon' - 1 \\
\alpha''' = \delta'' & \delta''' = h'''\delta'' - \delta' & \gamma''' = \varepsilon'' & \varepsilon''' = h'''\varepsilon'' - \varepsilon' \\
\alpha'''' = \delta''' & \delta'''' = h''''\delta''' - \delta'' & \gamma'''' = \varepsilon''' & \varepsilon'''' = h''''\varepsilon''' - \varepsilon'' \\
\multicolumn{4}{c}{\text{etc.}}
\end{array}$$

Omnes has transformationes esse proprias tum ex ipsarum formatione tum ex art. 159 nullo negotio deduci potest.

Algorithmus hic perquam simplex et ad calculum expeditus, algorithmo in art. 27 exposito est analogus, ad quem etiam reduci potest *). Ceterum solutio

*) Erit scilicet in signis art. 27, $\delta^n = \pm[-h'', h''', -h'''', \ldots \pm h^n]$
ubi signa ambigue posita, esse debent $- -$; $- +$; $+ -$; $+ +$; prout n formae $4k+0$; 1; 2; 3,
et $\varepsilon^n = \pm[h', -h'', h''' \ldots \pm h^n]$
ubi signa ambigua esse debent $+ -$; $+ +$; $- -$; $- +$, prout n formae $4k+0$; 1; 2; 3. Sed hoc, quod quivis facile ipse confirmare poterit, fusius exsequi, nobis brevitas non permittit.

haec ad formas determinantis negativi non est restricta, sed ad omnes casus patet, si modo nullus numerorum a', a'', a''' etc. $= 0$.

178.

Problema. *Propositis duabus formis F, f, eiusdem determinantis negativi, proprie aequivalentibus: invenire transformationem aliquam propriam alterius in alteram.*

Sol. Supponamus formam F esse (A, B, A') et per methodum art. 171 inventam esse progressionem formarum (A', B', A''), (A'', B'', A''') etc. usque ad (A^m, B^m, A^{m+1}), quae sit reducta: similiterque f esse (a, b, a') et per eandem methodum inventam seriem (a', b', a''), (a'', b'', a''') usque ad (a^n, b^n, a^{n+1}), quae sit reducta. Tum duo casus locum habere possunt.

I. Si formae (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) sunt aut identicae, aut oppositae simulque ancipites. Tum formae (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$ erunt contiguae (designante A^{m-1} terminum progressionis $A, A', A'' \ldots A^m$ penultimum, similiaque B^{m-1}, a^{n-1}, b^{n-1}). Nam $A^m = a^n$, $B^{m-1} \equiv -B^m \pmod{A^m}$, $b^{n-1} \equiv -b^n \pmod{a^n \text{ sive } A^m}$, unde $B^{m-1} - b^{n-1} \equiv b^n - B^m$ adeoque $\equiv 0$, si formae (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) sunt identicae, et $\equiv 2b^n$ adeoque $\equiv 0$, si sunt oppositae et ancipites. Quare in progressione formarum

$$(A, B, A'), (A', B', A'') \ldots (A^{m-1}, B^{m-1}, A^m),$$
$$(a^n, -b^{n-1}, a^{n-1}), (a^{n-1}, -b^{n-2}, a^{n-2}) \ldots (a', -b, a), (a, b, a')$$

quaevis forma praecedenti contigua erit, adeoque per art. praec. transformatio propria primae F in ultimam f inveniri poterit.

II. Si formae (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) non identicae, sed oppositae simulque $A^m = A^{m+1} = a^n = a^{n+1}$. Tum progressio formarum

$$(A, B, A'), (A', B', A'') \ldots (A^m, B^m, A^{m+1}),$$
$$(a^n, -b^{n-1}, a^{n-1}), (a^{n-1}, -b^{n-2}, a^{n-2}) \ldots (a', -b, a), (a, b, a')$$

eadem proprietate erit praedita. Nam $A^{m+1} = a^n$, et $B^m - b^{n-1} = -(b^n + b^{n-1})$ per a^n divisibilis. Unde per art. praec. invenietur transformatio propria formae primae F in ultimam f.

Ex. Ita pro formis $(23, 38, 63)$, $(15, 20, 27)$ habetur progressio

$(23, 38, 63)$, $(63, 25, 10)$, $(10, 5, 3)$, $(3, 1, 2)$, $(2, -7, 27)$, $(27, -20, 15)$, $(15, 20, 27)$

quare

$$k' = 1, \quad k'' = 3, \quad k''' = 2, \quad k'''' = -3, \quad k''''' = -1, \quad k'''''' = 0.$$

Hinc deducitur transformatio formae $23xx + 76xy + 63yy$ in $15tt + 40tu + 27uu$ haec: $x = -13t - 18u$, $y = 8t + 11u$.

Ex solutione hac nullo negotio sequitur solutio problematis: *Si formae F, f improprie sunt aequivalentes, invenire transformationem impropriam formae F in f.* Sit enim $f = att + 2btu + a'uu$ eritque forma opposita $app - 2bpq + a'qq$ formae F proprie aequivalens. Quaeratur transformatio propria formae F in illam, $x = \alpha p + \delta q$, $y = \gamma p + \varepsilon q$, patetque F transire in f positis $x = \alpha t - \delta u$, $y = \gamma t - \varepsilon u$, haneque transformationem fore impropriam.

Quodsi igitur formae F, f tam proprie quam improprie sunt aequivalentes: inveniri poterit tam transformatio propria aliqua quam impropria.

179.

Problema. *Si formae F, f sunt aequivalentes: invenire omnes transformationes formae F in f.*

Sol. Si formae F, f unico tantum modo sunt aequivalentes *i. e.* proprie tantum vel improprie tantum: quaeratur per art. praec. transformatio una formae F in f, patetque alias quam quae huic sint similes dari non posse. Si vero formae F, f tam proprie quam improprie aequivalent, quaerantur duae transformationes, altera propria, altera impropria. Iam sit forma $F = (A, B, C)$, $BB - AC = -D$, numerorumque $A, 2B, C$ divisor communis maximus $= m$. Tum ex art. 162 patet, in priori casu omnes transformationes formae F in f ex una transformatione, in posteriori omnes proprias ex propria omnesque improprias ex impropria deduci posse, si modo omnes solutiones aequationis $tt + Duu = mm$ habeantur. His igitur inventis problema erit solutum.

Habetur autem $D = AC - BB$, $4D = 4AC - 4BB$, quare $\frac{4D}{mm} = 4\frac{AC}{mm} - \left(\frac{2B}{m}\right)^2$ erit integer. Iam si

1) $\frac{4D}{mm} > 4$, erit $D > mm$: quare in $tt + Duu = mm$, u necessario debebit esse $= 0$, adeoque t alios valores quam $+m$, et $-m$ habere nequit. Hinc

si F, f unico tantum modo aequivalentes sunt et transformatio aliqua

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

praeter hanc ipsam quae prodit ex $t = m$ (art. 162), et hanc

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'$$

aliae locum habere non possunt. Si vero F, f tum proprie tum impropric aequivalent, atque propria aliqua transformatio habetur

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

impropriaque

$$x = \alpha' x' + \beta' y', \quad y = \gamma x' + \delta y'$$

praeter illam (ex $t = m$) et hancce

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y' \quad (\text{ex } t = -m)$$

alia propria non dabitur; similiterque nulla impropria praeter

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y' \quad \text{et} \quad x = -\alpha' x' - \beta' y', \quad y = -\gamma' x' - \delta' y'$$

2) Si $\frac{4D}{mm} = 4$, sive $D = mm$, aequatio $tt + Duu = mm$ quatuor solutiones admittet $t, u; = m, 0;\ -m, 0;\ 0, 1;\ 0, -1$. Hinc si F, f unico tantum modo aequivalentes et transformatio aliqua

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

quatuor omnino transformationes dabuntur,

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$

$$x = \mp\tfrac{\alpha B + \gamma C}{m} x' \mp \tfrac{\beta B + \delta C}{m} y', \quad y = \pm\tfrac{\alpha A + \gamma B}{m} x' \pm \tfrac{\beta A + \delta B}{m} y'$$

Si vero F, f duobus modis aequivalent, sive praeter transformationem illam datam alia ipsi dissimilis habetur: haec quoque suppeditabit quatuor illis dissimiles, ita ut *octo* transformationes habeantur. — Ceterum facile demonstrari potest in hoc casu F, f semper revera duobus modis aequivalere. Nam quum $D = mm = AC - BB$, m etiam ipsum B metietur. Formae $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ determinans erit $= -1$, quare formae $(1, 0, 1)$ vel huic $(-1, 0, -1)$ erit aequivalens.

Facile vero perspicitur, per eandem transformationem, per quam $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ transeat in $(\pm 1, 0, \pm 1)$, formam (A, B, C) transire in $(\pm m, 0, \pm m)$, ancipitem. Quare forma (A, B, C), ancipiti aequivalens, cuivis formae, cui aequivalet, tum proprie tum improprie aequivalebit.

3) Si $\frac{4D}{mm} = 3$, sive $4D = 3mm$. Tum m erit par omnesque solutiones aequationis $tt + Duu = mm$ erunt sex

$$t, u; = m, 0;\ -m, 0;\ \tfrac{1}{2}m, 1;\ -\tfrac{1}{2}m, -1;\ \tfrac{1}{2}m, -1;\ -\tfrac{1}{2}m, 1$$

Si itaque duae transformationes dissimiles formae F in f habentur,

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$
$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

habebuntur duodecim transformationes, scilicet sex priori similes

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$
$$x = \pm(\tfrac{1}{2}\alpha - \tfrac{\alpha B + \gamma C}{m}) x' \pm (\tfrac{1}{2}\beta - \tfrac{\beta B + \delta C}{m}) y'$$
$$y = \pm(\tfrac{1}{2}\gamma + \tfrac{\alpha A + \gamma B}{m}) x' \pm (\tfrac{1}{2}\delta + \tfrac{\beta A + \delta B}{m}) y'$$
$$x = \pm(\tfrac{1}{2}\alpha + \tfrac{\alpha B + \gamma C}{m}) x' \pm (\tfrac{1}{2}\beta + \tfrac{\beta B + \delta C}{m}) y'$$
$$y = \pm(\tfrac{1}{2}\gamma - \tfrac{\alpha A + \gamma B}{m}) x' \pm (\tfrac{1}{2}\delta - \tfrac{\beta A + \delta B}{m}) y'$$

et sex posteriori similes, quae ex his nascuntur ponendo pro α, β, γ, δ hos α', β', γ', δ'.

Quod vero in hoc casu semper F, f utroque modo aequivalent, ita demonstramus. Formae $(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m})$ determinans erit $= -\frac{4D}{mm} = -3$, adeoque haec forma (art. 176) aut formae $(\pm 1, 0, \pm 3)$ aut huic $(\pm 2, \pm 1, \pm 2)$ aequivalens. Unde facile perspicitur, formam (A, B, C) aut formae $(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m)$ aut huic $(\pm m, \frac{1}{2}m, \pm m)$ *) quae ambae sunt ancipites, aequivalere adeoque cuivis aequivalenti, utroque modo.

4) Si supponitur $\frac{4D}{mm} = 2$, fit $(\frac{2B}{m}, -1, \frac{2C}{mm} = 2$, adeoque $\equiv 2 \pmod 4$.

*) Demonstrari potest, formam (A, B, C) necessario posteriori aequivalere; sed hoc hic non necessarium.

Sed quum nullum quadratum esse possit $\equiv 2 \pmod 4$, hic casus locum habere nequit.

5) Supponendo $\frac{4D}{mm} = 1$, fit $(\frac{2B}{m})^2 \equiv 4\frac{AC}{mm} - 1 \equiv -1 \pmod 4$. Quod quum impossibile sit, etiam hic casus nequit locum habere.

Ceterum quum D neque $= 0$, neque negativus sit, alii casus praeter enumeratos dari non possunt.

180.

Problema. *Invenire omnes repraesentationes numeri dati M per formam $axx + 2bxy + cyy \ldots F$, determinantis negativi $-D$, in quibus x, y valores inter se primos nanciscuntur.*

Sol. Ex art. 154 patet, M eo quo requiritur modo repraesentari non posse, nisi $-D$ sit resid. quadr. ipsius M. Investigentur itaque primo omnes valores diversi (*i. e.* incongrui) expr. $\sqrt{-D} \pmod M$, qui sint N, $-N$, N', $-N'$, N'', $-N''$ etc.; quo simplicior evadat calculus, omnes N, N' etc. ita determinari possunt, ut non sint $> \frac{1}{2}M$. Iam quoniam quaevis repraesentatio ad aliquem horum valorum pertinere debet, singuli seorsim considerentur.

Si formae F, $(M, N, \frac{D+NN}{M})$ non sunt proprie aequivalentes, nulla repraesentatio ipsius M ad valorem N pertinens dari potest (art. 168). Si vero sunt, investigetur transformatio propria formae F in

$$Mx'x' + 2Nx'y' + \frac{D+NN}{M}y'y'$$

quae sit

$$x = \alpha x' + \delta y', \quad y = \gamma x' + \delta y'$$

eritque $x = \alpha, y = \gamma$ repraesentatio numeri M per F ad N pertinens. Sit div. comm. max. numerorum $A, 2B, C, = m$ distinguanturque tres casus art. praec.:

1) Si $\frac{4D}{mm} > 4$, aliae repraesentationes ad N pertinentes quam hae *duae* $x = \alpha, y = \gamma$; $x = -\alpha, y = -\gamma$ non dabuntur (artt. 169, 179).

2) Si $\frac{4D}{mm} = 4$, habebuntur *quatuor* repraesentationes

$$x = \pm\alpha, \quad y = \pm\gamma; \quad x = \mp\frac{\alpha B + \gamma C}{m}, \quad y = \pm\frac{\alpha A + \gamma B}{m}$$

3) Si $\frac{4D}{mm} = 3$, habebuntur *sex* repraesentationes.

$$x = \pm\alpha, \quad y = \pm\gamma;$$
$$x = \pm(\tfrac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m}), \quad y = \pm(\tfrac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m})$$
$$x = \pm(\tfrac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m}), \quad y = \pm(\tfrac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m})$$

Eodem modo quaerendae sunt repraesentationes ad valores $-N, N', -N'$ etc. pertinentes.

181.

Investigatio repraesentationum numeri M per formam F, in quibus x, y valores inter se non primos habent, ad casum iam consideratum facile reduci potest. Fiat talis repraesentatio ponendo $x = \mu e$, $y = \mu f$, ita ut μ sit div. comm. max. ipsorum $\mu e, \mu f$ sive e, f inter se primi. Tum erit $M = \mu\mu(Aee + 2Bef + Cff)$ adeoque per $\mu\mu$ divisibilis; substitutio vero $x = e$, $y = f$ erit repraesentatio numeri $\frac{M}{\mu\mu}$ per formam F, in qua x, y valores inter se primos habent. Si itaque M per nullum quadratum (praeter 1) divisibilis est, *e. g.* si est numerus primus: tales repraesentationes ipsius M non dabuntur. Si vero M divisores quadraticos implicat, sint hi $\mu\mu, \nu\nu, \pi\pi$, etc. Quaerantur primo omnes repraesentationes numeri $\frac{M}{\mu\mu}$ per formam (A, B, C), in quibus x, y valores inter se primos habent, qui valores si per μ multiplicantur, praebebunt omnes repraesentationes ipsius M, in quibus div. comm. max. numerorum x, y est μ. Simili modo omnes repraesentationes ipsius $\frac{M}{\nu\nu}$, in quibus valores ipsorum x, y inter se primi sunt, praebebunt omnes repraesentationes ipsius M, in quibus div. comm. max. valorum ipsorum x, y est ν etc.

Palam igitur est, per praecepta praecedentia omnes repraesentationes numeri dati per formam datam determinantis negativi inveniri posse.

Applicationes speciales ad discerptionem numerorum in quadrata duo, in quadratum simplex et duplex, in simplex et triplex.

182.

Descendimus ad quosdam casus particulares, tum propter insignem ipsorum elegantiam tum propter assiduam operam ab ill. Eulero ipsis impensam, unde classicam quasi dignitatem sunt nacti.

I. Per formam $xx + yy$ ita repraesentari ut x ad y sit primus (sive in

duo quadrata inter se prima discerpi) nullus numerus potest nisi cuius residuum quadraticum est $+1$, tales vero numeri, positive accepti, omnes poterunt. Sit M talis numerus, omnesque valores expr. $\sqrt{-1} \pmod{M}$ hi: $N, -N, N', -N'$, $N'', -N''$ etc. Tum per art. 176 forma $(M, N, \frac{NN+1}{M})$ formae $(1, 0, 1)$ proprie aequivalens erit. Sit transformatio aliqua propria huius in illam, $x = \alpha x' + \delta y'$, $y = \gamma x' + \varepsilon y'$, eruntque repraesentationes numeri M per formam $xx+yy$ ad N pertinentes hae quatuor *): $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\gamma$, $y = \pm\alpha$.

Quum forma $(1, 0, 1)$ sit anceps, patet, etiam formam $(M, -N, \frac{NN+1}{M})$ ipsi proprie aequivalentem fore, illamque proprie in hanc transmutari positis $x = \alpha x' - \delta y'$, $y = -\gamma x' + \varepsilon y'$. Hinc derivantur quatnor repraesentationes ipsius M ad $-N$ pertinentes, $x = \pm\alpha$, $y = \mp\gamma$; $x = \pm\gamma$, $y = \pm\alpha$. Manifestum itaque est, octo repraesentationes ipsius M dari, quarum semissis altera ad N, altera ad $-N$ pertineat; sed hae omnes *unicam* tantummodo discerptionem numeri M in duo quadrata exhibent, $M = \alpha\alpha + \gamma\gamma$, siquidem ad quadrata ipsa tantum, neque vero ad ordinem radicumve signa spectamus.

Quodsi itaque alii valores expr. $\sqrt{-1} \pmod{M}$ praeter N et $-N$ non dantur, quod *e. g.* evenit, quando M est numerus primus, M unico tantum modo in duo quadrata inter se prima resolvi poterit. Iam quum -1 sit residuum quadraticum cuiusvis numeri primi formae $4n+1$ (art. 108), manifestoque numerus primus in duo quadrata inter se non prima discerpi nequeat, habemus theorema:

Quivis numerus primus formae $4n+1$ in duo quadrata decomponi potest, et quidem unico tantum modo.

$1 = 0+1$, $5 = 1+4$, $13 = 4+9$, $17 = 1+16$, $29 = 4+25$, $37 = 1+36$, $41 = 16+25$, $53 = 4+49$, $61 = 25+36$, $73 = 9+64$, $89 = 25+64$, $97 = 16+81$ etc.

Theorema hoc elegantissimum iam Fermatio notum fuit, sed ab ill. Eulero primo demonstratum est. *Comm. nov. Petr. T. V, ad annos* 1754, 1755, *p.* 3 sqq. In *T. IV*, diss. exstat ad idem argumentum pertinens, *p.* 3 sqq., sed tum rem penitus nondum absolverat; vid. imprimis art. 27.

*) Patet enim, hunc casum sub (2) art. 180 contentum esse.

Si igitur numerus aliquis formae $4n+1$ aut pluribus modis aut nullo modo in duo quadrata resolvi potest, certo non erit primus.

Vice versa autem, si expr. $\sqrt{-1} \pmod{M}$ praeter N et $-N$ alios adhuc valores habet, aliae adhuc repraesentationes ipsius M dabuntur, ad hos pertinentes. In hoc itaque casu M pluribus modis in duo quadrata resolvi poterit *e. g.* $65 = 1+64 = 16+49$, $221 = 25+196 = 100+121$.

Repraesentationes reliquae, in quibus x, y valores obtinent non primos inter se, per methodum nostram generalem facile inveniri possunt. Observamus tantummodo, si numerus aliquis factores formae $4n+3$ involvens, per nullam divisionem per quadratum ab his liberari possit (quod fiet, si aliquis aut plures talium factorum *dimensionem imparem* habet), hunc nullo modo in duo quadrata resolvi posse *).

II. Per formam $xx+2yy$ nullus numerus, cuius non-residuum -2, ita repraesentari potest, ut x ad y sit primus, reliqui omnes poterunt. Sit -2 residuum numeri M, atque N valor aliquis expr. $\sqrt{-2} \pmod{M}$. Tum per art. 176 formae $(1, 0, 2)$, $(M, N, \frac{NN+2}{M})$ proprie aequivalentes erunt. Transeat illa proprie in hanc ponendo $x = \alpha x' + \delta y'$, $y = \gamma x' + \varepsilon y'$, eritque $x = \alpha$, $y = \gamma$ repraesentatio numeri M ad N pertinens. Praeter quam et hanc $x = -\alpha$, $y = -\gamma$ aliae ad N non pertinebunt (art. 180).

Simili modo, ut supra, perspicitur, repraesentationes $x = \pm\alpha$, $y = \mp\gamma$ ad valorem $-N$ pertinere. Omnes vero hae quatuor repraesentationes unicam tantum discerptionem ipsius M in quadratum et quadratum duplex exhibent, et si praeter N et $-N$ alii valores expr. $\sqrt{-2} \pmod{M}$ non dantur, aliae discerptiones non dabuntur. Hinc adiumento proposs. art. 116 facile deducitur theorema:

*) Si numerus $M = 2^\mu S a^\alpha b^\beta c^\gamma \ldots$, ita ut a, b, c etc. sint numeri primi inaequales formae $4n+1$, atque S productum ex omnibus factoribus primis ipsius M formae $4n+3$ (ad quam formam quivis numerus positivus reduci potest, faciendo $\alpha = 0$ quando M est impar, et $S = 1$ quando M nullos factores formae $4n+3$ implicat): M *nullo modo* in duo quadrata resolvi poterit, si S est non-quadratus; si vero S est quadratus, dabuntur $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ etc. discerptiones ipsius M, quando aliquis numerorum α, β, γ etc. est impar, aut $\frac{1}{4}(\alpha+1)(\beta+1)(\gamma+1)$ etc. $+\frac{1}{4}$, quando omnes α, β, γ etc. sunt pares (siquidem ad quadrata ipsa tantum respicitur). Qui in calculo combinationum aliquantum sunt versati, demonstrationem huius theorematis (cui, perinde ut aliis *particularibus*, immorari nobis non licet) ex theoria nostra generali haud difficulter eruere poterunt. Cf. art. 105.

Quivis numerus primus formae $8n+1$ *vel* $8n+3$ *in quadratum et quadratum duplex decomponi potest et quidem unico tantum modo.*

$1=1+0$, $3=1+2$, $11=9+2$, $17=9+8$, $19=1+18$, $41=9+32$, $43=25+18$, $59=9+50$, $67=49+18$, $73=1+72$, $83=81+2$, $89=81+8$, $97=25+72$ etc.

Etiam hoc theorema, uti plura similia, Fermatio innotuit: sed ill. La Grange primus demonstrationem dedit, *Suite des recherches d'Arithmétique*, Nouv. Mém. de l'Ac. de Berlin 1775, p. 323 sqq. Multa ad idem argumentum pertinentia iam ill. Euler absolverat, *Specimen de usu observationum in mathesi pura* Comm. nov. Petr. T. VI p. 185 sqq. Sed demonstratio completa theorematis semper ipsius industriam elusit, p. 220. Conf. etiam diss. in T. VIII (ad annos 1760, 1761), *Supplementum quorundam theorematum arithmeticorum*, sub fin.

III. Per methodum similem demonstratur, quemvis numerum, cuius residuum quadr. sit -3, repraesentari posse aut per formam $xx+3yy$, aut per hanc $2xx+2xy+2yy$, ita ut valor ipsius x ad valorem ipsius y sit primus. Quare quum -3 sit residuum omnium numerorum primorum formae $3n+1$ (art. 119) manifestoque per formam $2xx+2xy+2yy$ numeri *pares* tantum repraesentari possint: eodem modo ut supra habetur theorema:

Quivis numerus primus formae $3n+1$ *in quadratum et quadratum triplex decomponi potest, et quidem unico tantum modo.*

$1=1+0$, $7=4+3$, $13=1+12$, $19=16+3$, $31=4+27$, $37=25+12$, $43=16+27$, $61=49+12$, $67=64+3$, $73=25+48$ etc.

Demonstrationem huius theorematis ill. Euler primus tradidit in commentatione modo laudata, *Comm. nov. Petr.* T. VIII, p. 105 sqq.

Simili modo ulterius progredi et *e. g.* ostendere possemus, quemvis numerum primum formae $20n+1$, vel $20n+3$, vel $20n+7$, vel $20n+9$ (quippe quorum residuum -5) per alterutram formam $xx+5yy$, $2xx+2xy+3yy$ repraesentari posse, et quidem numeros primos formae $20n+1$ et $20n+9$ per priorem, primos formae $20n+3$, $20n+7$ per posteriorem, nec non dupla primorum formae $20n+1$, $20n+9$ per formam $2xx+2xy+3yy$, dupla primorum formae $20n+3$, $20n+7$ per formam $xx+5yy$: sed hanc propositionem infinitasque alias particulares quivis proprio marte ex praecedentibus et infra tradendis derivare poterit. — Transimus itaque ad *formas determinantis positivi*, et quum harum indoles prorsus alia sit, quando determinans est quadratus, alia, quando non-quadratus: formas determinantis quadrati hic primo excludimus postcaque seorsim considerabimus.

De formis determinantis positivi non-quadrati.

183.

Problema. *Proposita forma quacunque* (a, b, a'), *cuius determinans positivus non-quadratus* $=D$: *invenire formam huic proprie aequivalentem* (A, B, C), *in qua* B *sit positivus et* $<\sqrt{D}$; A *vero si est positivus, vel* $=A$, *si* A *negativus, inter* $\sqrt{D}+B$ *et* $\sqrt{D}-B$ *situs.*

Sol. Supponimus in forma proposita utramque conditionem nondum locum habere; alioquin enim aliam formam quaerere opus non esset. Porro observamus, in forma determinantis *non-quadrati* terminum primum vel ultimum $=0$ esse non posse (art. 171 anm.). Sit $b' \equiv -b \pmod{a}$ atque intra limites $\sqrt{D}$ et $\sqrt{D}\mp a'$ situs (accepto signo superiori quando a' positivus, inferiori quando est negativus) quod fieri posse simili ratione ut art. 3, facile demonstratur, ponaturque $\frac{bb'-D}{a'}=a''$, qui erit integer, quia $bb'-D \equiv bb-D \equiv aa' \equiv 0 \pmod{a'}$. Iam si $a''<a'$, fiat denuo $b'' \equiv -b' \pmod{a''}$ et inter $\sqrt{D}$ et $\sqrt{D}\mp a''$ situs (prout a'' positivus vel negativus) et $\frac{b''b''-D}{a''}=a'''$. Si hic iterum $a'''<a''$, sit rursus $b''' \equiv -b'' \pmod{a'''}$, et inter $\sqrt{D}$ et $\sqrt{D}\mp a'''$ situs atque $\frac{b'''b'''-D}{a'''}=a''''$. Haec operatio continuetur, donec in progressione a', a'', a''', a'''' etc. ad terminum a^{m+1} perveniatur, praecedente a^m non minorem, quod tandem evenire debet, quia alioquin progressio infinita numerorum integrorum continuo decrescentium haberetur. Tum positis $a^m=A$, $b^m=B$, $a^{m+1}=C$, forma (A, B, C) omnibus conditionibus satisfaciet.

Dem. I. Quoniam in progressione formarum (a, b, a'), (a', b', a''), (a'', b'', a''') etc. quaevis praecedenti est contigua: ultima (A, B, C) primae (a, b, a') proprie aequivalens erit.

II. Quia B inter $\sqrt{D}$ et $\sqrt{D}\mp A$ situs est (accipiendo semper signum superius quando A est positivus, inferius quando A est negativus): patet, si ponatur $\sqrt{D}-B=p$, $B-(\sqrt{D}\mp A)=q$, hos p, q fore positivos. Iam facile confirmatur, fore $qq+2pq+2p\sqrt{D}=D+AA-BB$, quare $D+AA-BB$ erit numerus positivus, quem ponemus $=r$. Hinc propter $D=BB-AC$,

fit $r = AA - AC$, adeoque $AA - AC$ numerus positivus; quia vero per hyp. A non est maior quam C, manifesto illud aliter fieri nequit, quam si AC est negativus, adeoque signa ipsorum A, C opposita. Hinc $BB = D + AC < D$ adeoque $B < \sqrt{D}$.

III. Porro quia $-AC = D - BB$, erit $AC < D$, et hinc (quia A non $> C$), $A < \sqrt{D}$. Quare $\sqrt{D} \mp A$ erit positivus, adeoque etiam B, qui inter limites $\sqrt{D}$ et $\sqrt{D} \mp A$ est situs.

IV. Hinc a potiori $\sqrt{D} + B \mp A$ positivus, et quia $\sqrt{D} - B \mp A = -q$ est negativus, $\pm A$ situs erit inter $\sqrt{D} + B$ et $\sqrt{D} - B$. Q. E. D.

Ex. Proposita sit forma $(67, 97, 140)$, cuius determinans $= 29$. Hic invenitur progressio formarum $(67, 97, 140)$, $(140, -97, 67)$, $(67, -37, 20)$, $(20, -3, -1)$, $(-1, 5, 4)$. Ultima erit quaesita.

Tales formas (A, B, C) determinantis positivi non-quadrati D, in quibus A positive acceptus iacet inter $\sqrt{D} + B$ et $\sqrt{D} - B$, B vero positivus est atque $< \sqrt{D}$, *formas reductas* vocabimus. Formae itaque reductae determinantis positivi non-quadrati aliquantum differunt a formis reductis determinantis negativi; sed propter magnam analogiam inter has et illas, denominationes diversas introducere noluimus.

184.

Si aequivalentia duarum formarum *reductarum* determinantis positivi aeque facile dignosci posset, ut in formis determinantis negativi (art. 172), aequivalentiam duarum formarum *quarumcunque* eiusdem determinantis positivi nullo negotio diiudicare possemus. Sed hic res longe aliter se habet, fierique potest ut permultae formae reductae inter se aequivalentes sint. Antequam itaque problema hoc aggrediamur, profundius in naturam formarum reductarum (determinantis positivi non-quadrati, quod semper hic subintelligendum) inquirere necesse erit.

1) Si (a, b, c) est forma reducta, a et c signa opposita habebunt. Nam posito determinante formae $= D$, erit $ac = bb - D$, adeoque, propter $b < \sqrt{D}$ negativus.

2) Numerus c perinde ut a, positive acceptus, inter $\sqrt{D} + b$ et $\sqrt{D} - b$ situs erit. Nam $-c = \frac{D - bb}{a}$; quare, abstractione facta a signo, c iacebit inter $\frac{D-bb}{\sqrt{D}+b}$ et $\frac{D-bb}{\sqrt{D}-b}$ *i. e.* inter $\sqrt{D} - b$ et $\sqrt{D} + b$.

3) Hinc patet, etiam (c, b, a) fore formam reductam.

4) Tum a tum c erunt $< 2\sqrt{D}$. Uterque enim est $< \sqrt{D} + b$, adeoque a potiori $< 2\sqrt{D}$.

5) Numerus b situs erit inter $\sqrt{D}$ et $\sqrt{D} \mp a$ (accepto signo superiori quando a positivus, inferiori quando est negativus). Quia enim $\pm a$ iacet inter $\sqrt{D} + b$ et $\sqrt{D} - b$, erit $\pm a - (\sqrt{D} - b)$, sive $b - (\sqrt{D} \mp a)$ positivus; $b - \sqrt{D}$ autem est negativus; quamobrem b inter $\sqrt{D}$ et $\sqrt{D} \mp a$ erit situs. Prorsus eodem modo demonstratur, b inter $\sqrt{D}$ et $\sqrt{D} \mp c$ iacere (prout c pos. vel neg.).

6) *Cuivis formae reductae (a, b, c) ab utraque parte contigua est reducta una, et non plures.*

Fiat $a' = c$, $b' \equiv -b \pmod{a'}$ et inter $\sqrt{D}$ et $\sqrt{D} \mp a'$ situs *), $c' = \frac{b'b' - D}{a'}$, eritque forma (a', b', c') formae (a, b, c) ab ultima parte contigua, simulque manifestum est, si ulla forma reducta formae (a, b, c) ab ultima parte contigua detur, eam ab hac (a', b', c') diversam esse non posse. Hanc vero revera esse reductam, ita demonstramus.

A) Si ponitur

$$\sqrt{D} + b \mp a' = p, \quad \pm a' - (\sqrt{D} - b) = q, \quad \sqrt{D} - b = r$$

hi p, q, r ex (2) supra et defin. formae reductae erunt positivi. Porro ponatur

$$b' - (\sqrt{D} \mp a') = q', \quad \sqrt{D} - b' = r'$$

eruntque q', r' positivi, quia b' iacet inter $\sqrt{D}$ et $\sqrt{D} \mp a'$. Denique sit $b + b' = \pm m a'$ eritque m integer. Iam patet esse $p + q' = b + b'$, adeoque $b + b'$ sive $\pm m a'$ positivum, et proin etiam m; unde sequitur $m - 1$ certe non esse negativum. Porro fit

$$r + q' \pm m a' = 2b' \pm a', \quad \text{sive} \quad 2b' = r + q' \pm (m-1) a'$$

unde $2b'$ et b' necessario erunt positivi. Et quoniam $b' + r' = \sqrt{D}$, erit $b' < \sqrt{D}$.

B) Porro fit

$$r \pm m a' = \sqrt{D} + b', \quad \text{sive} \quad r \pm (m-1) a' = \sqrt{D} + b' \mp a'$$

quare $\sqrt{D} + b' \mp a'$ erit positivus. Hinc et quoniam $\pm a' - (\sqrt{D} - b') = q'$,

*) Ubi signa ambigua sunt, superiora semper valent quando a' est positivus, inferiora quando a' negativus.

adeoque positivus, $\pm a'$ iacebit inter $\sqrt{D}+b'$ et $\sqrt{D}-b'$. — Quocirca (a',b',c') erit forma reducta.

Eodem modo demonstratur, si fiat $'c=a$, $'b\equiv -b \pmod{'c}$ et inter $\sqrt{D}$ et $\sqrt{D}\pm{}'c$ situs, $'a=\frac{'b'b-D}{c}$, formam $('a,'b,'c)$ fore reductam. Manifesto autem forma haec formae (a,b,c) a parte prima est contigua, aliaque reducta praeter $('a,'b,'c)$ hac proprietate praedita esse non poterit.

Ex. Formae reductae $(5,11,-14)$, cuius determinans $=191$, a parte ultima contigua reducta $(-14,3,13)$, a parte prima vero haec $(-22,9,5)$.

7) Si formae reductae (a,b,c) a parte ultima contigua est reducta (a',b',c'), reductae (c,b,a) contigua erit a prima parte forma (c',b',a'); et si reductae (a,b,c) a prima parte contigua est forma $('a,'b,'c)$, reductae (c,b,a) reducta $('c,'b,'a)$ contigua erit ab ultima parte. Porro etiam formae $(-'a,'b,-'c)$, $(-a,b,-c)$, $(-a',b',-c')$ reductae erunt, et secunda primae, tertia secundae ab ultima parte contiguae, sive prima secundae, secundaque tertiae a parte prima; similiterque tres formae $(-c',b',-a')$, $(-c,b,-a)$, $(-'c,'b,-'a)$. Haec tam obvia sunt ut explicatione non egeant.

185.

Multitudo omnium formarum reductarum determinantis dati D semper est finita, ipsae vero duplici modo inveniri possunt. Designemus indefinite omnes formas reductas determinantis D per (a,b,c), ita ut omnes valores ipsorum a,b,c determinare oporteat.

Methodus prima. Accipiantur pro a omnes numeri (tum positive, tum negative) minores quam $2\sqrt{D}$, quorum residuum quadraticum D, et pro singulis a, ponatur b aequalis omnibus valoribus positivis expr. $\sqrt{D} \pmod{a}$ inter $\sqrt{D}$ et $\sqrt{D}\mp a$ iacentibus, c vero pro singulis valoribus determinatis ipsorum a,b ponatur $=\frac{bb-D}{a}$. Si quae formae hoc modo oriuntur, in quibus $\pm a$ extra $\sqrt{D}+b$ et $\sqrt{D}-b$ situs est, reiiciendae sunt.

Methodus secunda. Accipiantur pro b omnes numeri positivi minores quam $\sqrt{D}$, pro singulis b resolvatur $bb-D$ omnibus quibus fieri potest modis in binos factores, qui neglecto signo inter $\sqrt{D}+b$ et $\sqrt{D}-b$ iaceant, ponaturque alter $=a$, alter $=c$. Manifestum est, singulas resolutiones in factores praebere binas formas, quia uterque factor tum $=a$, tum $=c$ poni debet.

Ex. Sit $D=79$ eruntque valores ipsius a viginti duo $\mp 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15$. Unde inveniuntur formae undeviginti:

$(1,8,-15)$, $(2,7,-15)$, $(3,8,-5)$, $(3,7,-10)$, $(5,8,-3)$, $(5,7,-6)$, $(6,7,-5)$, $(6,5,-9)$, $(7,4,-9)$, $(7,3,-10)$, $(9,5,-6)$, $(9,4,-7)$, $(10,7,-3)$, $(10,3,-7)$, $(13,1,-6)$, $(14,3,-5)$, $(15,8,-1)$, $(15,7,-2)$, $(15,2,-5)$

totidemque aliae quae fiunt ex his, si terminorum exterorum signa commutantur, puta $(-1,8,15)$, $(-2,7,15)$ etc., ita ut omnes triginta octo sint. Sed ex his reiiciendae sex $(\pm 13,1,\mp 6)$, $(\pm 14,3,\mp 5)$, $(\pm 15,2,\mp 5)$, reliquae triginta duae omnes reductas amplectuntur. Per methodum secundam eaedem formae prodeunt sequenti ordine*):

$(\pm 7,3,\mp 10)$, $(\pm 10,3,\mp 7)$, $\pm 7,4,\mp 9)$, $(\pm 9,4,\mp 7)$, $(\pm 6,5,\mp 9)$, $(\pm 9,5,\mp 6)$, $(\pm 2,7,\mp 15)$, $(\pm 3,7,\mp 10)$, $(\pm 5,7,\mp 6)$, $(\pm 6,7,\mp 5)$, $(\pm 10,7,\mp 3)$, $(\pm 15,7,\mp 2)$, $(\pm 1,8,\mp 15)$, $(\pm 3,8,\mp 5)$, $(\pm 5,8,\mp 3)$, $(\pm 15,8,\mp 1)$.

186.

Sit F forma reducta determinantis D, ipsique ab ultima parte contigua forma reducta F'; huic iterum ab ultima parte contigua reducta F''; reducta F''' ipsi F'' contigua ab ultima parte etc. Tum patet, omnes formas F', F'', F''' etc. esse prorsus determinatas, et tum inter se tum formae F proprie aequivalentes. Quoniam vero multitudo omnium formarum reductarum determinantis dati est finita, manifestum est, omnes formas in progressione infinita F, F', F'' etc. diversas esse non posse. Ponamus F^m et F^{m+n} esse identicas, eruntque F^{m-1}, F^{m+n-1} reductae, eidem formae reductae a parte prima contiguae, adeoque identicae; hinc eodem modo F^{m-2} et F^{m+n-2} etc. tandemque F et F^n identicae erunt. Quare in progressione F, F', F'' etc., si modo satis longe continuatur, necessario tandem forma prima F recurret; et si supponimus F^n esse primam identicam cum F, sive omnes $F, F', F'' \ldots F^{n-1}$ a forma F diversas: facile perspicitur, omnes formas $F, F', F'' \ldots F^{n-1}$ diversas fore. Complexum harum for-

*) Pro $b=1$, -7 in duos factores, qui neglecto signo inter $\sqrt{79}+1$ et $\sqrt{79}-1$ iaceant, resolvi nequit; quare hic valor est praetereundus, ex eademque ratione valores 2 et 6.

marum vocabimus *periodum formae F*. Si igitur progressio ultra ultimam periodi formam producitur, eaedem formae F, F', F'' etc. iterum prodibunt, progressioque tota infinita F, F', F'' etc. constituta erit ex hac periodo formae F infinities repetita.

Progressio F, F', F'' etc. etiam retro continuari potest, praeponendo formae F reductam $'F$, quae ipsi a parte prima est contigua; huic iterum reductam $''F$, quae ipsi a prima parte contigua etc. Hoc modo habebitur progressio formarum *utrimque* infinita

$$\ldots\ ,\ ''F,\ 'F,\ F,\ F',\ F'',\ F''',\ \ldots$$

perspicieturque facile, $'F$ identicam fore cum F^{n-1}, $''F$ cum F^{n-2} etc. adeoque progressionem etiam a laeva parte e periodo formae F, infinities repetita, esse constitutam.

Si formis F, F', F'' etc. $'F, ''F$ etc. tribuuntur indices $0, 1, 2$ etc. $-1, -2$ etc. generaliterque formae F^m index m, formae ^mF index $-m$, patet, *formas quascunque seriei identicas fore vel diversas, prout ipsarum indices congrui sint vel incongrui secundum modulum n*.

Ex. Periodus formae $(3, 8, -5)$, cuius determinans $= 79$, invenitur haec: $(3, 8, -5)$, $(-5, 7, 6)$, $(6, 5, -9)$, $(-9, 4, 7)$, $(7, 3, -10)$, $(-10, 7, 3)$. Post ultimam iterum prodit $(3, 8, -5)$. Hic itaque $n = 6$.

187.

Eece quasdam observationes generales circa has periodos.

1) Si formae F, F', F'' etc.; $'F, ''F, '''F$ etc. ita exhibentur:

$$(a, b, -a'),\ (-a', b', a''),\ (a'', b'', -a'''),\ \text{etc.};\quad (-'a, 'b, a),\ ('a, ''b, -a),\ (-''a, '''b, 'a)$$

omnes a, a', a'', a''' etc. $'a, ''a, '''a$ etc. *eadem signa* habebunt (art. 184, 1), omnes vero b, b', b'' etc. $'b, ''b$ etc. erunt positivi.

2) Hinc manifestum est, numerum n (multitudinem formarum ex quibus, periodus formae F constat) semper esse *parem*. Etenim terminus primus formae cuiusvis F^m ex hac periodo manifesto idem signum habebit uti terminus primus a formae F, si m est par, oppositum, si m est impar. Quare quum F^n et F identicae sint, n necessario erit par.

3) Algorithmus, per quem numeri b', b'', b''' etc., a'', a''' etc. inveniuntur, ex art. 184, 6 est hic:

$$\begin{aligned}
b' &\equiv -b \pmod{a'} \quad \text{inter limites } \sqrt{D} \text{ et } \sqrt{D} \mp a'; & a'' &= \frac{D - b'b'}{a'} \\
b'' &\equiv -b' \pmod{a''} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ \sqrt{D} \mp a''; & a''' &= \frac{D - b''b''}{a''} \\
b''' &\equiv -b'' \pmod{a'''} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ \sqrt{D} \mp a'''; & a'''' &= \frac{D - b'''b'''}{a'''}
\end{aligned}$$

etc.

ubi in columna secunda signa superiora vel inferiora sunt accipienda, prout a, a', a'' etc. sunt positivi vel negativi. Loco formularum in columna tertia etiam sequentes adhiberi possunt, quae commodiores evadunt, quando D est numerus magnus:

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

etc.

4) Forma quaecunque F^m, in periodo formae F contenta, proprie eandem periodum habet ut F. Scilicet periodus illa erit $F^m, F^{m+1} \ldots F^{n-1}, F, F' \ldots F^{m-1}$, in qua eaedem formae eodemque ordine occurrunt, ut in periodo formae F, et quae ab hac tantummodo respectu initii et finis discrepat.

5) Hinc patet, omnes formas reductas eiusdem determinantis D in periodos *distribui* posse. Accipiatur aliqua harum formarum, F, ad libitum investigeturque ipsius periodus, $F, F', F'' \ldots F^{n-1}$, quam designemus per P. Si haec omnes formas reductas determinantis D nondum amplectitur, sit aliqua in ipsa non contenta G huiusque periodus Q. Tum patet P et Q nullam formam communem habere posse; alioquin enim etiam G in P contenta esse deberet periodique omnino coincideret. Si P et Q omnes formas reductas nondum exhauriunt, aliqua ex deficientibus, H, periodum tertiam, R, suppeditabit, quae neque cum P neque cum Q formam communem habebit. Hoc modo continuare possumus, usquedum omnes formae reductae sint exhaustae. Ita *e. g.* omnes formae reductae determinantis 79 in sex periodos distribuuntur:

I. $(1, 8, -15)$, $(-15, 7, 2)$, $(2, 7, -15)$, $(-15, 8, 1)$.
II. $(-1, 8, 15)$, $(15, 7, -2)$, $(-2, 7, 15)$, $(15, 8, -1)$.
III. $(3, 8, -5)$, $(-5, 7, 6)$, $(6, 5, -9)$, $(-9, 4, 7)$, $(7, 3, -10)$, $(-10, 7, 3)$.
IV. $(-3, 8, 5)$, $(5, 7, -6)$, $(-6, 5, 9)$, $(9, 4, -7)$, $(-7, 3, 10)$, $(10, 7, -3)$.
V. $(5, 8, -3)$, $(-3, 7, 10)$, $(10, 3, -7)$, $(-7, 4, 9)$, $(9, 5, -6)$, $(-6, 7, 5)$.
VI. $(-5, 8, 3)$, $(3, 7, -10)$, $(-10, 3, 7)$, $(7, 4, -9)$, $(-9, 5, 6)$, $(6, 7, -5)$.

6) Vocemus *formas socias*, quae ex iisdem terminis constant, sed ordine inverso positis, ut $(a, b, -a')$, $(-a', b, a)$. Tum facile perspicitur ex art. 184, 7, si periodus formae reductae F sit $F, F', F'' \dots F^{n-1}$, formae F socia f formisque $F^{n-1}, F^{n-2} \dots F''. F'$ resp. sociae sint formae $f', f'' \dots f^{n-2}, f^{n-1}$: periodum formae f fore $f, f', f'' \dots f^{n-2}, f^{n-1}$, adeoque ex totidem formis constare, ut periodum formae F. Periodos formarum sociarum vocabimus *periodos socias*. Ita in exemplo nostro sociae sunt periodi III et VI; IV et V.

7) Sed fieri etiam potest, ut forma f ipsa in periodo sociae suae F occurrat, uti in ex. nostro in periodo I et II, adeoque periodus formae F cum periodo formae f conveniat, sive ut *periodus formae F sibi ipsi sit socia*. Quoties hoc evenit, in hac periodo duae formae ancipites invenientur. Ponamus enim periodum formae F constare e $2n$ formis sive F et F^{2n} esse identicas; porro sit $2m+1$ index formae f in periodo formae F *), sive F^{2m+1} et F sociae. Tum patet etiam F' et F^{2m} fore socias nec non F'' et F^{2m-1} etc., adeoque etiam F^m et F^{m+1}. Sit $F^m = (a^m, b^m, -a^{m+1})$, $F^{m+1} = (-a^{m+1}, b^{m+1}, a^{m+2})$. Tum erit $b^m + b^{m+1} \equiv 0 \pmod{a^{m+1}}$; ex defin. formarum sociarum vero erit $b^m \equiv b^{m+1}$ atque hinc $2b^{m+1} \equiv 0 \pmod{a^{m+1}}$, sive forma F^{m+1} anceps. — Eodem modo F^{2m+1} et F^{2n} erunt sociae; hinc F^{2m+2} et F^{2n-1}; F^{2m+3} et F^{2n-2} etc. tandemque F^{m+n} et F^{m+n+1}, quarum posterior erit anceps, uti per simile ratiocinium facile probatur. Quia vero $m+1$ et $m+n+1$ secundum mod. $2n$ sunt incongrui, formae F^{m+1} et F^{m+n+1} identicae non erunt (art. 186, ubi n idem denotat, quod hic $2n$). Ita in I sunt formae ancipites $(1, 8, -15)$, $(2, 7, -15)$, in II vero $(-1, 8, 15)$, $(-2, 7, 15)$.

*) Index hic necessario erit impar, quia manifesto termini primi formarum F, f signa opposita habent (*vid. supra*, 2).

8) Vice versa, *quaevis periodus, in qua forma anceps occurrit, sibi ipsi socia est.* Facile enim perspicitur, si F^m sit forma reducta anceps: formam ipsi sociam (quae etiam est reducta) simul ipsi a parte prima contiguam esse, *i. e.* F^{m-1} et F^m socias. Tum vero tota periodus sibi ipsi socia erit. — Hinc patet, *fieri non posse, ut unica tantum forma anceps in periodo aliqua contenta sit.*

9) Sed etiam *plures quam duae in eadem periodo esse nequeunt.* Ponamus enim in periodo formae F, ex $2n$ formis constante, tres formas ancipites dari F^λ, F^μ, F^ν, ad indices λ, μ, ν respective pertinentes, ita ut λ, μ, ν sint numeri inaequales inter limites 0 et $2n-1$ (incl.) siti. Tum formae $F^{\lambda-1}$ et F^λ erunt sociae; similiterque $F^{\lambda-2}$ et $F^{\lambda+1}$ etc. tandemque F et $F^{2\lambda-1}$. Ex eadem ratione F et $F^{2\mu-1}$ sociae erunt, nec non F et $F^{2\nu-1}$; quare $F^{2\lambda-1}$, $F^{2\mu-1}$, $F^{2\nu-1}$ identicae, indicesque $2\lambda-1$, $2\mu-1$, $2\nu-1$ secundum modulum $2n$ congrui erunt, et proin etiam $\lambda \equiv \mu \equiv \nu \pmod{n}$. *Q. E. A.* quia manifesto inter limites 0 et $2n-1$ tres numeri diversi secundum modulum n congrui iacere nequeunt.

188.

Quum omnes formae ex eadem periodo proprie sint aequivalentes, quaestio oritur, annon etiam formae e periodis diversis proprie aequivalentes esse possint. Sed antequam ostendamus, *hoc esse impossibile*, quaedam de transformatione formarum reductarum sunt exponenda.

Quoniam in sequentibus de formarum transformationibus persaepe agendum erit: ut prolixitatem quantum fieri potest evitemus, sequenti scribendi compendio abhinc semper utemur. Si forma aliqua $LXX + 2MXY + NYY$ per substitutionem $X = \alpha x + \delta y$, $Y = \gamma x + \delta y$ in formam $lxx + 2mxy + nyy$ transformatur: simpliciter dicemus, (L, M, N) transformari in (l, m, n) per substitutionem $\alpha, \delta, \gamma, \delta$. Hoc modo opus non erit, indeterminatas formarum singularum, de quibus agitur, per signa propria denotare. — Palam vero est, indeterminatam *primam* a *secunda* in quavis forma probe distingui debere.

Proposita sit forma reducta $(a, b, -a') \dots f$, determinantis D. Formetur simili modo ut in art. 186 progressio formarum reductarum utrimque infinita, $\dots f'', f', f, f', f'' \dots$ et quidem sit

$$f' = (-a', b', a''), \quad f''' = (a'', b'', -a''') \quad \text{etc.}$$
$$'f = (-'a, 'b, a), \quad ''f = (''a, ''b, -'a) \quad \text{etc.}$$

Ponatur

$$\frac{b+b'}{-a'} = k, \quad \frac{b'+b''}{a''} = k'', \quad \frac{b''+b'''}{-a'''} = k''' \quad \text{etc.}$$
$$\frac{'b+b}{a} = h, \quad \frac{''b+'b}{-'a} = 'h, \quad \frac{'''b+''b}{''a} = ''h \quad \text{etc.}$$

Tum patet, si (ut in art. 177) numeri $\alpha', \alpha'', \alpha'''$ etc. $\vec{\alpha}', \vec{\alpha}'', \vec{\alpha}'''$ etc. etc. formentur secundum algorithmum sequentem

$\alpha' = 0$	$\vec{\alpha}' = -1$	$\gamma' = 1$	$\vec{\gamma}' = k$
$\alpha'' = \vec{\alpha}'$	$\vec{\alpha}'' = k''\vec{\alpha}'$	$\gamma'' = \vec{\gamma}'$	$\vec{\gamma}'' = k''\vec{\gamma}' - 1$
$\alpha''' = \vec{\alpha}''$	$\vec{\alpha}''' = k'''\vec{\alpha}'' - \vec{\alpha}'$	$\gamma''' = \vec{\gamma}''$	$\vec{\gamma}''' = k'''\vec{\gamma}'' - \vec{\gamma}'$
$\alpha'''' = \vec{\alpha}'''$	$\vec{\alpha}'''' = k''''\vec{\alpha}''' - \vec{\alpha}''$	$\gamma'''' = \vec{\gamma}'''$	$\vec{\gamma}'''' = k''''\vec{\gamma}''' - \vec{\gamma}''$

etc.

f transformatum iri

in f'	per substitutionem	α',	$\vec{\alpha}'$, γ', $\vec{\gamma}'$
f''		α'',	$\vec{\alpha}''$, γ'', $\vec{\gamma}''$
f'''		α''',	$\vec{\alpha}'''$, γ''', $\vec{\gamma}'''$

etc.

omnesque has transformationes fore proprias.

Quum $'f$ transeat in f per substitutionem propriam $0, -1, 1, h$ (art. 158): f transibit in $'f$ per subst. prop. $h, 1, -1, 0$. Ex simili ratione $'f$ transibit in $''f$ per subst. propr. $''h, 1, -1, 0$; $''f$ in $'''f$ per subst. pr. $'''h, 1, -1, 0$ etc. Hinc per art. 159 eodem modo ut art. 177 colligitur, si numeri $'\alpha, ''\alpha, '''\alpha$ etc. $'\vec{\alpha}, ''\vec{\alpha}, '''\vec{\alpha}$ etc. etc. formentur secundum algorithmum sequentem

$'\alpha = h$	$'\vec{\alpha} = 1$	$'\gamma = -1$	$'\vec{\gamma} = 0$
$''\alpha = 'h\,'\alpha - 1$	$''\vec{\alpha} = 'a$	$''\gamma = 'h\,'\gamma$	$''\vec{\gamma} = 'c$
$'''\alpha = ''h\,''\alpha - 'a$	$'''\vec{\alpha} = ''\alpha$	$'''\gamma = ''h\,''\gamma - 'c$	$'''\vec{\gamma} = ''c$
$''''\alpha = '''h\,'''\alpha - ''\alpha$	$''''\vec{\alpha} = '''\alpha$	$''''\gamma = '''h\,'''\gamma - ''c$	$''''\vec{\gamma} = '''c$

etc.

f transformatum iri

in $'f$	per substitutionem	$'\alpha$,	$'\vec{\alpha}$, $'\gamma$, $'\vec{\gamma}$
$''f$		$''\alpha$,	$''\vec{\alpha}$, $''\gamma$, $''\vec{\gamma}$
$'''f$		$'''\alpha$,	$'''\vec{\alpha}$, $'''\gamma$, $'''\vec{\gamma}$

etc.

omnesque has transformationes fore proprias.

Si ponitur $\alpha = 1$, $\vec{\alpha} = 0$, $\gamma = 0$, $\vec{\gamma} = 1$: hi numeri eandem relationem habebunt ad formam f, quam habent $\alpha', \vec{\alpha}', \gamma', \vec{\gamma}'$ ad f'; $\alpha'', \vec{\alpha}'', \gamma'', \vec{\gamma}''$ ad f'' etc.; $'\alpha, '\vec{\alpha}, '\gamma, '\vec{\gamma}$ ad $'f$ etc. Scilicet per substitutionem $\alpha, \vec{\alpha}, \gamma, \vec{\gamma}$ forma f transibit in f. Tum vero progressiones infinitae $\alpha', \alpha'', \alpha'''$ etc., $'\alpha, ''\alpha, '''\alpha$ etc., per intercalationem termini α, concinne iungentur ita ut unam continuam utrimque infinitam constituere concipi possint secundum eandem legem ubique progredientem $\ldots '''\alpha, ''\alpha, '\alpha, \alpha, \alpha', \alpha'', \alpha''' \ldots$ Lex progressionis haec est:

$$'''\alpha + ''\alpha = ''h\,''\alpha, \quad ''\alpha + '\alpha = 'h\,'\alpha, \quad '\alpha + \alpha = h\alpha, \quad \alpha + \alpha' = k\alpha', \quad \alpha' + \alpha'' = h''\alpha' \text{ etc.}$$

sive generaliter (si indicem negativum a dextra scriptum idem designare supponimus, ac positivum a laeva)

$$\alpha^{m-1} + \alpha^{m+1} = h^m \alpha^m$$

Simili modo progressio $\ldots ''\vec{\alpha}, '\vec{\alpha}, \vec{\alpha}, \vec{\alpha}', \vec{\alpha}'' \ldots$ continua erit, cuius lex

$$\vec{\alpha}^{m-1} + \vec{\alpha}^{m+1} = h^{m+1}\vec{\alpha}^m$$

et proprie cum praecedente identica, omnibus terminis uno loco promotis. $''\vec{\alpha} = '\alpha, '\vec{\alpha} = \alpha, \vec{\alpha} = \alpha'$ etc. Lex progressionis continuae $\ldots ''\gamma, '\gamma, \gamma, \gamma', \gamma'' \ldots$ erit haec

$$\gamma^{m-1} + \gamma^{m+1} = h^m \gamma^m$$

et lex huius $\ldots ''\vec{\gamma}, '\vec{\gamma}, \vec{\gamma}, \vec{\gamma}', \vec{\gamma}'' \ldots$ erit

$$\vec{\gamma}^{m-1} + \vec{\gamma}^{m+1} = h^{m+1}\vec{\gamma}^m$$

insuperque generaliter $\vec{\gamma}^m = \gamma^{m+1}$.

Ex. Sit forma proposita f haec $(3, 8, -5)$, quae transformabitur

in formam $''''f$	$(-10, 7, 3)$	per substitutionem	-805,	-152,	$+143$, $+27$
$'''f$	$(3, 8, -5)$		-152,	$+45$,	$+27$, -8
$''f$	$(-5, 7, 6)$		$+45$,	$+17$,	-8, -3
$'f$	$(6, 5, -9)$		$+17$,	-11,	-3, $+2$
f	$(-9, 4, 7)$		-11,	-6,	$+2$, $+1$
f'	$(7, 3, -10)$		-6,	$+5$,	$+1$, -1
f''	$(-10, 7, 3)$		$+5$,	$+1$,	-1, 0
f'''	$(3, 8, -5)$		$+1$,	0,	0, $+1$
f''''	$(-5, 7, 6)$		0,	-1,	$+1$, -3
f'''''	$(6, 5, -9)$		-1,	-2,	-3, -7
f''''''	$(-9, 4, 7)$		-2,	$+3$,	-7, $+10$
f'''''''	$(7, 3, -10)$		$+3$,	$+5$,	$+10$, $+17$
f''''''''	$(-10, 7, 3)$		$+5$,	-8,	$+17$, -27
f'''''''''	$(3, 8, -5)$		-8,	-45,	-27, -152
f''''''''''	$(-5, 7, 6)$		-45,	$+143$,	-152, $+483$

etc.

189.

Circa hunc algorithmum sequentia sunt annotanda:

1) Omnes a, a', a'' etc., $'a, ''a$ etc. eadem signa habebunt; omnes b, b', b'' etc. $'b, ''b$ etc. erunt positivi; in progressione $\ldots ''h, 'h, h, h', h'' \ldots$ signa alternabunt, scilicet si omnes a, a' etc. sunt positivi, h^m vel $^m h$ erit positivus quando m est par, negativus quando m impar; si vero a, a' etc. sunt negativi, h^m vel $^m h$ pro m pari erit negativus, pro impari positivus.

2) Si a est positivus adeoque h' negativus, h'' positivus etc., erit $\alpha'' = +1$ neg., $\alpha''' = h''\alpha''$ neg. et $> \alpha''$ (vel $= \alpha''$ si $h'' = 1$); $\alpha'''' = h'''\alpha''' - \alpha''$ pos. et $> \alpha'''$ (quia $h'''\alpha'''$ pos., α'' neg.); $\alpha''''' = h''''\alpha'''' - \alpha'''$ pos. et $> \alpha''''$ (quia $h''''\alpha''''$ pos.) etc. Hinc facile concluditur, progressionem $\alpha', \alpha'', \alpha'''$ etc. in infinitum crescere duoque signa positiva semper duo negativa excipere ita ut α^m habeat signum $+, +, -, -$, prout $m \equiv 0, 1, 2, 3 \pmod 4$. Si a est negativus, per simile ratiocinium invenitur α'' neg., α''' pos. et vel $>$ vel $= \alpha''$; α'''' pos. $> \alpha'''$; α''''' neg. $> \alpha''''$ etc.,

ita ut progressio $\alpha', \alpha'', \alpha'''$ etc. continuo crescat, signumque termini α^m sit $+, -, -, +$, prout $m \equiv 0, 1, 2, 3 \pmod 4$.

3) Hoc modo invenitur, omnes quatuor progressiones infinitas $\alpha', \alpha'', \alpha'''$ etc. $\gamma, \gamma', \gamma''$ etc.; $\alpha, {}'\alpha, {}''\alpha$ etc.; $\gamma, {}'\gamma, {}''\gamma$ etc. continuo crescere, adeoque etiam sequentes cum illis identicas: $\vec{\alpha}, \vec{\alpha}', \vec{\alpha}''$ etc.; ${}'\hat{\alpha}, \hat{\alpha}, \hat{\alpha}', \hat{\alpha}''$ etc.; $\vec{\alpha}, {}'\vec{\alpha}, {}''\vec{\alpha}$ etc.; ${}'\hat{\alpha}, {}''\hat{\alpha}$ etc.; et, prout $m \equiv 0, 1, 2, 3 \pmod 4$, signum

ipsius α^m, $+ \pm - \mp$; ipsius $\vec{\alpha}^m$, $\pm - \mp +$

ipsius γ^m, $\pm + \mp -$; ipsius $\hat{\alpha}^m$, $+ \mp - \pm$

ipsius ${}^m\alpha$, $+ \pm - \mp$; ipsius ${}^m\vec{\alpha}$, $\mp + \pm -$

ipsius ${}^m\gamma$, $\mp - \pm +$; ipsius ${}^m\hat{\alpha}$, $+ \mp - \pm$

valentibus superioribus quando a est positivus, inferioribus quando a negativus. Teneatur imprimis haec proprietas: Designante m indicem quemcunque positivum, α^m et γ^m habebunt eadem signa quando a positivus, opposita quando a negativus, similiterque $\vec{\alpha}^m$ et $\hat{\alpha}^m$; contra ${}^m\alpha$ et ${}^m\gamma$, vel ${}^m\vec{\alpha}$ et ${}^m\hat{\alpha}$ habebunt eadem signa quando a negativus, opposita quando a positivus.

4) In signis art. 27 magnitudo ipsorum α^m etc. concinne ita exhiberi potest, ponendo

$$\mp k' = k', \quad \pm k' = k'', \quad \mp k'' = k''' \text{ etc.} \quad \pm h = k, \quad \mp {}'h = {}'k, \quad \pm {}''h = {}''k \text{ etc.}$$

ita ut omnes k', k'' etc. $k, {}'k$ etc. sint numeri positivi:

$$\alpha^m = \pm [k', k'', k''' \ldots k^{m-1}]; \quad \vec{\alpha}^m = \pm [k'', k''', k'''' \ldots k^m]$$

$$\gamma^m = \pm [k', k'', k'' \ldots k^{m-1}]; \quad \hat{\alpha}^m = \pm [k', k'', k''' \ldots k^m]$$

$${}^m\alpha = \pm [k, {}'k, {}''k \ldots {}^{m-1}k]; \quad {}^m\vec{\alpha} = \pm [k, {}'k, {}''k \ldots {}^{m-2}k]$$

$${}^m\gamma = \pm [{}'k, {}''k \ldots {}^{m-1}k]; \quad {}^m\hat{\alpha} = \pm [{}'k, {}''k \ldots {}^{m-2}k]$$

signa vero ad praecepta modo tradita determinari debent. Secundum has formulas, quarum demonstrationem propter facilitatem omittimus, calculus semper expeditissime absolvi poterit.

190.

LEMMA. *Designantibus* m, μ, m', n, ν, n' *numeros integros quoscunque, ita tamen ut trium posteriorum nullus sit* $=0$: *dico, si* $\frac{\mu}{\nu}$ *iacet inter limites* $\frac{m}{n}$ *et* $\frac{m'}{n'}$ *exclusive, atque sit* $mn' - nm' = \mp 1$, *denominatorem* ν *fore maiorem quam* n *et* n'.

Dem. Manifesto $\mu nn'$ iacebit inter $\nu mn'$ et $\nu nm'$, adeoque ab utroque limite minus differet quam limes alter ab altero, *i. e.* erit $\nu mn' - \nu nm' > \mu nn' - \nu mn'$ et $> \mu nn' - \nu nm'$, sive $\nu > n'(\mu n - \nu m)$ et $> n(\mu n' - \nu m')$. Hinc sequitur, quoniam $\mu n - \nu m$ certe non $= 0$ (alioquin enim foret $\frac{\mu}{\nu} = \frac{m}{n}$ contra hyp.), neque $\mu n' - \nu m' = 0$ (ex simili ratione), sed uterque ad minimum $= 1$, fore $\nu > n'$ et $> n$. *Q. E. D.*

Perspicuum itaque est, ν non posse esse $=1$, *i. e.* si fuerit $mn' - nm' = \mp 1$, inter fractiones $\frac{m}{n}, \frac{m'}{n'}$ nullum numerum integrum iacere posse. Quare etiam cifra inter ipsas iacere nequit, *i. e.* fractiones istae signa opposita habere nequeunt.

191.

THEOREMA. *Si forma reducta* $(a, b, -a')$ *determinantis* D *per substitutionem* $\alpha, \beta, \gamma, \delta$ *transit in reductam* $(A, B, -A')$ *eiusdem determinantis: iacebit, primo,* $\frac{\pm\sqrt{D}-b}{a}$ *inter* $\frac{\alpha}{\gamma}$ *et* $\frac{\beta}{\delta}$ *(siquidem neque* γ *neque* $\delta = 0$, *i. e. si uterque limes est finitus), accepto signo superiori, quando neuter horum limitum habet signum signo ipsius* a *oppositum (sive clarius, quando aut uterque idem habet, aut alter idem, alter est* $= 0$*), inferiori quando neuter habet idem ut* a; secundo $\frac{\pm\sqrt{D}+b}{a}$ *inter* $\frac{\gamma}{\alpha}$ *et* $\frac{\delta}{\beta}$ *(siquidem neque* α *neque* $\beta = 0$*), signo superiori accepto quando limes neuter signum signo ipsius* a' *(vel* a*) oppositum habet, inferiori quando neuter habet idem ut* a' **).*

Dem. Habentur aequationes

$$a\alpha\alpha + 2b\alpha\gamma - a'\gamma\gamma = A \quad \ldots\ldots\ldots [1]$$

$$a\beta\beta + 2b\beta\delta - a'\delta\delta = -A' \quad \ldots\ldots\ldots [2]$$

Unde deducitur

$$\frac{\alpha}{\gamma} = \frac{\pm\sqrt{(D + \frac{aA}{n})} - b}{a} \quad \ldots\ldots\ldots [3]$$

$$\frac{\beta}{\delta} = \frac{\pm\sqrt{(D - \frac{aA'}{\delta\delta})} - b}{a} \quad \ldots\ldots\ldots [4]$$

*) Manifestum est, alios casus locum habere non posse, quum ex art. praec. propter $\alpha\delta - \beta\gamma = \pm 1$, limites bini neque signa opposita habere, neque simul $= 0$ esse possint.

$$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{(D - \frac{a'A}{\gamma\gamma})} + b}{a'} \quad \ldots\ldots\ldots [5]$$

$$\frac{\delta}{\beta} = \frac{\pm\sqrt{(D + \frac{a'A'}{\beta\beta})} + b}{a'} \quad \ldots\ldots\ldots [6]$$

Aequatio 3, 4, 5, 6 reiicienda erit, si $\gamma, \delta, \alpha, \beta$ resp. $= 0$. — Sed dubium hic manet, quae *signa* quantitatibus radicalibus tribui debeant; hoc sequenti modo decidemus.

Statim patet in [3] et [4] necessario signa superiora accipi debere, quando neque $\frac{\alpha}{\gamma}$ neque $\frac{\beta}{\delta}$ signum habeat signo ipsius a oppositum; quoniam accepto signo inferiori $\frac{a\alpha}{\gamma}$ et $\frac{a\beta}{\delta}$ fierent quantitates negativae. Quia vero A et A' signa eadem habent, $\sqrt{D}$ cadet inter $\sqrt{(D + \frac{aA}{\gamma\gamma})}$ et $\sqrt{(D - \frac{aA'}{\delta\delta})}$ adeoque in hocce casu $\frac{\sqrt{D}-b}{a}$ inter $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$. Quare pars prima theorematis pro casu priori est demonstrata.

Eodem modo perspicitur, in [5] et [6] necessario signa inferiora accipi debere, quando neque $\frac{\gamma}{\alpha}$ neque $\frac{\delta}{\beta}$ signum idem habeant ut a' sive a, quia accepto superiori $\frac{a'\gamma}{\alpha}$, $\frac{a'\delta}{\beta}$ necessario fierent quantitates positivae. Unde protinus sequitur, $\frac{-\sqrt{D}+b}{a'}$ pro hocce casu iacere inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$. Demonstrata est itaque etiam pars secunda theorematis pro casu posteriori. Quodsi aeque facile ostendi posset, in [3] et [4] signa inferiora accipi debere, quando neutra quantitatum $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ signum idem habeat ut a, et in [5] et [6] superiora, quando neque $\frac{\gamma}{\alpha}$ neque $\frac{\delta}{\beta}$ signum oppositum habeat: hinc simili modo sequeretur, pro illo casu $\frac{-\sqrt{D}-b}{a}$ iacere inter $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$, pro hoc $\frac{\sqrt{D}+b}{a'}$ inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$, sive pars prima theorematis etiam pro casu posteriori, et secunda pro casu priori demonstratae forent. Sed quum illud difficile quidem non sit, attamen sine quibusdam ambagibus fieri nequeat, methodum sequentem praeferimus.

Quando nullus numerorum $\alpha, \beta, \gamma, \delta = 0$, $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ eadem signa habebunt ut $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$. Quando itaque neutra harum quantitatum signum idem habet ut a' sive a, adeoque $\frac{-\sqrt{D}+b}{a'}$ inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$ cadit: neutra quantitatum $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ signum idem ut a habebit, cadetque $\frac{a'}{-\sqrt{D}+b} = \frac{-\sqrt{D}-b}{a}$ (propter $aa' = D - bb$) inter $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$. Quare pro eo casu ubi neque α neque $\beta = 0$, pars prima theor. etiam pro casu secundo est demonstrata (nam conditio ut neque γ neque $\delta = 0$, iam in theor. ipso est adiecta). Simili modo, quando nullus numerorum $\alpha, \beta, \gamma, \delta = 0$,

et neque $\frac{\alpha}{\gamma}$ neque $\frac{\beta}{\delta}$ signum signo ipsius a vel a' oppositum habet, adeoque $\frac{\sqrt{D}-b}{a'}$ inter $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ iacet: etiam $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$ signum oppositum signo ipsius a' non habebit, cadetque $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$ inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\beta}$. In eo igitur casu ubi neque γ neque $\delta = 0$ pars secunda theor. etiam pro casu secundo est demonstrata.

Nihil itaque superesset quam ut demonstretur, partem primam theor. etiam pro casu secundo locum habere si alteruter numerorum α, β sit $= 0$, et partem secundam pro casu primo si aut γ aut $\delta = 0$. At *omnes hi casus sunt impossibiles*. Supponamus enim, pro parte *prima* theor., esse neque γ neque $\delta = 0$; $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ non habere signum idem ut a atque esse 1) $\alpha = 0$. Tum ex aequ. $\alpha\delta - \beta\gamma = \pm 1$ fit $\beta = \pm 1$, $\gamma = \pm 1$. Hinc ex [1] $A = -a'$, quare A et a', adeoque etiam a et A' signa opposita habent, unde fit $\sqrt{(D - \frac{aA}{\alpha\alpha})} > \sqrt{D} > b$. Hinc patet in [4] necessario signum inferius accipi debere, quia accepto superiori $\frac{\beta}{\delta}$ manifesto signum idem obtineret ut a. Fit itaque $\frac{\beta}{\delta} > \frac{-\sqrt{D}-b}{a} > 1$ (propter $a < \sqrt{D}+b$ ex def. formae reductae). *Q. E. A.* quum $\beta = \pm 1$, et δ non $= 0$. — 2) Sit $\beta = 0$. Tum ex aequ. $\alpha\delta - \beta\gamma = \pm 1$ fit $\alpha = \pm 1$, $\delta = \pm 1$. Hinc ex [2] $-A' = -a'$, quare a' et a et A signa eadem habebunt, unde fit $\sqrt{(D + \frac{aA}{\alpha\alpha})} > \sqrt{D} > b$. Hinc patet in [3] signum inferius accipi debere, quia accepto superiori $\frac{\alpha}{\gamma}$ signum idem obtineret ut a. Fit itaque $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$, *Q. E. A.* eadem ratione ut ante. — Pro parte *secunda* si supponimus neque α neque $\beta = 0$; $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$ non habere signum signo ipsius a' oppositum atque 1) $\gamma = 0$: ex aequ. $\alpha\delta - \beta\gamma = \pm 1$ fit $\alpha = \pm 1$, $\delta = \pm 1$. Hinc ex [1] $A = a$, quare a' et A' signa eadem habebunt, unde fit $\sqrt{(D + \frac{a'A'}{\beta\beta})} > \sqrt{D} > b$. Quocirca in [6] signum superius erit accipiendum, quia accepto inferiori, $\frac{\delta}{\beta}$ obtineret signum oppositum signo ipsius a'. Fit igitur $\frac{\delta}{\beta} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.*, quia $\delta = \pm 1$ et β non $= 0$. Tandem 2) si esset $\delta = 0$, ex $\alpha\delta - \beta\gamma = \pm 1$ fit $\beta = \pm 1$, $\gamma = \pm 1$, adeoque ex [2] $-A' = a$. Hinc $\sqrt{(D - \frac{a'A}{\alpha\alpha})} > \sqrt{D} > b$, quare in [5] signum superius accipiendum. Hinc $\frac{1}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.* — Quare theorema in omni sua extensione est demonstratum.

Quum differentia inter $\frac{\alpha}{1}$ et $\frac{\beta}{\delta}$ sit $= \frac{1}{\gamma\delta}$; differentia inter $\frac{\pm\sqrt{D}-b}{a}$ et $\frac{\alpha}{\gamma}$ vel $\frac{\gamma}{\delta}$ erit $< \frac{1}{\gamma\delta}$; inter $\frac{\pm\sqrt{D}-b}{a}$ autem et $\frac{\alpha}{1}$, vel inter illam quantitatem et $\frac{\beta}{\delta}$ nulla fractio iacere poterit, cuius denominator non sit maior quam γ aut δ (*lemma praec.*). — Eodem modo differentia quantitatis $\frac{\pm\sqrt{D}+b}{a}$ a fractione $\frac{\gamma}{\alpha}$ vel hac $\frac{\delta}{\beta}$

erit minor quam $\frac{1}{\alpha\beta}$, et inter illam quantitatem et neutram harum fractionum iacere potest fractio cuius denominator non sit maior quam α et β.

192.

Ex applicatione theor. praec. ad algorithmum art. 188 sequitur, quantitatem $\frac{\sqrt{D}-b}{a}$ quam per L designabimus, iacere inter $\frac{\alpha'}{\gamma'}$ et $\frac{\beta'}{\delta'}$; inter $\frac{\alpha''}{\gamma''}$ et $\frac{\beta''}{\delta''}$; inter $\frac{\alpha'''}{\gamma'''}$ et $\frac{\beta'''}{\delta'''}$ etc. (facile enim ex art. 189, 3 fin. deducitur, nullum horum limitum habere signum oppositum signo ipsius a; quare quantitati radicali $\sqrt{D}$ signum positivum tribui debet) sive inter $\frac{\alpha'}{\gamma'}$ et $\frac{\alpha''}{\gamma''}$; inter $\frac{\alpha''}{\gamma''}$ et $\frac{\alpha'''}{\gamma'''}$ etc. Omnes itaque fractiones $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha''''}{\gamma''''}$ etc. ipsi L ab eadem parte iacebunt, omnesque $\frac{\alpha''}{\gamma''}$, $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha''''''}{\gamma''''''}$ etc. a parte altera. Quoniam vero $\gamma' < \gamma'''$, $\frac{\alpha'}{\gamma'}$ iacebit *extra* $\frac{\alpha'''}{\gamma'''}$ et L, similique ratione $\frac{\alpha''}{\gamma''}$ extra L et $\frac{\alpha''''}{\gamma''''}$; $\frac{\alpha'''}{\gamma'''}$ extra L et $\frac{\alpha'''''}{\gamma'''''}$ etc. Unde manifestum est, has quantitates iacere sequenti ordine:

$$\frac{\alpha'}{\gamma'}, \frac{\alpha'''}{\gamma'''}, \frac{\alpha''''''}{\gamma''''''} \ldots L \ldots \frac{\alpha''''''}{\gamma''''''}, \frac{\alpha''''}{\gamma''''}, \frac{\alpha''}{\gamma''}$$

Differentia autem inter $\frac{\alpha'}{\gamma'}$ et L erit minor quam differentia inter $\frac{\alpha''}{\gamma''}$ et $\frac{\alpha''}{\gamma''}$ *i. e.* $< \frac{1}{\gamma'\gamma''}$, similique ratione differentia inter $\frac{\alpha''}{\gamma''}$ et L erit $< \frac{1}{\gamma''\gamma'''}$ etc. Quamobrem fractiones $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$ etc. continuo propius ad limitem L accedunt, et quoniam γ', γ'', γ''' continuo in infinitum crescunt, differentia fractionum a limite quavis quantitate data minor fieri potest.

Ex art. 189 nulla quantitatum $\frac{\gamma}{\alpha}$, $\frac{\gamma'}{\alpha'}$, $\frac{\gamma''}{\alpha''}$ etc. signum idem habebit ut a; hinc per ratiocinia praecedentibus omnino similia sequitur, illas et hanc $\frac{-\sqrt{D}+b}{a'}$, quam per L' designabimus, iacere sequenti ordine:

$$\frac{\gamma}{\alpha}, \frac{\gamma''}{\alpha''}, \frac{\gamma''''}{\alpha''''} \ldots\ldots L' \ldots\ldots \frac{\gamma''''}{\alpha''''}, \frac{\gamma''}{\alpha''}, \frac{\gamma}{\alpha}$$

Differentia autem inter $\frac{\gamma}{\alpha}$ et L' minor erit quam $\frac{1}{\alpha\alpha}$, differentia inter $\frac{\gamma}{\alpha}$ et L' minor quam $\frac{1}{\alpha^2\alpha^2}$ etc. Quare fractiones $\frac{\gamma}{\alpha}$, $\frac{\gamma'}{\alpha'}$ etc. continuo propius ad L' accedent, et differentia quavis quantitate data minor fieri poterit.

In *ex.* art. 188 fit $L = \frac{\sqrt{79}-8}{3} = 0{,}2960648$ et fractiones appropinquantes $\frac{0}{1}$, $\frac{1}{3}$, $\frac{3}{10}$, $\frac{8}{27}$, $\frac{11}{37}$, $\frac{30}{101}$, $\frac{41}{138}$, etc. Est autem $\frac{1}{4}\frac{1}{6}\frac{3}{3} = 0{,}2960662$. — Ibidem fit $L' = \frac{-\sqrt{79}+8}{5} = -0{,}1776388$, fractionesque approximantes $\frac{0}{1}$, $-\frac{1}{5}$, $-\frac{1}{6}$, $-\frac{2}{11}$, $-\frac{3}{17}$, $-\frac{8}{45}$, $-\frac{35}{197}$, $-\frac{43}{242}$ etc. Est vero $\frac{1}{5}\frac{1}{6}\frac{3}{3} = 0{,}1776397$.

193.

THEOREMA. *Si formae reductae f, F proprie aequivalentes sunt: altera in alterius periodo contenta erit.*

Sit $f = (a, b, -a')$, $F = (A, B, -A')$, determinans harum formarum D, transeatque illa in hanc per substitutionem propriam $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$. Tum dico, si periodus formae f quaeratur progressioque utrimque infinita formarum reductarum atque transformationum formae f in ipsas eruatur, eodem modo ut art. 188. *vel* $+\mathfrak{A}$ fore aequalem termino alicui progressionis $\ldots\alpha, \alpha', \alpha, \alpha', \alpha'', \ldots$, hocque posito $= \alpha^m$, $+\mathfrak{B}$ fore $= \delta^m$, $+\mathfrak{C} = \gamma^m$, $+\mathfrak{D} = \delta^m$; *vel* $-\mathfrak{A}$ fore aequalem termino alicui α^m, et $-\mathfrak{B}$, $-\mathfrak{C}$, $-\mathfrak{D}$ resp. $= \delta^m$, γ^m, δ^m (ubi m etiam indicem negativum designare potest). In utroque casu F manifesto identica erit cum f^m.

Dem. I. Habentur quatuor aequationes,

$$a\mathfrak{A}\mathfrak{A} + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}\mathfrak{C} = A \quad \ldots\ldots\ldots [1]$$
$$a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}\mathfrak{D} = B \quad \ldots\ldots [2]$$
$$a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D} = -A' \quad \ldots\ldots [3]$$
$$\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1 \quad \ldots\ldots\ldots\ldots [4]$$

Consideramus autem *primo* casum, ubi aliquis numerorum $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$.

1° Si $\mathfrak{A} = 0$, fit ex [4] $\mathfrak{B}\mathfrak{C} = -1$, adeoque $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. Hinc ex [1], $-a' = A$; ex [2], $-b \pm a'\mathfrak{D} = B$ sive $B \equiv -b \pmod{a'}$ vel A); unde sequitur formam $(A, B, -A')$ formae $(a, b, -a')$ ab ultima parte contiguam esse. Quoniam vero illa est reducta, necessario cum f' identica erit. Ergo $B = b'$, adeoque ex [2] $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$; hinc propter $\frac{b+b'}{-a'} = h'$, fit $\mathfrak{D} = \mp h'$. Unde colligitur, $\mp\mathfrak{A}, \mp\mathfrak{B}, \mp\mathfrak{C}, \mp\mathfrak{D}$ esse resp. $= 0, -1, +1, h'$ sive $= \alpha', \delta', \gamma', \delta'$.

2° Si $\mathfrak{B} = 0$, fit ex [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; ex [3] $a' = A$; ex [2] $b \mp a'\mathfrak{C} = B$, sive $b \equiv B \pmod{a'}$. Quoniam vero tum f tum F sunt formae reductae: tum b tum B iacebunt inter $\sqrt{D}$ et $\sqrt{D} \mp a'$ (prout a' pos. vel neg., art. 185, 5). Quare erit necessario $b = B$, et $\mathfrak{C} = 0$. Hinc formae f, F sunt identicae atque $\pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{C}, \pm\mathfrak{D} = 1, 0, 0, 1 = \alpha, \delta, \gamma\ \delta$ (resp.).

3° Si $\mathfrak{C} = 0$, fit ex [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; ex [1] $a = A$; ex [2] $\pm a\mathfrak{B} + b = B$ sive $b \equiv B \pmod{a}$. Quia vero tum b tum B iacent inter $\sqrt{D}$ et $\sqrt{D} \mp a$: erit necessario $B = b$ et $\mathfrak{B} = 0$. Quare casus hic a praecedente non differt.

4° Si $\mathfrak{D} = 0$, fit ex [4] $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$; ex [3] $a = -A'$; ex [2] $\pm a\mathfrak{A} - b = B$ sive $B \equiv -b \pmod{a}$. Hinc forma F formae f a parte prima contigua erit, et proin cum forma f identica. Quare propter $\frac{b+b'}{a} = h$, et $B = b$, erit $\mp\mathfrak{A} = h$. Unde colligitur $\pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{C}, \pm\mathfrak{D}$ resp. esse $= h, 1, -1, 0$. $= \alpha, \delta, \gamma, \delta$. ...

Superest itaque casus ubi nullus numerorum $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$. Hic per Lemma art. 190 quantitates $\frac{\mathfrak{A}}{\mathfrak{C}}, \frac{\mathfrak{B}}{\mathfrak{D}}, \frac{\mathfrak{C}}{\mathfrak{A}}, \frac{\mathfrak{D}}{\mathfrak{B}}$ idem signum habebunt, oriunturque inde duo casus, quum signum hoc vel cum signo ipsorum a, a' convenire vel ipsi oppositum esse possit.

II. Si $\frac{\mathfrak{A}}{\mathfrak{C}}, \frac{\mathfrak{B}}{\mathfrak{D}}$ idem signum habent ut a: quantitas $\frac{\sqrt{D}-b}{a}$ (quam designabimus per L) inter has fractiones sita erit (art. 191). Demonstrabimus iam, $\frac{\mathfrak{A}}{\mathfrak{C}}$ aequalem fore alicui fractionum $\frac{\alpha''}{\gamma''}, \frac{\alpha'''}{\gamma'''}, \frac{\alpha''''}{\gamma''''}$ etc., atque $\frac{\mathfrak{B}}{\mathfrak{D}}$ proxime sequenti, scilicet si $\frac{\mathfrak{A}}{\mathfrak{C}}$ fuerit $= \frac{\alpha^m}{\gamma^m}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ fore $= \frac{\alpha^{m+1}}{\gamma^{m+1}}$. In art. praec. ostendimus, quantitates $\frac{\alpha'}{\gamma'}, \frac{\alpha''}{\gamma''}, \frac{\alpha'''}{\gamma'''}$ etc. (quas brevitatis gratia per (1), (2), (3) etc. denotabimus), atque L, hunc ordinem (I) observare: (1), (3), (5) ... L ... (6), (4), (2); prima harum quantitatum est $= 0$ (propter $a' = 0$), reliquae omnes idem signum habent ut L sive a. Quoniam vero per hyp. $\frac{\mathfrak{A}}{\mathfrak{C}}, \frac{\mathfrak{B}}{\mathfrak{D}}$ (pro quibus scribemus $\mathfrak{M}, \mathfrak{N}$) idem signum habent: patet has quantitates ipsi (1) a dextra iacere (aut si mavis ab eadem parte a qua L), et quidem, quum L iaceat inter ipsas, alteram ipsi L a dextra, alteram a laeva. Facile vero ostendi potest, $\mathfrak{M}$ ipsi (2) a dextra iacere non posse, alioquin enim $\mathfrak{N}$ iaceret inter (1) et L, unde sequeretur *primo* (2) iacere inter $\mathfrak{M}$ et $\mathfrak{N}$, adeoque denominatorem fractionis (2) maiorem esse denominatore fractionis $\mathfrak{N}$ (art. 190), *secundo* $\mathfrak{N}$ iacere inter (1) et (2), adeoque denom. fractionis $\mathfrak{N}$ esse maiorem quam denom. fractionis (2). *Q. E. A.*

Supponamus $\mathfrak{M}$ nulli fractionum (2), (3), (4) etc. aequalem esse, ut, quid inde sequatur, videamus. Tum manifestum est, si fractio $\mathfrak{M}$ ipsi L a laeva iaceat, necessario eam sitam esse aut inter (1) et (3), aut inter (3) et (5), aut inter (5) et (7) etc. (quoniam L est irrationalis, adeoque ipsi $\mathfrak{M}$ certo inaequalis, fractionesque (1), (3), (5) etc. quavis quantitate data, ipsi L inaequali, propius ad L accedere possunt). Si vero $\mathfrak{M}$ ipsi L a dextra iacet: necessario iacebit aut inter (2) et (4), aut inter (4) et (6) aut inter (6) et (8) etc. Ponamus itaque $\mathfrak{M}$ iacere inter

(m) et $(m+2)$, patetque quantitates $\mathfrak{M}$, (m), $(m+1)$, $(m+2)$, L iacere sequenti ordine,

$$(\text{II})^*): \qquad (m),\ (\mathfrak{M}),\ (m+2),\ L,\ (m+1)$$

Tum erit necessario $\mathfrak{N} = (m+1)$. Iacebit enim $\mathfrak{N}$ ipsi L a dextra; si vero etiam ipsi $(m+1)$ a dextra iaceret, $(m+1)$ iaceret inter $\mathfrak{M}$ et $\mathfrak{N}$, unde $\gamma^{m+1} > \mathfrak{C}$, $\mathfrak{M}$ vero inter (m) et $(m+1)$ unde $\mathfrak{C} > \gamma^{m+1}$ (art. 190), *Q. E. A.*; si vero $\mathfrak{N}$ ipsi $(m+1)$ a laeva iaceret, sive inter $(m+2)$ et $(m+1)$, foret $\mathfrak{D} > \gamma^{m+2}$, et quia $(m+2)$ inter $\mathfrak{M}$ et $\mathfrak{N}$, foret $\gamma^{m+2} > \mathfrak{D}$, *Q. E. A.* Erit itaque $\mathfrak{N} = (m+1)$, sive $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{m+1}}{\gamma^{m+1}} = \frac{\beta^m}{\delta^m}$.

Quia $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, $\mathfrak{B}$ erit primus ad $\mathfrak{D}$ et ex simili ratione β^m primus ad δ^m. Unde facile perspicitur aequationem $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\beta^m}{\delta^m}$ consistere non posse, nisi fuerit aut $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$, aut $\mathfrak{B} = -\beta^m$, $\mathfrak{D} = -\delta^m$. Iam quum forma f per substitutionem propriam $\alpha^m, \beta^m, \gamma^m, \delta^m$ in formam f^m transmutetur, quae est $(\pm a^m, b^m, \mp a^{m+1})$: habebuntur aequationes

$$a\alpha^m\alpha^m + 2b\alpha^m\gamma^m - a'\gamma^m\gamma^m = \pm a^m \quad \ldots\ldots [5]$$
$$a\alpha^m\beta^m + b(\alpha^m\delta^m + \beta^m\gamma^m) - a'\gamma^m\delta^m = b^m \quad \ldots\ldots [6]$$
$$a\beta^m\beta^m + 2b\beta^m\delta^m - a'\delta^m\delta^m = \mp a^{m+1} \quad \ldots\ldots [7]$$
$$\alpha^m\delta^m - \beta^m\gamma^m = 1 \quad \ldots\ldots [8]$$

Hinc fit: (ex aequ. 7 et 3), $\mp a^{m+1} = -A'$. Porro multiplicando aequationem [2] per $\alpha^m\delta^m - \beta^m\gamma^m$, aequationem [6] per $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C}$ et subtrahendo facile per evolutionem confirmatur esse

$$B - b^m = (\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\beta^m + b(\mathfrak{D}\beta^m + \mathfrak{B}\delta^m) - a'\mathfrak{D}\delta^m) + (\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)(a\mathfrak{A}\alpha^m + b(\mathfrak{C}\alpha^m + \mathfrak{A}\gamma^m) - a'\mathfrak{C}\gamma^m) \quad [9]$$

sive quoniam vel $\beta^m = \mathfrak{B}$, $\delta^m = \mathfrak{D}$ vel $\beta^m = -\mathfrak{B}$, $\delta^m = -\mathfrak{D}$,

$$B - b^m = \pm(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D}) = \mp(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)A'$$

Hinc $B \equiv b^m \pmod{A'}$; quia vero tum B tum b^m inter $\sqrt{D}$ et $\sqrt{D \mp A'}$ iacent, necessario erit $B = b^m$ adeoque $\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m = 0$, sive $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^m}{\gamma^m}$, i. e. $\mathfrak{M} = (m)$.

Hoc modo itaque ex suppositione, $\mathfrak{M}$ nulli quantitatum (2), (3), (4) etc. aequalem esse, deduximus, eam revera alicui aequalem esse. Quodsi vero ab initio supponimus, esse $\mathfrak{M} = (m)$, manifesto erit vel $\mathfrak{A} = \alpha^m$, $\mathfrak{C} = \gamma^m$, vel $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. In utroque casu fit ex [1] et [5] $A = \pm a^m$, et ex [9] $B - b^m = \pm(\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)A$, sive $B \equiv b^m \pmod{A}$. Hinc simili modo ut supra concluditur $B = b^m$, et hinc $\mathfrak{B}\delta^m = \mathfrak{D}\beta^m$; quare quum $\mathfrak{B}$ ad $\mathfrak{D}$ primus sit et β^m ad δ^m: erit aut $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$ aut $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$, et proin ex [7] $-A' = \mp a^{m+1}$. Quamobrem formae F, f^m identicae erunt. Adiumento aequationis $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = \alpha^m\delta^m - \beta^m\gamma^m$ autem nullo negotio probatur, poni debere $+\mathfrak{B} = \beta^m$, $+\mathfrak{D} = \delta^m$, quando $+\mathfrak{A} = \alpha^m$, $+\mathfrak{C} = \gamma^m$; contra $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = -\delta^m$, quando $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. *Q. E. D.*

*) Nihil hic refert, sive ordo in (II) idem sit ut in (I), sive huic oppositus, *i. e.* sive (m) etiam in (I) ipsi L a laeva iaceat sive a dextra.

III. Si signum quantitatum $\frac{\mathfrak{A}}{\mathfrak{C}}$ etc. signo ipsius a oppositum: demonstratio praecedenti tam similis est, ut praecipua tantum momenta addigitavisse sufficiat. Iacebit $\frac{-\sqrt{D}+b}{a'}$ inter $\frac{\mathfrak{C}}{\mathfrak{A}}$ et $\frac{\mathfrak{D}}{\mathfrak{B}}$. Fractio $\frac{\mathfrak{D}}{\mathfrak{B}}$ alicui fractionum

$$\frac{\gamma}{\varepsilon}, \frac{m\gamma}{m\varepsilon}, \frac{m^2\gamma}{m^2\varepsilon} \text{ etc. aequalis erit} \quad \ldots\ldots\ldots\ldots (\text{I})$$

qua posita $= \frac{m\gamma}{m\varepsilon}$,

$$\frac{\mathfrak{C}}{\mathfrak{A}} \text{ erit} = \frac{m\gamma}{m\alpha} \quad \ldots\ldots\ldots\ldots\ldots\ldots (\text{II})$$

Demonstratur autem (I) ita: Si $\frac{\mathfrak{D}}{\mathfrak{B}}$ nulli illarum fractionum aequalis esse supponitur: inter duas tales $\frac{m\gamma}{m\varepsilon}$ et $\frac{m+n\gamma}{m+n\varepsilon}$ iacere debebit. Hinc vero eodem modo ut supra deducitur, necessario esse

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{m+\gamma}{m+\varepsilon} = \frac{m\gamma}{m\varepsilon}$$

atque vel $\mathfrak{A} = {}^m\alpha$, $\mathfrak{C} = {}^m\gamma$, vel $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{C} = {}^m\gamma$. Quoniam vero f per substitutionem propriam ${}^m\alpha$, ${}^m\beta$, ${}^m\gamma$, ${}^m\delta$ in formam

$${}^mf = (\pm {}^ma, {}^mb, \mp {}^{m-1}a)$$

transit: hinc emergunt tres aequationes, ex quibus coniunctis cum aequ. 1, 2, 3, 4 atque hac, ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$ deducitur eodem modo ut supra, terminum primum A formae F termino primo formae ${}^mf$ aequalem esse, illiusque terminum medium medio huius congruum secundum modulum A, unde sequitur, quia utraque forma est reducta, adeoque utriusque terminus medius inter $\sqrt{D}$ et $\sqrt{D \mp A}$ situs, hos terminos medios aequales esse: hinc vero deducitur $\frac{m\gamma}{m\varepsilon} = \frac{\mathfrak{D}}{\mathfrak{B}}$. Veritas itaque assertionis (I) derivata hic est ex suppositione illam esse falsam.

Supponendo autem $\frac{m\gamma}{m\varepsilon} = \frac{\mathfrak{D}}{\mathfrak{B}}$, prorsus simili modo et per easdem aequatio-

nes demonstratur, esse etiam $\frac{{}^m\gamma}{{}^m\delta} = \frac{\mathfrak{C}}{\mathfrak{A}}$, quod erat secundum (II). Hinc vero adiumento aequationum $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, ${}^m\alpha\,{}^m\delta - {}^m\beta\,{}^m\gamma = 1$ deducitur esse vel

$$\mathfrak{A} = {}^m\alpha, \quad \mathfrak{B} = {}^m\beta, \quad \mathfrak{C} = {}^m\gamma, \quad \mathfrak{D} = {}^m\delta$$

vel

$$-\mathfrak{A} = {}^m\alpha, \quad -\mathfrak{B} = {}^m\beta, \quad -\mathfrak{C} = {}^m\gamma, \quad -\mathfrak{D} = {}^m\delta$$

formasque F, ${}^mf$ identicas. *Q. E. D.*

194.

Quum formae quas supra socias vocavimus (art. 187, 6) semper sint improprie aequivalentes (art. 159): perspicuum est, si formae reductae F, f improprie aequivalentes sint, formaeque F socia forma G, formas f, G proprie aequivalentes fore adeoque formam G in periodo formae f contentam. Quodsi itaque formae F, f tum proprie tum improprie aequivalentes sunt, patet, tum F tum G in periodo formae f reperiri debere. Quare periodus haec sibi ipsi socia erit, duasque formas ancipites continebit (art. 187, 7). Vnde theorema art. 165 egregie confirmatur, ex quo iam poteramus esse certi, formam aliquam ancipitem dari formis F, f aequivalentem.

195.

Problema. *Propositis duabus formis quibuscunque Φ, φ eiusdem determinantis: diiudicare utrum aequivalentes sint, annon.*

Sol. Quaerantur duae formae reductae F, f propositis Φ, φ resp. proprie aequivalentes (art. 183). Quae prout aut proprie tantum aequivalent, aut improprie tantum, aut utroque modo, aut neutro; etiam propositae aut proprie tantum aequivalentes erunt, aut improprie tantum, aut utroque aut neutro modo. Evolvatur periodus alterutrius formae reductae *e. g.* periodus formae f. Si forma F in hac periodo occurrit neque vero simul forma ipsi F socia, manifesto casus *primus* locum habebit; contra si socia haec adest neque vero F ipsa, *secundus*; si utraque, *tertius*; si neutra, *quartus*.

Ex. Propositae sint formae (129, 92, 65), (42, 59, 81) determinantis 79. His proprie aequivalentes inveniuntur reductae (10, 7, —3), (5, 8, —3). Periodus formae prioris haec est: (10, 7, —3), (—3, 8, 5), (5, 7, —6), (—6, 5, 9), (9, 4, —7), (—7, 3, 10). In qua quum forma (5, 8, —3) ipsa non reperiatur,

sed tamen socia (—3, 8, 5): formas propositas improprie tantum aequivalere concludimus.

Si omnes formae reductae determinantis dati eodem modo ut supra (art. 187, 5) in periodos P, Q, R etc. distribuuntur, atque e quavis periodo forma aliqua ad libitum eligitur, ex P, F; ex Q, G; ex R, H etc.: inter has formas F, G, H etc. duae quae proprie aequivalent esse non poterunt. Quaevis autem alia forma eiusdem determinantis alicui ex istis proprie aequivalens erit et quidem *unicae* tantum. Hinc manifestum est, *omnes formas huius determinantis in totidem classes distribui posse, quot habeantur periodi*, scilicet referendo eas quae formae F proprie aequivalent in primam classem, eas quae formae G proprie aequivalent in secundam etc. Hoc modo omnes formae in eadem classe contentae proprie aequivalentes erunt, formae vero e classibus diversis non poterunt proprie aequivalere. Sed hic huic argumento infra fusius explicando non immoramur.

196.

Problema. *Propositis duabus formis proprie aequivalentibus Φ, φ: invenire transformationem propriam alterius in alteram.*

Sol. Per methodum art. 183 inveniri poterunt duae series formarum

$$\Phi, \Phi', \Phi'' \ldots \Phi^n \quad \text{et} \quad \varphi, \varphi', \varphi'' \ldots \varphi^\nu$$

tales ut quaevis forma sequens praecedenti proprie aequivaleat, ultimaeque Φ^n, φ^ν sint formae reductae; et quum Φ, φ proprie aequivalentes esse supponantur, necessario Φ^n in periodo formae φ^ν contenta erit. Sit $\varphi^\nu = f$ ipsiusque periodus usque ad formam Φ^n haec

$$f, f', f'' \ldots f^{m-1}, \Phi^n$$

ita ut in hac periodo index formae Φ^n sit m; designenturque formae quae oppositae sunt sociis formarum

$$\Phi, \Phi', \Phi'' \ldots \Phi^n \quad \text{per} \quad \Psi, \Psi', \Psi'' \ldots \Psi^m \quad \text{resp.}\ *).$$

Tum in progressione

*) Ita ut Ψ oriatur ex Φ commutando terminum primum et ultimum tribuendoque medio signum oppositum, similiterque de reliquis.

$$\varphi, \varphi', \varphi'' \ldots f, f', f'' \ldots f^{m-1}, \Psi^{n-1}, \Psi^{n-2} \ldots \Psi, \Phi$$

quaevis forma praecedenti ab ultima parte contigua erit, unde per art. 177 inveniri poterit transformatio propria primae φ in ultimam Φ. Illud autem de formis reliquis progressionis nullo negotio perspicitur; de his f^{m-1}, Ψ^{n-1} sic probatur: Sit

$$f^{m-1} = (g, h, i); \quad f^m \text{ sive } \Phi^n = (g', h', i'); \quad \Phi^{n-1} = (g'', h'', i'')$$

Forma (g', h', i') tum formae (g, h, i) tum formae (g'', h'', i'') ab ultima parte contigua erit; hinc $i = g' = i''$, et $-h \equiv h' \equiv -h''$ (mod. i vel g' vel i''). Unde manifestum est, formam $(i'', -h'', g'')$, *i. e.* formam Ψ^{n-1} formae (g, h, i), *i. e.* formae f^{m-1} ab ultima parte contiguam esse.

Si formae Φ, φ improprie aequivalentes sunt: forma φ proprie aequivalebit formae cui opposita est Φ. Inveniri poterit itaque transformatio propria formae φ in formam cui Φ est opposita; quae si supponitur fieri per substitutionem $\alpha, \delta, \gamma, \delta$, facile perspicitur, φ improprie transformari in ipsam Φ per substitutionem $\alpha, -\delta, \gamma, -\delta$.

Hinc etiam perspicuum est, si formae Φ, φ tum proprie tum improprie aequivalentes sint, inveniri posse *duas* transformationes, propriam et impropriam.

Ex. Quaeritur transformatio impropria formae (129, 92, 65) in formam (42, 59, 81), quam illi improprie aequivalere in art. praec. invenimus. Investiganda erit itaque primo transformatio propria formae (129, 92, 65) in formam (42, −59, 81). Ad hunc finem evolvitur progressio formarum haec: (129, 92, 65), (65, −27, 10), (10, 7, −3), (−3, 8, 5), (5, 22, 81), (81, 59, 42), (42, −59, 81). Hinc deducitur transformatio propria −47, 56, 73, −87, per quam (129, 92, 65) transit in (42, −59, 81); quare per impropriam −47, −56, 73, 87 transibit in (42, 59, 81).

197.

Si transformatio una formae alicuius $(a, b, c) \ldots \varphi$ in aequivalentem Φ habetur: ex hac *omnes* transformationes similes formae φ in Φ deduci poterunt, si modo omnes solutiones aequationis indeterminatae $tt - Duu = mm$ assignari

possunt, designante D determinantem formarum Φ, φ; m divisorem communem maximum numerorum $a, 2b, c$ (art. 162). Hoc igitur problema, quod pro valore negativo ipsius D iam supra solvimus, nunc pro positivo aggrediemur. Quia vero manifesto quivis valor ipsius t aequationi satisfaciens etiamnum mutato signo satisfacit, similiterque quivis valor ipsius u: sufficiet si omnes valores *positivos* ipsorum t, u assignare possimus, fungeturque quaelibet solutio per valores positivos, quatuor solutionum vice. Hoc negotium ita absolvemus, ut *primo* valores *minimos* ipsorum t, u (praeter hos per se obvios $t = m$, $u = 0$) invenire, *tum* ex his omnes reliquos derivare doceamus.

198.

Problema. *Invenire numeros minimos t, u aequationi indeterminatae $tt - Duu = mm$ satisfacientes, siquidem forma aliqua (M, N, P) datur, cuius determinans est D, numerorumque $M, 2N, P$ divisor communis maximus m.*

Sol. Accipiatur ad lubitum forma reducta $(a, b, -a') \ldots f$, determinantis D, ubi divisor communis maximus numerorum $a, 2b, a'$ sit m, qualem dari vel inde manifestum est, quod forma reducta formae (M, N, P) aequivalens inveniri potest, quae per art. 161 hac proprietate erit praedita: sed ad propositum praesens quaevis forma reducta in qua conditio haec locum habet poterit adhiberi. Evolvatur periodus formae f, quam ex n formis constare supponemus. Retentis omnibus signis quibus in art. 188 usi sumus, f^n erit $(+a^n, b^n, -a^{n+1})$, quia n par, et in hanc formam transibit f per substitutionem propriam $\alpha^n, \delta^n, \gamma^n, \delta^n$. Quia vero f et f^n sunt identicae: f transibit in f^n etiam per substitutionem propriam 1, 0, 0, 1. Ex his duabus transformationibus similibus formae f in f^n per art. 162 deduci poterit solutio aequationis $tt - Duu = mm$ *in integris*, scilicet $t = \frac{1}{2}(\alpha^n + \delta^n)m$ (aequ. 18 art. 162), $u = \frac{\gamma^n m}{a}$ (aequ. 19)*). Designentur hi valores positive accepti si forte nondum sunt per T, U, eruntque hi T, U valores minimi ipsorum t, u, praeter hos $t = m$, $u = 0$ (a quibus necessario erunt diversi, quia manifesto γ^n non poterit esse $= 0$).

Supponamus enim dari adhuc minores valores ipsorum t, u puta t, u qui sint positivi et u non $= 0$. Tum per art. 162 forma f per substitutionem propriam $\frac{1}{m}(t - bu)$, $\frac{1}{m}a'u$, $\frac{1}{m}au$, $\frac{1}{m}(t + bu)$ transformabitur in formam cum ipsa

*) Quae in art. 162 erant $\alpha, \delta, \gamma, \delta$; $\alpha', \delta', \gamma', \delta'$; A, B, C; a, b, c; e,
hic sunt $1, 0, 0, 1$; $\alpha^n, \delta^n, \gamma^n, \delta^n$; $a, b, -a'$; $a, b, -a'$; 1.

identicam. Iam ex art. 193, II sequitur, *aut* $\frac{1}{m}(t-bu)$ *aut* $-\frac{1}{m}(t-bu)$ alicui numerorum α'', α''', α'''' etc. aequalem esse debere, puta $=\alpha^{\mu}$ (quia enim $tt=Duu+mm=bbuu+aa'uu+mm$, erit $tt>bbuu$, adeoque $t-bu$ positivus; hinc fractio $\frac{t-bu}{au}$, quae respondet fractioni $\frac{\mathfrak{A}}{\mathfrak{C}}$ in art. 193, idem signum habebit ut a vel a'); atque in casu priori $\frac{1}{m}a'u$, $\frac{1}{m}au$, $\frac{1}{m}(t+bu)$, in posteriori easdem quantitates mutatis signis, resp. $=\delta^{\mu}$, γ^{μ}, δ^{μ}. Sed quum sit $u<U$ *i. e.* $u<\frac{\gamma^n m}{a}$ et >0: erit $\gamma^{\mu}<\gamma^n$ et >0; quocirca quum progressio γ, γ', γ'' etc. continuo crescat, necessario μ iacebit inter 0 et n excl. Forma vero respondens, f^{μ}, identica erit cum forma f, *Q. E. A.*, quum omnes formae f, f'', f''' etc. usque ad f^{n-1} diversae esse supponantur. Ex his colligitur, minimos valores ipsorum t, u (exceptis valoribus m, 0) esse T, U.

Ex. Si $D=79$, $m=1$: adhiberi poterit forma $(3, 8, -5)$, pro qua $n=6$, atque $\alpha^n=-8$, $\gamma^n=-27$, $\delta^n=-152$ (art. 188). Hinc $T=80$, $U=9$, qui sunt valores minimi numerorum t, u, aequationi $tt-79uu=1$ satisfacientes.

199.

Ad praxin formulae adhuc commodiores erui possunt. Erit nimirum $2b\gamma^n=-a(\alpha^n-\delta^n)$, quod facile ex art. 162 deducitur, multiplicando aequ. [19] per $2b$, [20] per a et mutando characteres illic adhibitos in praesentes. Hinc fit $\alpha^n+\delta^n=2\delta^n-\frac{2b}{a}\gamma^n$, adeoque

$$\pm T=m(\delta^n-\frac{b}{a}\gamma^n),\quad \pm U=\frac{\gamma^n m}{a}$$

Per similem methodum hos valores obtinemus

$$\pm T=m(\alpha^n+\frac{b}{a'}\delta^n),\quad \pm U=\frac{\delta^n m}{a'}$$

Tum hae tum illae formulae perquam commodae evadunt, propter $\gamma^n=\delta^{n-1}$, $\alpha^n=\delta^{n-1}$, ita ut si his uteris, solam progressionem δ', δ'', $\delta'''\ldots\delta^n$; si illis uti mavis, solam hanc δ', δ'', δ''' etc. supputavisse sufficiat. Praeterea ex art. 189, 3 facile deducitur, quum n necessario sit par, α^n et $\frac{b}{a'}\delta^n$ eadem signa habere; neque minus δ^n et $\frac{b}{a}\gamma^n$, ita ut in formula priori pro T differentia absoluta, in posteriori summa absoluta accipi debeat, neque adeo ad signa respicere omnino opus sit. Receptis signis in art. 189, 4 adhibitis erit ex formula priori

$$T=m[k', k'', k'''\ldots k^n]-\frac{mb}{a}[k, k', k''\ldots k^{n-1}],\quad U=\frac{m}{a}[k, k', k'''\ldots k^{n-1}]$$

ex posteriori

$$T=m[k'', k'''\ldots k^{n-1}]+\frac{mb}{a'}[k'', k'''\ldots k^n],\quad U=\frac{m}{a'}[k'', k'''\ldots k^n]$$

ubi pro valore ipsius T etiam $m[k'', k'''\ldots k^n, \frac{b}{a'}]$ scribi poterit.

Ex. Pro $D=61$, $m=2$ adhiberi potest forma $(2, 7, -6)$, pro qua eruitur $n=6$; k', k'', k''', k'''', k''''', k'''''' resp. $=2, 2, 7, 2, 2, 7$. Hinc fit

$$T=2[2, 2, 7, 2, 2, 7]-7[2, 2, 7, 2, 2]=2888-1365=1523$$

ex formula prima; idem provenit ex secunda

$$T=2[2, 7, 2, 2]+\tfrac{1}{3}[2, 7, 2, 2, 7]$$

U vero fit $=[2, 2, 7, 2, 2]=\frac{1}{3}[2, 7, 2, 2, 7]=195$.

Ceterum plura artificia adhuc dantur, per quae calculus contrahi potest, sed de his fusius hic loqui brevitas non permittit.

200.

Ut ex valoribus minimis ipsorum t, u *omnes* obtineamus, aequationem $TT-DUU=mm$ ita exhibemus

$$(\tfrac{T}{m}+\tfrac{U}{m}\sqrt{D})(\tfrac{T}{m}-\tfrac{U}{m}\sqrt{D})=1$$

unde etiam erit

$$(\tfrac{T}{m}+\tfrac{U}{m}\sqrt{D})^e(\tfrac{T}{m}-\tfrac{U}{m}\sqrt{D})^e=1\quad\ldots\ldots\quad[1]$$

denotante e numerum quemcunque. Iam designabimus brevitatis caussa valores quantitatum

$$\tfrac{m}{2}(\tfrac{T}{m}+\tfrac{U}{m}\sqrt{D})^e+\tfrac{m}{2}(\tfrac{T}{m}-\tfrac{U}{m}\sqrt{D})^e,\quad \tfrac{m}{2\sqrt{D}}(\tfrac{T}{m}+\tfrac{U}{m}\sqrt{D})^e-\tfrac{m}{2\sqrt{D}}(\tfrac{T}{m}-\tfrac{U}{m}\sqrt{D})^e\ *)$$

generaliter per t^e, u^e resp. *i. e.* illarum valores pro $e=0$, per t^0, u^0 (qui erunt m, 0); pro $e=1$ per t', u' (qui fiunt T, U); pro $e=2$ per t'', u''; pro $t=3$ per t''', u''' etc. — demonstrabimusque, si pro e accipiantur omnes numeri integri non negativi *i. e.* 0, omnesque positivi ab 1 usque ad ∞, expressiones illas exhibere omnes valores positivos ipsorum t, u: scilicet I) omnes valores illarum expressio-

*) In his solis quatuor expressionibus et in aequ. [1] e denotat *exponentem* potestatis; in reliquis literae apici adscriptae semper *indicem* designant.

num esse revera valores ipsorum t, u; II) omnes valores illos esse numeros integros; III) nullos valores positivos ipsorum t, u dari qui sub formulis illis non contineantur.

I. Substitutis pro t^e, u^e valoribus suis nullo negotio adiumento aequ. [1] confirmatur, esse

$$(t^e + u^e\sqrt{D})(t^e - u^e\sqrt{D}) = mm, \quad i.e. \quad t^e t^e - Du^e u^e = mm$$

II. Eodem modo facile confirmatur, esse generaliter

$$t^{e+1} + t^{e-1} = \tfrac{2T}{m} t^e, \quad u^{e+1} + u^{e-1} = \tfrac{2T}{m} u^e$$

Hinc manifestum est, duas progressiones t^0, t', t'', t''' etc., u^0, u', u'', u''' etc. esse recurrentes, et utriusque scalam relationis $\frac{2T}{m}, -1$, scilicet

$$t'' = \tfrac{2T}{m} t' - t^0, \quad t''' = \tfrac{2T}{m} t'' - t' \text{ etc.}, \quad u'' = \tfrac{2T}{m} u' \text{ etc.}$$

Iam quoniam per hyp. forma aliqua datur, (M, N, P), determinantis D, in qua $M, 2N, P$ per m sunt divisibiles: habebitur

$$TT = (NN - MP)UU + mm$$

eritque adeo manifesto $4TT$ per mm divisibilis. Hinc $\frac{2T}{m}$ erit numerus integer et quidem positivus. Quia vero $t^0 = m$, $t' = T$, $u^0 = 0$, $u' = U$, adeoque integri: omnes t'', t''' etc. u'', u''' etc. etiam integri erunt. Porro perspicuum est, quia $TT > mm$, omnes t^0, t', t'', t''' etc. positivos et continuo in infinitum crescentes esse, nec non omnes u^0, u', u'', u''' etc.

III. Supponamus, dari adhuc alios valores positivos ipsorum t, u qui in progressione t^0, t', t'' etc. u^0, u', u'' etc. non contenti sint, puta $\mathfrak{T}, \mathfrak{U}$. Manifestum est, quum progressio u^0, u' etc. a 0 in infinitum crescat, $\mathfrak{U}$ necessario inter duos terminos proximos, u^n et u^{n+1} situm fore, ita ut sit $\mathfrak{U} > u^n$ et $\mathfrak{U} < u^{n+1}$. Ut absurditatem huius suppositionis demonstremus, observamus

1° Aequationi $tt - Duu = mm$ satisfactum iri etiam ponendo

$$t = \tfrac{1}{m}(\mathfrak{T} t^n - D\mathfrak{U} u^n), \quad u = \tfrac{1}{m}(\mathfrak{U} t^n - \mathfrak{T} u^n)$$

Hoc quidem nullo negotio per substitutionem confirmatur: quod vero hi valores quos ponemus brevitatis gratia $= \tau, \upsilon$, semper sunt numeri *integri*, ita ostendimus. Si (M, N, P) est forma determinantis D, atque m divisor communis numerorum $M, 2N, P$: erit tum $\mathfrak{T} + N\mathfrak{U}$ tum $t^n + Nu^n$ per m divisibilis adeoque etiam $\mathfrak{U}(t^n + Nu^n) - u^n(\mathfrak{T} + N\mathfrak{U})$ sive $\mathfrak{U} t^n - \mathfrak{T} u^n$. Quare υ erit integer et proin etiam τ, quia $\tau\tau = D\upsilon\upsilon + mm$.

2° Patet υ non posse esse $= 0$; hinc enim sequeretur

$$\mathfrak{U}\mathfrak{U} t^n t^n = \mathfrak{T}\mathfrak{T} u^n u^n$$

sive

$$\mathfrak{U}\mathfrak{U}(Du^n u^n + mm) = u^n u^n (D\mathfrak{U}\mathfrak{U} + mm)$$

sive $\mathfrak{U}\mathfrak{U} = u^n u^n$, contra hyp. ex qua $\mathfrak{U} > u^n$. Quum igitur praeter valorem 0, minimus valor ipsius u sit U, erit υ certe non minor quam U.

3° Facile ex valoribus ipsorum $t^n, t^{n+1}, u^n, u^{n+1}$ confirmari potest, esse

$$mU = u^{n+1} t^n - t^{n+1} u^n.$$

Quare $\mathfrak{U} t^n - \mathfrak{T} u^n$ certe non erit minor quam $u^{n+1} t^n - t^{n+1} u^n$.

4° Iam ex aequatione $\mathfrak{T}\mathfrak{T} - D\mathfrak{U}\mathfrak{U} = mm$ habetur

$$\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{(D + \frac{mm}{\mathfrak{U}\mathfrak{U}})}$$

et similiter

$$\frac{t^{n+1}}{u^{n+1}} = \sqrt{(D + \frac{mm}{u^{n+1} u^{n+1}})}$$

unde facile deducitur esse $\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t^{n+1}}{u^{n+1}}$. Hinc vero et ex conclusione in 3° sequitur

$$(\mathfrak{U} t^n - \mathfrak{T} u^n)(t^n + u^n \tfrac{\mathfrak{T}}{\mathfrak{U}}) > (u^{n+1} t^n - t^{n+1} u^n)(t^n + u^n \tfrac{t^{n+1}}{u^{n+1}})$$

sive, evolutione facta, et loco ipsorum $\mathfrak{T}\mathfrak{T}$, $t^n t^n$, $t^{n+1} t^{n+1}$ substitutis valoribus suis $D\mathfrak{U}\mathfrak{U} + mm$, $Du^n u^n + mm$, $Du^{n+1} u^{n+1} + mm$,

$$\tfrac{1}{\mathfrak{U}}(\mathfrak{U}\mathfrak{U} - u^n u^n) > \tfrac{1}{u^{n+1}}(u^{n+1} u^{n+1} - u^n u^n)$$

unde, quoniam utraque quantitas manifesto positiva, fit transponendo $\mathfrak{U} + \frac{u^n u^n}{u^{n+1}} > u^{n+1} + \frac{u^n u^n}{\mathfrak{U}}$, *Q. E. A.*, quia quantitatis prioris pars prima *minor* est

quam pars prima quantitatis secundae, nec non illius secunda minor quam secunda huius. Quamobrem suppositio consistere nequit et progressiones t^0, t', t'' etc. u^0, u', u'' etc. omnes valores positivos ipsorum t, u exhibebunt.

Ex. Pro $D=61$, $m=2$ valores minimos positivos ipsorum t, u invenimus 1523, 195: quare *omnes* valores positivi exhibebuntur per has formulas

$$t = (\tfrac{1523}{2} + \tfrac{195}{2}\sqrt{61})^e + (\tfrac{1523}{2} - \tfrac{195}{2}\sqrt{61})^e$$

$$u = \tfrac{1}{\sqrt{61}}((\tfrac{1523}{2} + \tfrac{195}{2}\sqrt{61})^e - (\tfrac{1523}{2} - \tfrac{195}{2}\sqrt{61})^e)$$

Invenitur autem

$t^0=2$, $t'=1523$, $t''=1523\,t'-t^0=2319527$, $t'''=1523\,t''-t'=3532618098$ etc.
$u^0=0$, $u'=195$, $u''=1523\,u'-u^0=296985$, $u'''=1523\,u''-u'=452307960$ etc.

201.

Circa problema in artt. praecc. tractatum sequentes observationes adhuc adiicimus.

1) Quum aequationem $tt-Duu=mm$ pro omnibus casibus solvere docuerimus, ubi m est divisor communis maximus trium numerorum $M, 2N, P$, talium ut $NN-MP=D$: operae pretium est omnes numeros qui tales divisores esse possunt sive omnes valores ipsius m pro valore dato ipsius D assignare. Ponatur $D=nnD'$, ita ut D' a factoribus quadraticis omnino sit liber, quod obtinetur si pro nn assumitur maximum quadratum ipsum D metiens: sin vero D iam per se nullum factorem quadraticum implicaret, fieri deberet $n=1$. Tum dico

Primo, si D' fuerit formae $4k+1$, quemvis divisorem ipsius $2n$ fore valorem ipsius m, et vice versa. Si enim g est divisor ipsius $2n$, habebitur forma $(g, n, \frac{nn(1-D')}{g})$, cuius determinans est D, et in qua manifesto divisor communis maximus numerorum $g, 2n, \frac{nn(D'-1)}{g}$ erit g (patet enim $\frac{nn(D'-1)}{gg} = \frac{4nn}{gg}\cdot\frac{D'-1}{4}$ esse numerum integrum). Si vero, vice versa, g supponitur esse valor ipsius m, scilicet divisor communis maximus numerorum $M, 2N, P$, atque $NN-MP=D$: manifesto $4D$ sive $4nnD'$ divisibilis erit per gg. Hinc vero sequitur, $2n$ necessario per g divisibilem esse. Si enim g ipsum $2n$ non metiretur, g et $2n$ haberent divisorem communem maximum minorem quam g, quo posito $=\delta$, atque $2n=\mathfrak{C}n'$, $g=\mathfrak{C}g'$, foret $n'n'D'$ per $g'g'$ divisibilis, n' ad g' adeoque etiam $n'n'$ ad $g'g'$ primus et proin etiam D' per $g'g'$ divisibilis, contra hyp. secundum quam D' ab omni factore quadratico est liberatus.

Secundo, si D' fuerit formae $4k+2$ vel $4k+3$, quemvis divisorem ipsius n fore valorem ipsius m, et vice versa quemvis valorem ipsius m metiri ipsum n. Si enim g est divisor ipsius n, habebitur forma $(g, 0, -\frac{nnD'}{g})$, cuius determinans $=D$, et ubi manifesto numerorum $g, 0, \frac{nnD'}{g}$ divisor communis maximus erit g. — Si vero g supponitur esse valor ipsius m, puta divisor communis maximus numerorum $M, 2N, P$, atque $NN-MP=D$: eodem modo ut supra g metietur ipsum $2n$, sive $\frac{2n}{g}$ erit integer. Si quotiens hic esset impar: quadratum $\frac{4nn}{gg}$ foret $\equiv 1 \pmod 4$, adeoque $\frac{4nnD'}{gg}$ aut $\equiv 2$ aut $\equiv 3 \pmod 4$. At $\frac{4nnD'}{gg} = \frac{4D}{gg} = \frac{4NN}{gg} - \frac{4MP}{gg} \equiv \frac{4NN}{gg} \pmod 4$, et proin $\frac{4NN}{gg}$ aut $\equiv 2$ aut $\equiv 3 \pmod 4$, *Q. E. A.*, quia omne quadratum aut cifrae aut unitati secundum modulum 4 congruum esse debet. Quare quotiens $\frac{2n}{g}$ necessario erit par, adeoque $\frac{n}{g}$ integer, sive g divisor ipsius n.

Patet itaque, 1 semper esse valorem ipsius m, sive aequationem $tt-Duu=1$ pro quovis valore positivo non quadrato ipsius D per praecedentia resolubilem esse; 2 tunc tantummodo esse valorem ipsius m, si D fuerit aut formae $4k$, aut formae $4k+1$.

2) Si m est maior quam 2, attamen numerus idoneus, solutio aequationis $tt-Duu=mm$ reduci potest ad solutionem similis aequationis, ubi m est aut 1 aut 2. Scilicet posito ut ante $D=nnD'$, si m ipsum n metitur, metietur mm ipsum D. Tum si valores minimi ipsorum p, q in aequatione $pp-\frac{D}{mm}qq=1$ supponuntur esse $p=P$, $q=Q$, valores minimi ipsorum t, u in aequatione $tt-Duu=mm$ erunt $t=mP$, $u=Q$. — Si vero m ipsum n non metitur, metietur saltem ipsum $2n$ eritque certo par; $\frac{4D}{mm}$ autem integer. Et si tunc valores minimi ipsorum p, q in aequatione $pp-\frac{4D}{mm}qq=4$ inventi sunt $p=P$, $q=Q$: valores minimi ipsorum t, u in aequatione $tt-Duu=mm$ erunt $t=\frac{m}{\sqrt{2}}P$, $u=Q$. — In utroque autem casu non solum ex valoribus minimis ipsorum p, q valores minimi ipsorum t, u, sed ex *omnibus* valoribus illorum *omnes* valores horum per hanc methodum manifesto deduci poterunt.

3) Designantibus t^0, u^0; t', u'; t'', u'' etc. omnes valores positivos ipsorum

t, u in aequatione $tt - Duu = mm$ (ut in art. praec.), si contingit ut valores quidam ex serie illa, valoribus primis in eadem secundum modulum quemcunque datum r, congrui sint, puta $t^\rho \equiv t$ (sive $\equiv m$), $u^\rho \equiv u^0$ sive $\equiv 0 \pmod r$); simulque valores proxime sequentes valoribus secundis, puta

$$t^{\rho+1} \equiv t', \quad u^{\rho+1} \equiv u' \pmod r$$

erit etiam

$$t^{\rho+2} \equiv t'', \; u^{\rho+2} \equiv u''; \quad t^{\rho+3} \equiv t''', \; u^{\rho+3} \equiv u''' \text{ etc.}$$

Hoc facile inde deducitur, quod utraque series t^0, t', t'' etc., u^0, u', u'' etc. est ex recurrentium genere, scilicet quoniam

$$t'' = \frac{2T}{m} t' - t^0, \quad t^{\rho+2} = \frac{2T}{m} t^{\rho+1} - t^\rho$$

erit

$$t''' \equiv t^{\rho+2}$$

similiterque de reliquis. — Hinc autem sequitur, fore generaliter

$$t^{h+\rho} \equiv t^h, \quad u^{h+\rho} \equiv u^h \pmod r$$

denotante h numerum quemcunque, nec non adhuc generalius, si fuerit

$$\mu \equiv \nu \pmod \rho, \text{ fore } t^\mu \equiv t^\nu, \quad u^\mu \equiv u^\nu \pmod r.$$

4) Conditionibus autem in observ. praec. requisitis semper satisfieri potest, scilicet semper inveniri potest index ρ (pro modulo quocunque dato r), pro quo sit

$$t^\rho \equiv t^0, \; t^{\rho+1} \equiv t', \quad u^\rho \equiv u^0, \; u^{\rho+1} \equiv u'$$

Ad quod demonstrandum observamus

primo, conditioni tertiae semper satisfieri posse. Nullo enim negotio per criteria in (1) tradita perspicietur, etiam aequationem $pp - rrDqq = mm$ solubilem fore; et si valores minimi positivi ipsorum p, q (praeter hos m, o) supponuntur esse P, Q: inter valores ipsorum t, u manifesto erunt etiam $t = P$, $u = rQ$. Quare P, rQ in progressionibus t^0, t' etc., u^0, u' etc. contenti erunt, et si $P = t^\lambda$, $rQ = u^\lambda$, erit $u^\lambda \equiv 0 \equiv u^0 \pmod r$. Praeterea facile perspicietur, inter u^0 et u^λ nullum terminum fore ipsi u^0 secundum modulum r congruum.

Secundo patet, si hic insuper tres reliquae conditiones adimpletae sint, puta si etiam $u^{\lambda+1} \equiv u'$, $t^\lambda \equiv t^0$, $t^{\lambda+1} \equiv t'$, poni tantummodo debere $\rho = \lambda$. Si

vero una aut altera illarum conditionum locum non habet, dico certe statui posse $\rho = 2\lambda$. Nam ex aequat. [1] formulisque generalibus pro t^e, u^e in art. praec. deducitur

$$t^{2\lambda} = \tfrac{1}{m}(t^\lambda t^\lambda + Du^\lambda u^\lambda) = \tfrac{1}{m}(mm + 2Du^\lambda u^\lambda)$$

adeoque

$$\frac{t^{2\lambda} - t^0}{r} = \frac{2Du^\lambda u^\lambda}{mr}$$

quae quantitas erit numerus integer, quia per hyp. r ipsum u^λ metitur, nec non mm ipsum $4D$, adeoque a potiori m ipsum $2D$. — Porro erit $u^{2\lambda} = \frac{2}{m} t^\lambda u^\lambda$, et quoniam

$$4t^\lambda t^\lambda = 4Du^\lambda u^\lambda + 4mm$$

adeoque per mm divisibilis, $2t^\lambda$ erit divisibilis per m, et proin $u^{2\lambda}$ per r, sive

$$u^{2\lambda} \equiv u^0 \pmod r$$

Tertio invenitur

$$t^{2\lambda+1} = t' + \frac{2Du^\lambda u^{\lambda+1}}{m}$$

et quoniam ex simili ratione $\frac{2Du^\lambda}{mr}$ est integer, erit

$$t^{2\lambda+1} \equiv t' \pmod r$$

Tandem reperitur

$$u^{2\lambda+1} = u' + \frac{2t^{\lambda+1}u^\lambda}{m}$$

et quoniam $2t^{\lambda+1}$ per m divisibilis est, u^λ per r; erit

$$u^{2\lambda+1} \equiv u' \pmod r. \quad Q.\ E.\ D.$$

Ceterum usus posteriorum duarum observationum in sequentibus apparebit.

202.

Casus particularis problematis, nempe solvere aequationem $tt - Duu = 1$, iam a geometris seculi praecedentis fuit agitatus. Sagacissimus Fermatius problema hoc analystis Anglis proposuit, Wallisiusque Brounkerum tamquam inventorem solutionis, quam in *Alg. Cap.* 98, *Opp. T.* II *p.* 418 sqq. tradit, nominat; Ozanam Fermatium; denique ill. Euler, qui de illo egit in *Comm. Petr.* VI *p.* 175, *Comm. nov.* XI *p.* 28 *), *Algebra P.* II *p.* 226, *Opusc. An.* I *p.* 310, Pellium, unde

*) In hac comm. algorithmus quem art. 27 exposuimus, per similia signa exhibetur, quod nos illic annotare negleximus.

problema illud a quibusdam auctoribus *Pellianum* vocatum est. Omnes hae solutiones, si essentiam spectas, conveniunt cum ea quam obtinemus, si in art. 198 formam reductam eam adoptamus in qua $a = 1$; attamen operationem quam praescribunt tandem necessario *finiri*, sive problema semper *revera solubile* esse, nemo ante ill. La Grange rigorose *) demonstravit. *Mélanges de la Soc. de Turin T.* IV *p.* 19, et concinnius *Hist. de l'Ac. de Berlin*, 1767, *p.* 237. Exstat haec disquisitio etiam in *supplementis ad Euleri Algebram* iam saepius laudatis. Ceterum methodus nostra (ex principiis omnino diversis petita, neque ad casum $m = 1$ restricta) plerumque plures vias ad solutionem perveniendi suppeditat, quoniam in art. 198 a quavis alia forma reducta $(a, b, -a')$ proficisci possumus.

203.

Problema. *Si formae* Φ, φ *sunt aequivalentes, omnes transformationes alterius in alteram exhibere.*

Sol. Quando formae hac unico tantum modo aequivalentes sunt (*i. e.* aut proprie tantum aut improprie tantum) quaeratur per art. 196 transformatio una formae φ in Φ, quae sit $\alpha, \vec{o}, \gamma, \hat{o}$, patetque alias quam quae huic sint similes, dari non posse. Quando vero φ, Φ tum proprie tum improprie aequivalent, quaerantur duae transformationes dissimiles, *i. e.* altera propria altera impropria, puta $\alpha, \vec{o}, \gamma, \hat{o}$ et $\alpha', \vec{o}', \gamma', \hat{o}'$, eritque quaevis alia transformatio aut huic aut illi similis. Si itaque forma φ est (a, b, c), ipsius determinans $= D$, divisor communis maximus numerorum $a, 2b, c$ (uti semper in praec.) m, atque t, u indefinite omnes numeri aequationi $tt - Duu = mm$ satisfacientes: in casu priori omnes transformationes formae φ in Φ contentae erunt sub prima formularum sequentium I, in posteriori vel sub prima I vel sub secunda II.

$$\text{I} \ldots\ldots \quad \tfrac{1}{m}(\alpha t - (\alpha b + \gamma c)u), \quad \tfrac{1}{m}(\vec{o} t - (\vec{o} b + \hat{o} c)u)$$
$$\tfrac{1}{m}(\gamma t + (\alpha a + \gamma b)u), \quad \tfrac{1}{m}(\hat{o} t + (\vec{o} a + \hat{o} b)u)$$
$$\text{II} \ldots\ldots \quad \tfrac{1}{m}(\alpha' t - (\alpha' b + \gamma' c)u), \quad \tfrac{1}{m}(\vec{o}' t - (\vec{o}' b + \hat{o}' c)u)$$
$$\tfrac{1}{m}(\gamma' t + (\alpha' a + \gamma' b)u), \quad \tfrac{1}{m}(\hat{o}' t + (\vec{o}' a + \hat{o}' b)u)$$

*) Quae Wallisius ad hunc finem protulit l. c. p. 127, 128 nihil ponderis habent. Paralogismus in eo consistit, quod p. 128 l. 1, supponit, proposita quantitate p inveniri posse numeros integros a, z tales ut $\frac{z}{a}$ minor sit quam p, defectus vero *assignato* minor. Hoc utique verum est, quando defectus *assignatus* est *quantitas data*, neque vero, quando ab a et z pendet adeoque variabilis est, uti in casu praesenti evenit.

Ex. Desiderantur omnes transformationes formae $(129, 92, 65)$ in formam $(42, 59, 81)$. Has improprie tantum aequivalentes esse in art. 195 invenimus et in art. seq. transformationem impropriam illius in hanc eruimus $-47, -56, 73, 87$. Quamobrem omnes transformationes formae $(129, 92, 65)$ in $(42, 59, 81)$ exhibebuntur per formulam

$$-(47t + 421u), \quad -(56t + 593u), \quad 73t + 653u, \quad 87t + 780u$$

ubi t, u sunt indefinite omnes numeri aequationi $tt - 79uu = 1$ satisfacientes; hi vero exhibentur per formulas

$$\pm t = \tfrac{1}{2}((80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e)$$
$$\pm u = \tfrac{1}{2\sqrt{79}}((80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e).$$

ubi pro e omnes numeri integri non negativi sunt accipiendi.

204.

Perspicuum est, formulam generalem omnes transformationes exhibentem eo *simpliciorem* evadere, quo simplicior fuerit transformatio initialis ex qua formula est deducta. Iam quum arbitrarium sit, a qua transformatione proficiscamur, saepenumero formula generalis simplicior reddi potest, si ex formula primo inventa transformatio simplicior deducitur tribuendo ipsis t, u valores determinatos, et tunc ex hac alia formula componitur. Ita *e. g.* positis in formula in ex. art. praec. inventa, $t = 80, u = -9$, prodit transformatio simplicior quam ea a qua profecti eramus, scilicet $29, 47, -37, -60$, unde deducitur formula generalis $29t - 263u, 47t - 424u, -37t + 337u, -60t + 543u$. Quando itaque per praecepta praecedentia formula generalis eruta est, tentari poterit, annon, tribuendo ipsis t, u valores determinatos $\pm t', \pm u'$; $\pm t'', \pm u''$ etc. transformatio obtineatur simplicior quam ea ex qua formula deducta fuit, in quo casu ex illa transformatione formula simplicior derivari poterit. — Ceterum in diiudicanda simplicitate aliquid arbitrarii remanet, quod si operae pretium esset ad normam fixam revocare, nec non in progressione $t', u'; t'', u''$ etc. *limites* assignare possemus, ultra quos transformationes continuo minus simplices prodeant, ita ut ultra progredi opus non sit sed intra illos tentamen instituisse sufficiat: attamen quum plerumque per methodos a nobis praescriptas transformatio simplicissima vel sta-

tim vel adhibitis pro t, u valoribus $\pm t'$, $\pm u'$ prodire soleat, hanc disquisitionem brevitatis gratia supprimimus.

205.

Problema. *Invenire omnes repraesentationes numeri dati M per formulam datam $axx + 2bxy + cyy$, cuius determinans positivus non-quadratus $= D$.*

Sol. Primo observamus, investigationem repraesentationum per valores ipsorum x, y inter se non primos, hic prorsus eodem modo, ut supra (art. 181) pro formis determinantis negativi, ad eum casum reduci posse, ubi repraesentationes per valores indeterminatarum inter se primos quaeruntur, quod igitur hic repetere superfluum foret. Ad possibilitatem repraesentationum per valores ipsorum x, y inter se primos autem requiritur, ut D sit residuum quadraticum ipsius M, et si omnes valores expressionis $\sqrt{D} \pmod{M}$ sunt $N, -N, N', -N', N'', -N''$ etc. (quos ita accipere licet ut nullus sit $> \frac{1}{2}M$), quaevis repraesentatio numeri M per formam propositam ad aliquem horum valorum pertinebit. Ante omnia itaque valores illi erui debebunt; tunc repraesentationes ad singulos pertinentes deinceps investigari. Repraesentationes ad valorem N pertinentes non dabuntur, nisi formae (a, b, c) et $(M, N, \frac{NN-D}{M})$ proprie aequivalentes sunt; si vero sunt, quaeratur transformatio aliqua propria prioris in posteriorem, quae sit $\alpha, \beta, \gamma, \delta$. Tum habebitur repraesentatio numeri M per formam (a, b, c) ad valorem N pertinens haec: $x = \alpha$, $y = \gamma$, omnesque repraesentationes ad hunc valorem pertinentes exhibebuntur per formulam

$$x = \tfrac{1}{m}(\alpha t - (\alpha b + \gamma c)u), \quad y = \tfrac{1}{m}(\gamma t + (\alpha a + \gamma b)u)$$

designante m divisorem communem maximum numerorum a, $2b$, c; et t, u indefinite omnes numeros aequationi $tt - Duu = mm$ satisfacientes. — Ceterum manifestum est, formulam hanc generalem eo simpliciorem evadere, quo simplicior sit transformatio $\alpha, \beta, \gamma, \delta$ ex qua deducta est; quare haud inutile erit, transformationem simplicissimam formae (a, b, c) in $(M, N, \frac{NN-D}{M})$, secundum art. praec. antea eruere, et ex hac formulam deducere. — Prorsus eodem modo repraesentationes ad valores reliquos $-N, N', -N'$ etc. pertinentes (si quae dantur) per formulas generales exhiberi possunt.

Ex. Quaeruntur omnes repraesentationes numeri 585 per formulam

$42xx + 62xy + 21yy$. Quod ad repraesentationes per valores ipsorum x, y inter se non primos pertinet, statim patet alias huius generis dari non posse, quam in quibus divisor communis maximus ipsorum x, y sit 3: quum 585 per unicum quadratum 9 divisibilis sit. Quando itaque omnes repraesentationes numeri $\frac{585}{9}$ *i. e.* 65 per formam $42x'x' + 62x'y' + 21y'y'$ inventae sunt, in quibus x' ad y' primus; omnes repraesentationes numeri 585 per formam $42xx + 62xy + 21yy$, in quibus x ad y non primus, ex illis derivabuntur ponendo $x = 3x'$, $y = 3y'$. Valores expressionis $\sqrt{79} \pmod{65}$ sunt ± 12, ± 27. Repraesentatio numeri 65 ad valorem -12 pertinens invenitur $x' = 2$, $y' = -1$; quocirca omnes repraesentationes ipsius 65 ad hunc valorem pertinentes exhibebuntur per formulam $x' = 2t - 41u$, $y' = -t + 53u$, adeoque omnes repraesentationes ipsius 585 *hinc* oriundae per formulam $x = 6t - 123u$, $y = -3t + 159u$. Simili modo invenitur formula generalis omnes repraesentationes numeri 65 ad valorem $+12$ pertinentes exhibens $x' = 22t - 199u$, $y' = -23t + 211u$; et formula omnes repraesentationes numeri 585 hinc oriundas complectens $x = 66t - 597u$, $y' = -69t + 633u$. Ad valores $+27$ et -27 autem nulla repraesentatio numeri 65 pertinet. — Ut repraesentationes numeri 585 per valores ipsorum x, y inter se primos inveniantur, primo valores expressionis $\sqrt{79} \pmod{585}$ eruere oportet, qui sunt ± 77, ± 103, ± 157, ± 248. Ad valores ± 77, ± 103, ± 248 invenitur nullam repraesentationem pertinere; ad valorem -157 autem pertinet repraesentatio $x = 3$, $y = 1$, unde deducitur formula generalis omnes repraesentationes ad hunc valorem pertinentes exhibens $x = 3t - 114u$, $y = t + 157u$; similiterque invenitur repraesentatio ad $+157$ pertinens $x = 83$, $y = -87$, et formula in qua omnes similes sunt contentae $x = 83t - 746u$, $y = -87t + 789u$. Habentur itaque quatuor formulae generales, sub quibus omnes repraesentationes numeri 585 per formam $42xx + 62xy + 21yy$ contentae sunt

$$\begin{array}{llll} x = & 6t - 123u & y = & -3t + 159u \\ x = & 66t - 597u & y = & -69t + 633u \\ x = & 3t - 114u & y = & t + 157u \\ x = & 83t - 746u & y = & -87t + 789u \end{array}$$

ubi t, u indefinite omnes numeros integros denotant, qui aequationi $tt - 79uu = 1$ satisfaciunt.

Applicationibus specialibus disquisitionum praecedentium de formis deter-

minantis positivi non-quadrati brevitatis gratia non immoramur, quippe quas simili modo ut artt. 176, 182 quisque, sine negotio, proprio marte instituere poterit, statimque ad formas determinantis positivi quadrati, quae solae adhuc supersunt, properamus.

De formis determinantis quadrati.

206.

Problema. *Proposita forma (a, b, c) determinantis quadrati hh, designante h ipsius radicem positivam, invenire formam (A, B, C) illi proprie aequivalentem, in qua A iaceat inter limites 0 et $2h-1$ incl., B sit $= h$, $C = 0$.*

Sol. I. Quoniam $hh = bb - ac$, erit $(h-b) : a = c : -(h+b)$. Sit huic rationi aequalis ratio $\vec{o} : \hat{o}$, ita ut $\vec{o}$ ad $\hat{o}$ sit primus, determinenturque α, γ ita ut sit $\alpha\hat{o} - \vec{o}\gamma = 1$, quae fieri poterunt. Per substitutionem $\alpha, \vec{o}, \gamma, \hat{o}$ transeat forma (a, b, c) in (a', b', c'), quae igitur illi proprie aequivalens erit. Habebitur autem

$$\begin{aligned} b' &= a\alpha\vec{o} + b(\alpha\hat{o} + \vec{o}\gamma) + c\gamma\hat{o} \\ &= (h-b)\alpha\hat{o} + b(\alpha\hat{o} + \vec{o}\gamma) - (h+b)\vec{o}\gamma \\ &= h(\alpha\hat{o} - \vec{o}\gamma) = h \\ c' &= a\vec{o}\vec{o} + 2b\vec{o}\hat{o} + c\hat{o}\hat{o} \\ &= (h-b)\vec{o}\hat{o} + 2b\vec{o}\hat{o} - (h+b)\vec{o}\hat{o} = 0 \end{aligned}$$

Quodsi itaque insuper a' inter limites 0 et $2h-1$ iam est situs, forma (a', b', c') omnibus conditionibus satisfaciet.

II. Si vero a' extra limites 0 et $2h-1$ iacet, sit A residuum minimum positivum ipsius a' secundum modulum $2h$, quod manifesto inter hos limites situm erit, ponaturque $A - a' = 2hk$. Tum forma (a', b', c') *i. e.* $(a', h, 0)$ per substitutionem $1, 0, k, 1$ transibit in formam $(A, h, 0)$, quae formis (a', b', c'), (a, b, c) proprie aequivalens erit omnibusque conditionibus satisfaciet. — Ceterum perspicuum est, formam (a, b, c) transire in formam $(A, h, 0)$ per substitutionem $\alpha + \vec{o}k, \vec{o}, \gamma + \hat{o}k, \hat{o}$.

Ex. Proposita sit forma $(27, 15, 8)$ cuius determinans $= 9$. Hic $h = 3$; rationibus $-12 : 27 = 8 : -18$ in numeris minimis aequalis est ratio $4 : -9$. Positis itaque $\vec{o} = 4$, $\hat{o} = -9$, $\alpha = -1$, $\gamma = 2$, forma (a', b', c') fit $(-1, 3, 0)$, quae transit in formam $(5, 3, 0)$ per substitutionem $1, 0, 1, 1$. Haec igitur est

forma quaesita, transitque in eam proposita per substitutionem propriam $3, 4, -7, -9$.

Tales formas (A, B, C), in quibus $C = 0$, $B = h$, A inter limites 0 et $2h-1$ situs, *formas reductas* vocabimus, quae igitur a formis reductis determinantis negativi, vel positivi non-quadrati, probe sunt distinguendae.

207.

Theorema. *Duae formae reductae $(a, h, 0)$, $(a', h, 0)$, non identicae proprie aequivalentes esse non possunt.*

Dem. Si enim proprie aequivalere supponuntur, transeat prior in posteriorem per substitutionem propriam $\alpha, \vec{o}, \gamma, \hat{o}$, habebunturque quatuor aequationes:

$$\begin{aligned} a\alpha\alpha + 2h\alpha\gamma &= a' \quad \ldots\ldots\ldots [1] \\ a\alpha\vec{o} + h(\alpha\hat{o} + \vec{o}\gamma) &= h \quad \ldots\ldots\ldots [2] \\ a\vec{o}\vec{o} + 2h\vec{o}\hat{o} &= 0 \quad \ldots\ldots\ldots [3] \\ \alpha\hat{o} - \vec{o}\gamma &= 1 \quad \ldots\ldots\ldots [4] \end{aligned}$$

Multiplicando aequationem secundam per $\vec{o}$, tertiam per α et subtrahendo fit $-h(\alpha\hat{o} - \vec{o}\gamma)\vec{o} = \vec{o}h$, sive, propter [4], $-\vec{o}h = \vec{o}h$, unde necessario $\vec{o} = 0$. Quare ex [4], $\alpha\hat{o} = 1$, et $\alpha = \pm 1$. Hinc ex [1], $a \pm 2\gamma h = a'$, quae aequatio consistere nequit, nisi $\gamma = 0$ (quoniam tum a tum a' per hyp. inter 0 et $2h-1$ iacent) *i. e.* nisi $a = a'$, sive formae $(a, h, 0)$, $(a', h, 0)$ identicae, contra hyp.

Hinc sequentia problemata, quae pro determinantibus non-quadratis multo maiorem difficultatem facessebant, nullo negotio solvi poterunt.

I. *Propositis duabus formis F, F' eiusdem determinantis quadrati, investigare an proprie aequivaleant.* Quaerantur duae formae reductae formis F, F' resp. proprie aequivalentes; quae si identicae sunt, propositae proprie aequivalentes erunt, sin minus, non erunt.

II. *Iisdem positis investigare an improprie aequivaleant.* Sit forma alterutri propositarum *e. g.* formae F opposita, G; quae si formae F' proprie aequivalet, F et F' improprie aequivalebunt, et contra.

208.

Problema. *Propositis duabus formis F, F' determinantis hh proprie aequivalentibus: invenire transformationem propriam alterius in alteram.*

Sol. Formae F proprie aequivaleat forma reducta Φ, quae itaque per hyp. etiam formae F' proprie aequivalebit. Quaeratur per art. 206 transformatio propria formae F in Φ, quae sit $\alpha, \beta, \gamma, \delta$; nec non transformatio propria formae F' in Φ, quae sit $\alpha', \beta', \gamma', \delta'$. Tunc Φ transformabitur in F' per substitutionem propriam $\delta', -\beta', -\gamma', \alpha'$ et hinc F in F' per substitutionem propriam

$$\alpha\delta' - \beta\gamma', \quad \beta\alpha' - \alpha\beta', \quad \gamma\delta' - \delta\gamma', \quad \delta\alpha' - \gamma\beta'$$

Operae pretium est, aliam formulam pro hac transformatione formae F in F' evolvere, ad quam formam reductam Φ ipsam novisse ne opus quidem sit. Ponamus formam

$$F \text{ esse } (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0)$$

Quoniam rationibus $h - b : a$ vel $c : -(h + b)$ in numeris minimis aequalis est ratio $\beta : \delta$, facile perspicitur $\frac{h-b}{\delta} = \frac{a}{\beta}$ fore *integrum*, qui sit f; nec non $\frac{c}{\beta} = \frac{-h-b}{\delta}$ integrum fore qui ponatur $= g$. Habebitur autem

$$A = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma \text{ adeoque } \beta A = a\alpha\alpha\beta + 2b\alpha\beta\gamma + c\beta\gamma\gamma$$

sive (substitutis pro $a\beta$, $\delta(h-b)$, pro c, βg)

$$\beta A = a\alpha\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta\beta\gamma\gamma g$$

sive (propter $b = -h - \delta g$)

$$\beta A = 2a(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g$$

Simili modo

$$\begin{aligned}\delta A &= a\alpha\alpha\delta + 2b\alpha\gamma\delta + c\gamma\gamma\delta \\ &= a\alpha\delta\delta f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma\gamma h \\ &= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f\end{aligned}$$

Quare

$$\alpha = \frac{\beta A - g}{2h}, \quad \gamma = \frac{\delta A - f}{2h}$$

Prorsus eodem modo positis

$$\frac{h-b'}{\beta'} = \frac{a'}{\delta'} = f', \quad \frac{c'}{\beta'} = \frac{-h-b'}{\delta'} = g'$$

fit

$$\alpha' = \frac{\beta' A - g'}{2h}, \quad \gamma' = \frac{\delta' A - f'}{2h}$$

Quibus valoribus ipsorum $\alpha, \gamma, \alpha', \gamma'$ in formula modo tradita pro transformatione formae F in F' substitutis, transit in hanc:

$$\frac{\beta' f' - b' g}{2h}, \quad \frac{\beta' g + b g'}{2h}, \quad \frac{\delta' f' - b' f}{2h}, \quad \frac{\delta' f - b g'}{2h}$$

ex qua A omnino abiit.

Si duae formae F, F' impropriae aequivalentes proponuntur, et transformatio impropria alterius in alteram quaeritur, sit forma G opposita formae F, et transformatio propria formae G in F' haec $\alpha, \beta, \gamma, \delta$. Tunc manifestum est, $\alpha, \beta, -\gamma, -\delta$ fore transformationem impropriam formae F in F'.

Denique patet, si formae propositae et proprie et improprie aequivalentes sint, hoc modo inveniri posse transformationes duas alteram propriam alteram impropriam.

209.

Nihil itaque iam superest quam ut ex una transformatione omnes reliquas similes deducere doceamus. Hoc vero pendet a solutione aequationis indeterminatae $tt - hhuu = mm$, designante m divisorem communem maximum numerorum $a, 2b, c$, si (a, b, c) est alterutra formarum aequivalentium. Sed haec aequatio semper duobus tantum modis solvi potest, nempe ponendo aut $t = m$, $u = 0$, aut $t = -m$, $u = 0$. Ponamus enim dari adhuc aliam solutionem $t = T$, $u = U$, ita ut U non $= 0$. Quia mm ipsum $4hh$ certo metitur, erit $\frac{4TT}{mm} = \frac{4hhUU}{mm} + 4$, atque tum $\frac{4TT}{mm}$ tum $\frac{4hhUU}{mm}$ quadrata integra. Sed nullo negotio perspicitur, numerum 4 duorum quadratorum integrorum differentiam esse non posse, nisi quadratum minus sit 0 *i. e.* $U = 0$, contra hyp. — Si itaque forma F in formam F' per substitutionem $\alpha, \beta, \gamma, \delta$ transit, alia transformatio huic similis non dabitur praeter transformationem $-\alpha, -\beta, -\gamma, -\delta$. Quare si duae formae aut proprie tantum, aut improprie tantum aequivalent, *duae* tantum transformationes dabuntur; si vero tum proprie tum improprie, *quatuor*, nempe duae propriae duaeque impropriae.

210.

THEOREMA. *Si duae formae reductae $(a, h, 0)$, $(a', h, 0)$ improprie sunt aequivalentes, erit $aa' \equiv mm \pmod{2mh}$, designante m divisorem communem maximum numerorum $a, 2h$, vel $a', 2h$; et vice versa, si $a, 2h$; $a', 2h$ eundem divisorem*

communem maximum m habent, atque est $aa' \equiv mm \pmod{2mh}$, *formae* $(a, h, 0)$, $(a', h, 0)$ *proprie aequivalentes erunt.*

Dem. I. Transeat forma $(a, h, 0)$ in formam $(a', h, 0)$ per substitutionem propriam $\alpha, \beta, \gamma, \delta$ ita ut habeantur quatuor aequationes

$$a\alpha\alpha + 2h\alpha\gamma = a' \quad \ldots\ldots\ldots\ldots [1]$$
$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad \ldots\ldots\ldots\ldots [2]$$
$$a\beta\beta + 2h\beta\delta = 0 \quad \ldots\ldots\ldots\ldots [3]$$
$$\alpha\delta - \beta\gamma = -1 \quad \ldots\ldots\ldots\ldots [4]$$

Hinc sequitur, multiplicando [4] per h et subtrahendo a [2], quod ita exprimimus $[2] - h\,[4]$,

$$(a\alpha + 2h\gamma)\beta = 2h \quad \ldots\ldots\ldots\ldots [5]$$

similiter ex $\gamma\delta\,[2] - \gamma\gamma\,[3] - (a + a\beta\gamma + h\gamma\delta)\,[4]$ deletis quae sese destruunt

$$-a\alpha\delta = a + 2h\gamma\delta, \text{ sive } -(a\alpha + 2h\gamma)\delta = a \quad [6]$$

denique ex $a\,[1] \ldots a\alpha\,(a\alpha + 2h\gamma) = aa'$, sive

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$$

sive

$$(a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)} \quad \ldots\ldots [7]$$

Iam ex [5] et [6] sequitur $a\alpha + 2h\gamma$ metiri ipsos $2h$ et a, adeoque etiam ipsum m, qui est divisor communis maximus ipsorum $a, 2h$; manifesto autem m metietur etiam ipsum $a\alpha + 2h\gamma$; quare necessario $a\alpha + 2h\gamma$ erit aut $= +m$ aut $= -m$. Hinc statim sequitur ex [7], $mm \equiv aa' \pmod{2mh}$. *Q. E. P.*

II. Si $a, 2h$; $a', 2h$ eundem divisorem communem maximum m habent, insuperque est $aa' \equiv mm \pmod{2mh}$, $\frac{a}{m}, \frac{2h}{m}, \frac{a'}{m}, \frac{aa' - mm}{2mh}$ erunt integri. Facile vero confirmatur, formam $(a, h, 0)$ transire in $(a', h, 0)$ per substitutionem $-\frac{a'}{m}, -\frac{2h}{m}, \frac{aa' - mm}{2mh}, \frac{a}{m}$; nec non hanc transformationem esse impropriam. Quare formae illae erunt improprie aequivalentes. *Q. E. S.*

Hinc etiam statim diiudicari potest, an forma aliqua reducta data $(a, h, 0)$ sibi ipsi improprie aequivalens sit. Scilicet designato divisore communi maximo numerorum $a, 2h$ per m, esse debebit $aa \equiv mm \pmod{2mh}$.

211.

Omnes formae reductae determinantis dati hh obtinentur, si in forma indefinita $(A, h, 0)$ pro A omnes numeri a 0 usque ad $2h - 1$ incl substituuntur, quarum itaque multitudo erit $2h$. Perspicuum est, omnes formas determinantis hh in totidem *classes* distribui posse, hasque iisdem proprietatibus praeditas fore quas supra (artt. 175, 195) pro classibus formarum determinantis negativi, et positivi non-quadrati attigimus. Ita omnes formae determinantis 25 in decem classes distribuentur, quae per formas reductas in singulis contentas distingui poterunt. Hae formae reductae sunt: $(0, 5, 0)$, $(1, 5, 0)$, $(2, 5, 0)$, $(5, 5, 0)$, $(8, 5, 0)$, $(9, 5, 0)$, quae sibi ipsae simul improprie aequivalent; $(3, 5, 0)$ cui improprie aequivalet $(7, 5, 0)$; $(4, 5, 0)$ cui improprie aequivalet $(6, 5, 0)$.

212.

Problema. *Invenire omnes repraesentationes numeri dati M per formam datam* $axx + 2bxy + cyy$ *determinantis* hh.

Solutio huius problematis ex principiis art. 168 prorsus eodem modo peti potest, ut supra (artt. 180, 181, 205) pro formis determinantis negativi et positivi non-quadrati ostendimus; quod, quum nulli difficultati sit obnoxium, hic repetere superfluum esset. Contra haud abs re erit, solutionem ex alio principio quod casui praesenti proprium est deducere.

Positis ut artt. 206, 208

$$h - b : a = c : -(h + b) = \beta : \delta$$
$$\frac{h-b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-h-b}{\delta} = g$$

nullo negotio probatur, formam propositam esse productum ex factoribus $\delta x - \beta y$ et $fx - gy$. Unde manifestum est, quamvis repraesentationem numeri M per formam propositam praebere resolutionem numeri M in binos factores. Si itaque omnes divisores numeri M sunt d, d', d'' etc. (inclusis etiam 1, et M, et singulis *bis* sumtis puta tum positive tum negative), patet omnes repraesentationes numeri M obtineri, si successive ponatur

$$\delta x - \beta y = d, \quad fx - gy = \frac{M}{d}$$
$$\delta x - \beta y = d', \quad fx - gy = \frac{M}{d'} \quad \text{etc.}$$

valores ipsorum x, y hinc evolvantur, eaeque repraesentationes eiiciantur ubi x

aut y valores fractos obtinent. Manifesto vero ex duabus primis aequationibus sequitur

$$x = \frac{\delta M - gdd}{(\delta f - \delta g)d} \quad \text{et} \quad y = \frac{\delta M - fdd}{(\delta f - \delta g)d}$$

quos valores semper *determinatos* fore inde manifestum quod $\delta f - \delta g = 2h$, adeoque numerator certo non $= 0$. — Ceterum ex eodem principio, puta resolubilitate cuiusvis formae determinantis quadrati in binos factores, etiam reliqua problemata solvi potuissent: sed methodo ei quam supra pro formis determinantis non-quadrati tradidimus analoga etiam hic uti maluimus.

Ex. Quaeruntur omnes repraesentationes numeri 12 per formam $3xx + 4xy - 7yy$. Haec resolvitur in factores $x - y$ et $3x + 7y$. Omnes divisores numeri 12 sunt $\pm 1, 2, 3, 4, 6, 12$. Positis $x - y = 1$, $3x + 7y = 12$, fit $x = 1\frac{3}{10}$, $y = \frac{3}{10}$, qui valores tamquam fracti sunt reiiciendi. Eodem modo ex divisoribus $-1, \pm 3, \pm 4, \pm 6, \pm 12$ valores inutiles obtinentur; ex divisore $+2$ vero obtinentur valores $x = 2, y = 0$, et ex divisore -2 hi $x = -2$, $y = 0$; praeter has duas repraesentationes igitur aliae non dantur.

Methodus haec adhiberi nequit, si $M = 0$. In hoc casu manifestum est omnes valores ipsorum x, y aut aequationi $\delta x - \delta y = 0$, aut huic $fx - gy = 0$ satisfacere debere. Omnes autem solutiones aequationis prioris continentur in formula $x = \delta z$, $y = \delta z$, designante z indefinite numerum integrum quemcunque (siquidem uti supponitur δ, δ inter se primi sunt); similiterque ponendo divisorem communem maximum numerorum f, g, $= m$, omnes solutiones aequationis posterioris exhibebuntur per formulam $x = \frac{gz}{m}$, $y = \frac{hz}{m}$. Quare hae duae formulae generales omnes repraesentationes numeri M in hoc casu complectentur.

* * *

In praecedentibus omnia quae ad cognoscendam aequivalentiam et ad inveniendas omnes transformationes formarum nec non ad repraesentationes omnes numerorum datorum per formas datas indagandas pertinent, ita sunt explicata, ut nihil amplius desiderari posse videatur. Superest itaque tantummodo, ut propositis duabus formis quae propter *determinantium inaequalitatem* aequivalentes esse nequeunt, diiudicare doceamus, annon altera sub altera contenta sit, et in hoc casu omnes transformationes illius in hanc invenire.

Formae sub aliis contentae quibus tamen non aequivalent.

213.

Supra artt. 157, 158 ostendimus, si forma f determinantis D formam F determinantis E implicet atque in ipsam transeat per substitutionem $\alpha, \delta, \gamma, \delta$, fore $E = (\alpha\delta - \delta\gamma)^2 D$; si fuerit $\alpha\delta - \delta\gamma = \pm 1$, formam f non modo implicare formam F sed ipsi aequivalentem esse et proin si f ipsam F implicet neque vero eidem aequivaleat, quotientem $\frac{E}{D}$ esse integrum maiorem quam 1. Problema itaque hic solvendum erit, *diiudicare an forma data f determinantis D formam datam F determinantis Dee implicet*, ubi e supponitur esse numerus positivus maior quam 1. Hoc negotium ita absolvemus, ut multitudinem finitam formarum sub f contentarum assignare doceamus quae ita sint comparatae, ut F si sub f contenta est necessario alicui ex illis aequivalere debeat.

I. Ponamus omnes divisores (positivos) numeri e (inclusis etiam 1 et e) esse m, m', m'' etc., atque $e = mn = m'n' = m''n''$ etc. Designemus brevitatis gratia formam in quam f transit per substitutionem propriam $m, 0, 0, n$ ita $(m; 0)$, formam in quam f transit per substitutionem propriam $m, 1, 0, n$ per $(m; 1)$ etc. generaliterque formam in quam f per subst. propriam, $m, k, 0, n$ transmutatur per $(m; k)$. Simili modo transeat f per subst. propriam $m', 0, 0, n'$ in $(m'; 0)$; per hanc $m', 1, 0, n'$ in $(m'; 1)$ etc., per $m'', 0, 0, n''$ in $(m''; 0)$ etc. etc. Omnes hae formae sub f proprie contentae erunt, et cuiusvis determinans $= Dee$. Complexum omnium formarum $(m; 0), (m; 1), (m; 2) \ldots (m; m-1), (m'; 0), (m'; 1) \ldots (m'; m'-1)$; $(m''; 0)$ etc. quarum multitudo erit $m + m' + m'' +$ etc. et quas omnes inter se diversas fore facile perspicitur, designemus per Ω.

Si *e. g.* forma f est haec $(2, 5, 7)$ atque $e = 5$, Ω comprehendet sequentes sex formas $(1; 0)$, $(5; 0)$, $(5; 1)$, $(5; 2)$, $(5; 3)$, $(5; 4)$ quae si evolvuntur sunt $(2, 25, 175)$, $(50, 25, 7)$, $(50, 35, 19)$, $(50, 45, 35)$, $(50, 55, 55)$, $(50, 65, 79)$.

II. Iam dico, si forma F determinantis Dee sub f proprie contenta sit, necessario eandem alicui formarum Ω proprie aequivalentem fore. Ponamus formam f transformari in F per substitutionem propriam $\alpha, \delta, \gamma, \delta$, eritque $\alpha\delta - \delta\gamma = e$. Sit numerorum γ, δ (qui ambo simul 0 esse nequeunt) divisor communis maximus positive acceptus $= n$, atque $\frac{e}{n} = m$, qui manifesto erit in-

teger. Accipiantur g, h ita ut sit $\gamma g + \delta h = n$, denique sit k residuum minimum positivum numeri $\alpha g + \beta h$ secundum modulum m. Tum forma $(m; k)$ quae manifesto erit inter formas Ω, formae F proprie aequivalebit, et quidem in ipsam transformabitur per substitutionem propriam

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h, \quad \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

Nam *primo* perspicuum est hos quatuor numeros esse integros; *secundo* facile confirmatur substitutionem esse propriam; *tertio* patet, formam in quam $(m; k)$ per substitutionem illam transeat eandem esse in quam f*) transeat per substitutionem

$$m\left(\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h\right)+\frac{k\gamma}{n}, \quad m\left(\frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g\right)+\frac{k\delta}{n}, \quad \gamma, \quad \delta$$

sive quoniam $mn = e = \alpha\delta - \beta\gamma$, adeoque $\beta\gamma + mn = \alpha\delta$, $\alpha\delta - mn = \beta\gamma$, per hanc

$$\frac{1}{n}(\alpha\gamma g + \alpha\delta h), \quad \frac{1}{n}(\beta\gamma g + \beta\delta h), \quad \gamma, \quad \delta$$

sive denique quoniam $\gamma g + \delta h = n$, per hanc $\alpha, \beta, \gamma, \delta$ *i. e.* per hyp., in F. Quare $(m; k)$ et F proprie aequivalentes erunt. *Q. E. D.*

Ex his igitur semper diiudicari potest, an forma aliqua data f determinantis D formam F determinantis Dee proprie implicet. Si vero quaeritur an f ipsam F improprie implicet, investigari tantummodo debet an forma ipsi F opposita sub f proprie contenta sit, art. 159.

214.

Problema. *Propositis duabus formis, f determinantis D, et F determinantis Dee, quarum prior posteriorem proprie implicat: exhibere omnes transformationes proprias formae f in F.*

Sol. Designante Ω eundem formarum complexum ut in art. praec., excerpantur ex hoc complexu omnes formae quibus F proprie aequivalet, quae sint Φ, Φ', Φ'' etc. Quaevis harum formarum sequenti modo suppeditabit transformationes proprias formae f in F, et quidem aliae alias (*i. e.* singulae diversas), cunctae vero cunctas (*i. e.* nulla transformatio propria formae f in F erit quam non una ex formis Φ, Φ' etc. praebeat). Quoniam methodus pro omnibus formis Φ, Φ' etc. eadem est, de una tantum loquemur.

*) Quippe quae per substitutionem $m, k, 0, n$ in $(m; k)$ transit V. art. 159.

Ponamus Φ esse $(M; K)$, atque $e = MN$ ita ut f in Φ per substitutionem propriam $M, K, 0, N$ transeat. Porro designentur omnes transformationes propriae formae Φ in F indefinite per $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$. Tum manifesto f transibit in Φ per substitutionem propriam $M\mathfrak{a} + K\mathfrak{c}$, $M\mathfrak{b} + K\mathfrak{d}$, $N\mathfrak{c}$, $N\mathfrak{d}$, et hoc modo ex quavis transformatione propria formae Φ in F sequetur transformatio propria formae f in F. — Eodem modo tractandae sunt formae reliquae Φ', Φ'' etc., quarum singulae transformationes propriae in F transformationem propriam formae f in F praebebunt.

Ut appareat, hanc solutionem ex omni parte completam esse, ostendendum erit

I. *Hoc modo omnes transformationes proprias possibiles formae f in F obtineri.* Sit transformatio quaecunque propria formae f in F haec $\alpha, \beta, \gamma, \delta$ atque ut in art. praec. II, n divisor communis maximus numerorum γ, δ; numeri m, g, h, k autem eodem modo ut illic determinati. Tunc forma $(m; k)$ erit inter formas Φ, Φ' etc., et

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h, \quad \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

aliqua ex transformationibus propriis huius formae in F; ex hac vero per regulam modo traditam obtinetur transformatio $\alpha, \beta, \gamma, \delta$; haec omnia in art. praec. sunt demonstrata.

II. *Omnes transformationes hoc modo prodeuntes inter se diversas esse, seu nullam bis obtineri.* Nullo quidem negotio perspicitur, plures transformationes diversas eiusdem formae Φ vel Φ' etc. in F eandem transformationem formae f in F producere non posse; quod vero etiam formae diversae e. g. Φ et Φ' eandem transformationem suppeditare nequeant, ita demonstratur. Supponamus, transformationem propriam $\alpha, \beta, \gamma, \delta$ formae f in F obtineri *tum* ex transformatione propria $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ formae Φ in F, *tum* ex transformatione propria $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \mathfrak{d}'$ formae Φ' in F. Sit $\Phi = (M; K)$, $\Phi' = (M'; K')$, $e = MN = M'N'$. Habebuntur itaque aequationes

$$\alpha = M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}' \quad \ldots\ldots [1]$$

$$\beta = M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{b}' \quad \ldots\ldots [2]$$

$$\gamma = N\mathfrak{c} = N'\mathfrak{c}' \quad \ldots\ldots [3]$$

$$\delta = Nb = N'b' \quad \ldots\ldots\ldots\ldots [4]$$

$$ab - bc = a'b' - b'c' = 1 \quad \ldots\ldots\ldots [5]$$

Ex $a[4] - b[3]$ sequitur adiumento aequ. [5], $N = N'(ab' - bc')$, quare N' metietur ipsum N; similiter ex $a'[4] - b'[3]$ fit $N(a'b - b'c) = N'$, quare N metietur ipsum N', unde, quia tum N tum N' supponuntur esse positivi, erit necessario $N = N'$, et $M = M'$, et hinc ex 3 et 4, $c = c'$, $b = b'$. Porro fit ex $a[2] - b[1]$,

$$K = M'(ab' - ba') + K'(ab' - bc') = M(ab' - ba') + K'$$

hinc $K \equiv K' \pmod{M}$ quod fieri nequit nisi $K = K'$, quia tum K tum K' iacent inter limites 0 et $M - 1$. Quamobrem formae Φ, Φ' non sunt diversae, contra hyp.

Ceterum patet, si D fuerit negativus vel positivus quadratus, per methodum hanc omnes transformationes proprias formae f in F revera inveniri posse; si vero D positivus non-quadratus; formulae certae generales assignari poterunt, in quibus omnes transformationes propriae (quarum multitudo infinita) contentae erunt.

Denique, si forma F improprie sub forma f contenta est, omnes transformationes impropriae illius in hanc per methodum traditam facile exhiberi poterunt. Scilicet si $\alpha, \delta, \gamma, \delta$ indefinite omnes transformationes proprias formae f in formam quae formae F opposita est, designare supponitur: omnes transf. impropriae formae f in F exhibebuntur per $\alpha, -\delta, \gamma, -\delta$.

Ex. Desiderantur omnes transformationes formae $(2, 5, 7)$ in $(275, 0, -1)$, quae sub illa tum proprie tum improprie contenta est. Complexum formarum Ω pro hoc casu iam in art. praec. tradidimus; examine instituto invenitur, tum $(5; 1)$ tum $(5; 4)$ formae $(275, 0, -1)$ proprie aequivalere. Omnes transformationes propriae formae $(5; 1)$ *i. e.* $(50, 35, 19)$ in $(275, 0, -1)$ per theoriam nostram supra explicatam inveniuntur contineri sub formula generali

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u$$

ubi t, u designant indefinite omnes numeros integros aequationi $tt - 275uu = 1$

satisfacientes; quare omnes transformationes propriae formae $(2, 5, 7)$ in $(275, 0, -1)$ hinc oriundae contentae erunt sub formula generali

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275u, \quad t - 15u$$

Simili modo omnes transformationes propriae formae $(5, 4)$ *i. e.* $(50, 65, 79)$ in $(275, 0, -1)$ continentur sub formula generali

$$14t + 275u, \quad t + 14u, \quad -15t - 275u, \quad -t - 15u$$

adeoque omnes transformationes propriae formae $(2, 5, 7)$ in $(275, 0, -1)$ hinc oriundae sub hac

$$10t + 275u, \quad t + 10u, \quad -15t - 275u, \quad -t - 15u$$

Hae duae formulae igitur omnes transformationes proprias quaesitas amplectuntur *). — Eodem vero modo invenitur, omnes transformationes improprias formae $(2, 5, 7)$ in $(275, 0, -1)$ sub sequentibus duabus formulis contentas esse:

(I) . . . $65t - 1100u, \quad 4t - 65u, \quad -15t + 275u, \quad -t + 15u$

et (II) . . . $10t + 275u, \quad -t - 10u, \quad -15t - 275u, \quad t + 15u$

Formae determinantis 0.

215.

Hucusque formas determinantis 0 ab omnibus disquisitionibus exclusimus; de his itaque, ut theoria nostra ab omni parte completa evadat, quaedam adhuc sunt adiicienda. Quoniam generaliter demonstratum est, si forma aliqua determinantis D formam determinantis D' implicet, D' esse multiplum ipsius D, statim patet, formam cuius determinans $= 0$ aliam formam quam cuius determinans etiam sit $= 0$ implicare non posse. Quare duo tantummodo problemata solvenda restant, scilicet 1° *propositis duabis formis f, F, quarum posterior habet determinantem 0, diiudicare utrum prior posteriorem implicet necne, et in illo casu omnes transformationes illius in hanc exhibere.* 2° *Invenire omnes repraesentationes numeri dati per formam datam determinantis* 0. Problema primum aliam metho-

*) Concinnius omnes transformationes propriae exhibentur per formulam

$$10t + 55u, \quad t + 2u, \quad -15t - 55u, \quad -t - 3u$$

denotantibus t, u indefinite omnes integros aequationi $tt - 11uu = 1$ satisfacientes.

dum requirit, quando determinans prioris formae f etiam est 0, aliam quando non est 0. Haec omnia iam exponemus.

I. Ante omnia observamus, quamvis formam $axx+2bxy+cyy$, cuius determinans $bb-ac=0$, ita exhiberi posse $m(gx+hy)^2$, denotantibus g, h numeros inter se primos, m integrum. Sit enim m divisor communis maximus ipsorum a, c eodem signo acceptus quo hi numeri ipsi sunt affecti (hos signa opposita habere non posse facile perspicitur), eruntque $\frac{a}{m}, \frac{c}{m}$ integri inter se primi non negativi, productum ex ipsis $=\frac{bb}{mm}$ *i. e.* quadratum, adeoque illi ipsi quadrata (art. 21). Sit $\frac{a}{m}=gg$, $\frac{c}{m}=hh$, eruntque etiam g, h inter se primi. $ggh h=\frac{bb}{mm}$, et $gh=\pm\frac{b}{m}$. Hinc patet

$$m(gx\pm hy)^2 \text{ fore } = axx+2bxy+cyy$$

Iam propositae sint duae formae f, F, utraque determinantis 0, et quidem sit

$$f=m(gx+hy)^2, \quad F=M(GX+HY)^2$$

ita ut g ad h, G ad H sint primi. Tum dico, si forma f implicet formam F, m aut ipsi M aequalem esse aut saltem ipsum M metiri et quotientem esse quadratum; et vice versa si $\frac{M}{m}$ sit quadratum integrum, F contentam esse sub f. Si enim f per substitutionem

$$x=\alpha X+\vartheta Y, \quad y=\gamma X+\delta Y$$

in F transire supponitur, erit

$$\frac{M}{m}(GX+HY)^2=(\alpha g+\gamma h)X+(\vartheta g+\delta h)Y)^2$$

unde facile sequitur $\frac{M}{m}$ esse quadratum. Ponatur $=ee$, eritque

$$e(GX+HY)=\pm((\alpha g+\gamma h)X+(\vartheta g+\delta h)Y), \text{ i. e.}$$
$$\pm eG=\alpha g+\gamma h, \quad \pm eH=\vartheta g+\delta h$$

si itaque $\mathfrak{G}, \mathfrak{H}$ ita determinantur ut sit $\mathfrak{G}G+\mathfrak{H}H=1$, erit

$$\pm e=\mathfrak{G}(\alpha g+\gamma h)+\mathfrak{H}(\vartheta g+\delta h), \text{ adeoque } \textit{integer}. \quad Q.\ E.\ P.$$

Si vero, vice versa, supponitur, $\frac{M}{m}$ esse quadratum integrum $=ee$, forma f implicabit formam F. Scilicet integri $\alpha, \vartheta, \gamma, \delta$ ita poterunt determinari ut fiat

$$\alpha g+\gamma h=\pm eG, \quad \vartheta g+\delta h=\pm eH$$

Accipiantur enim integri $\mathfrak{g}, \mathfrak{h}$ ita ut fiat $\mathfrak{g}g+\mathfrak{h}h=1$, satisfictque aequationibus illis ponendo

$$\alpha=\pm eG\mathfrak{g}+hz, \quad \gamma=\pm eG\mathfrak{h}-gz$$
$$\vartheta=\pm eH\mathfrak{g}+hz', \quad \delta=\pm eH\mathfrak{h}-gz'$$

quicunque valores integri ipsis z, z' tribuantur; quare F contenta erit sub f. *Q. E. S.* Simul haud difficulter intelligitur, has formulas omnes valores quos $\alpha, \vartheta, \gamma, \delta$ nancisci possunt, *i. e.* omnes transformationes formae f in F exhibere, si modo z, z' indefinite omnes numeros integros exhibere supponantur.

II. Propositis duabus formis $f=axx+2bxy+cyy$ cuius determinans non $=0$, et $F=M(GX+HY)^2$ cuius determinans $=0$ (designantibus ut ante G, H numeros inter se primos), dico *primo*, si f implicet ipsam F, numerum M per formam f repraesentari posse; *secundo*, si M per f repraesentari possit, F sub f contentam esse; *tertio*, si in hoc casu omnes repraesentationes numeri M per formam f indefinite exhibeantur ita $x=\xi, y=\upsilon$, omnes transformationes formae f in F exhiberi ita $G\xi, H\xi, G\upsilon, H\upsilon$. Quae omnia sequenti modo demonstramus.

1° Ponamus f transire in F per substitutionem $\alpha, \vartheta, \gamma, \delta$, accipianturque numeri $\mathfrak{G}, \mathfrak{H}$ ita ut sit $\mathfrak{G}G+\mathfrak{H}H=1$. Tunc manifestum est, si ponatur $x=\alpha\mathfrak{G}+\vartheta\mathfrak{H}$, $y=\gamma\mathfrak{G}+\delta\mathfrak{H}$, valorem formae f fieri M, adeoque M repraesentabilem esse per formam f.

2° Si supponitur esse $a\xi\xi+2b\xi\upsilon+c\upsilon\upsilon=M$, manifestum est, per substitutionem $G\xi, H\xi, G\upsilon, H\upsilon$, formam f transire in F. Quod vero

3° in hoc casu substitutio $G\xi, H\xi, G\upsilon, H\upsilon$ *omnes* transformationes formae f in F exhibeat, si ξ, υ supponantur exhibere omnes valores ipsorum x, y, qui faciunt $f=M$, ita perspicitur. Sit $\alpha, \vartheta, \gamma, \delta$ transformatio quaecunque formae f in F, et ut ante $\mathfrak{G}G+\mathfrak{H}H=1$. Tum inter valores ipsorum x, y erunt etiam hi

$$x=\alpha\mathfrak{G}+\vartheta\mathfrak{H}, \quad y=\gamma\mathfrak{G}+\delta\mathfrak{H}$$

ex quibus obtinetur substitutio

$$G(\alpha\mathfrak{G}+\vec{\sigma}\mathfrak{H}),\quad H(\alpha\mathfrak{G}+\vec{\sigma}\mathfrak{H}),\quad G(\gamma\mathfrak{G}+\delta\mathfrak{H}),\quad H(\gamma\mathfrak{G}+\delta\mathfrak{H})$$

sive

$$\alpha+\mathfrak{H}(\vec{\sigma}G-\alpha H),\quad \vec{\sigma}+\mathfrak{G}(\alpha H-\vec{\sigma}G)$$
$$\gamma+\mathfrak{H}(\delta G-\gamma H),\quad \delta+\mathfrak{G}(\gamma H-\delta G)$$

Sed quoniam

$$a(\alpha X+\vec{\sigma}Y)^2+2b(\alpha X+\vec{\sigma}Y)(\gamma X+\delta Y)+c(\gamma X+\delta Y)^2 = M(GX+HY)^2$$

erit

$$a(\alpha\delta-\vec{\sigma}\gamma)^2 = M(\delta G-\gamma H)^2$$
$$c(\vec{\sigma}\gamma-\alpha\delta)^2 = M(\vec{\sigma}G-\alpha H)^2$$

adeoque (quum determinans formae f per $(\alpha\delta-\vec{\sigma}\gamma)^2$ multiplicatus aequalis sit determinanti formae F i. e. $=0$, adeoque etiam $\alpha\delta-\vec{\sigma}\gamma=0$),

$$\delta G-\gamma H = 0,\quad \vec{\sigma}G-\alpha H = 0$$

Hinc substitutio illa transit in hanc $\alpha, \vec{\sigma}, \gamma, \delta$, unde patet, formulam traditam *omnes* transformationes formae f in F suppeditare.

III. Superest ut omnes repraesentationes numeri dati per formam datam determinantis 0 exhibere doceamus. Sit forma haec $m(gx+hy)^2$, patetque statim, numerum illum per m divisibilem, et quotientem quadratum esse debere. Si itaque numerus propositus statuitur $=mee$, perspicuum est, pro quibus valoribus ipsorum x, y fiat $m(gx+hy)^2=mee$, pro iisdem fieri $gx+hy$ aut $=+e$, aut $=-e$. Quare omnes repraesentationes habebuntur, si omnes solutiones aequationum linearium $gx+hy=e$, $gx+hy=-e$ in integris, sunt inventae. Has vero solubiles esse constat (siquidem g, h sunt inter se primi ut supponitur). Scilicet si $\mathfrak{g}$, $\mathfrak{h}$ ita determinantur ut sit $\mathfrak{g}g+\mathfrak{h}h=1$, aequationi priori satisfiet ponendo $x=\mathfrak{g}e+hz$, $y=\mathfrak{h}e-gz$; posteriori vero faciendo $x=-\mathfrak{g}e+hz$, $y=-\mathfrak{h}e-gz$, denotante z integrum quemcunque. Simul vero formulae hae *omnes* valores integros ipsorum x, y exhibent, si z indefinite numerum quemvis integrum designare supponitur.

Solutio generalis omnium aequationum indeterminatarum secundi gradus duas incognitas implicantium per numeros integros.

His disquisitionibus coronidis loco apponimus

216.

Problema. *Invenire omnes solutiones aequationis generalis *) indeterminatae secundi gradus duas incognitas implicantis*

$$axx+2bxy+cyy+2dx+2ey+f = 0$$

(ubi a, b, c etc. sunt integri quicunque dati) per numeros integros.

Sol. Introducamus loco incognitarum x, y alias

$$p = (bb-ac)x+be-cd \quad \text{et} \quad q = (bb-ac)y+bd-ae$$

qui manifesto semper erunt integri, quando x, y sunt integri. Quo facto habebitur aequatio

$$app+2bpq+cqq+f(bb-ac)^2+(bb-ac)(aee-2bde+cdd) = 0$$

sive posito brevitatis gratia numero

$$f(bb-ac)^2+(bb-ac)(aee-2bde+cdd) = -M$$

haec

$$app+2bpq+cqq = M$$

Iam omnes solutiones huius aequationis, i. e. omnes repraesentationes numeri M per formam (a, b, c) in praecedentibus invenire docuimus. Si vero ex singulis valoribus ipsorum p, q, valores respondentes ipsorum x, y adiumento aequationum

$$x = \frac{p+cd-be}{bb-ac},\quad y = \frac{q+ae-bd}{bb-ac}$$

determinantur, facile perspicitur, omnes hos valores aequationi propositae satisfacere, et nullos valores integros ipsorum x, y dari qui hoc modo non obtineantur. Si itaque ex omnibus valoribus ipsorum x, y sic prodeuntibus valores fractos eiicimus, omnes solutiones quaesitae remanebunt.

Circa hanc solutionem sequentia sunt observanda.

*) Si aequatio proponeretur in qua coefficiens secundus, quartus vel quintus non esset par, multiplicata per 2 eam formam reciperet quam hic supponimus.

1° Si aut M per formam (a, b, c) repraesentari non potest, aut ex nulla repraesentatione valores *integri* ipsorum x, y sequuntur: aequatio in integris nullo modo solvi poterit.

2° Quando determinans formae (a, b, c), *i. e.* numerus $bb - ac$ est negativus, vel positivus quadratus simulque M non $= 0$; multitudo repraesentationum numeri M per formam (a, b, c) erit finita, et proin etiam multitudo omnium solutionum aequationis propositae (si quae omnino dantur) finita erit.

3° Quando $bb - ac$ est positivus non-quadratus, vel quadratus et simul $M = 0$: numerus M, si ullo modo, *infinitis modis diversis* per formam (a, b, c) repraesentari poterit; sed quoniam impossibile est, has repraesentationes omnes *ipsas* invenire et tentare utrum valores integros ipsorum x, y praebeant an fractos, necessarium est regulam tradere, per quam, quando forte nulla omnino repraesentatio valores integros ipsorum x, y praebere potest, de hac re *certi* fieri possimus (nam quotcunque repraesentationes in hoc casu *tentatae* fuerint, absque tali regula ad certitudinem numquam perveniremus); quando vero aliae repraesentationes dant valores integros ipsorum x, y, aliae fractos: docendum erit quomodo hae ab illis a priori generaliter dignosci possint.

4° Quando $bb - ac = 0$: valores ipsorum x, y per formulas praecedentes omnino non possunt determinari; quare pro hoc casu *methodus peculiaris* investigari debebit.

217.

Pro eo casu, ubi $bb - ac$ est numerus positivus non-quadratus, supra docuimus, omnes repraesentationes numeri M per formam $app + 2bpq + cqq$ (si quae omnino dentur) exhiberi posse, per unam vel per plures formulas tales

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

denotantibus $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ numeros integros datos, m divisorem communem maximum numerorum $a, 2b, c$, denique t, u indefinite omnes numeros integros aequationi $tt - (bb - ac)uu = mm$ satisfacientes. Quoniam omnes valores ipsorum t, u tum positive tum negative accipi possunt: pro singulis illarum formarum *quaternas* alias substituere poterimus,

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$
$$p = \tfrac{1}{m}(\mathfrak{A}t - \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t - \mathfrak{D}u)$$

$$p = \tfrac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u)$$
$$p = -\tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = -\tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

ita ut multitudo omnium formularum nunc quater maior sit quam antea, t et u vero non amplius omnes numeros aequationi $tt - (bb - ac)uu = mm$ satisfacientes exprimant, sed positivos tantum. Quaevis harum formarum itaque seorsim considerari, et qui valores ipsorum t, u praebeant valores integros ipsorum x, y, investigari debebit.

Ex formula

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \quad \ldots\ldots [1]$$

sequuntur valores ipsorum x, y hi:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(bb - ac)}, \quad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(bb - ac)}$$

Supra vero ostendimus, omnes valores (positivos) ipsorum t constituere progressionem recurrentem t^0, t', t'' etc., similiter valores respondentes ipsius u quoque seriem recurrentem formare u^0, u', u'' etc.; praeterea assignari posse numerum ρ talem, ut secundum modulum quemcunque datum fiat

$$t^\rho \equiv t^0, \; t^{\rho+1} \equiv t', \; t^{\rho+2} \equiv t'' \text{ etc.}, \quad u^\rho \equiv u^0, \; u^{\rho+1} \equiv u' \text{ etc.}$$

Pro hoc modulo accipiemus numerum $m(bb - ac)$, designabimusque brevitatis gratia valores ipsorum x, y qui prodeunt ponendo $t = t^0$, $u = u^0$, et quibus tribuemus indicem 0, per x^0, y^0; similiterque eos qui prodeunt faciendo $t = t'$, $u = u'$, per x', y' quibus tribuemus indicem 1, etc. Tunc nullo negotio perspicietur, si x^h, y^h fuerint numeri integri atque ρ rite determinatus, etiam $x^{h+\rho}$, $y^{h+\rho}$; nec non $x^{h+2\rho}$, $y^{h+2\rho}$ et generaliter $x^{h+k\rho}$, $y^{h+k\rho}$, integros fore; et contra si x^h vel y^h sit fractus, etiam $x^{h+k\rho}$, vel $y^{h+k\rho}$ fractum fore. Hinc facile concluditur, si valores ipsorum x, y, quibus indices $0, 1, 2 \ldots \rho - 1$ competunt, evolvantur, et pro nullo horum indicum *tum* x, *tum* y integer sit, nullum omnino indicem dari, pro quo tum x, tum y valores integros recipiant, in quo casu ex formula [1] nulli valores integri ipsorum x, y deduci poterunt. Si vero inter illos indices aliqui sunt, puta μ, μ', μ'' etc. quibus valores integri ipsorum x, y respondent, omnes valores integri ipsorum x, y, qui quidem ex formula [1] obtineri possunt, ii erunt, quorum indices sub aliqua formularum $\mu + k\rho$, $\mu' + k\rho$,

$\mu'' + k\rho$ etc. sunt contenti, denotante k indefinite omnes numeros integros positivos, inclusa etiam cifra.

Formulae reliquae sub quibus valores ipsorum p, q contenti sunt, prorsus eodem modo sunt tractandae. Si contingeret, ut ex nulla omnium harum formularum valores integri ipsorum x, y obtineantur, aequatio proposita in integris nullo prorsus modo solvi posset; quoties vero revera est solubilis, omnes solutiones in integris per praecepta in praecc. tradita exhiberi poterunt.

218.

Quando $bb - ac$ est numerus quadratus atque $M = 0$, omnes valores ipsorum p, q comprehensi erunt sub duabus huiusmodi formulis $p = \mathfrak{A}z$, $q = \mathfrak{B}z$; $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, ubi z indefinite designat quemvis numerum integrum, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}'$, $\mathfrak{B}'$ vero sunt integri dati, quorum primus cum secundo, tertius cum quarto divisorem communem non habent (art. 212). Omnes itaque valores integri ipsorum x, y ex formula prima oriundi contenti erunt sub formula [1]

$$x = \frac{\mathfrak{A}z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{bb - ac}$$

omnesque reliqui ex formula secunda oriundi sub hac [2]

$$x = \frac{\mathfrak{A}'z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{bb - ac}$$

Sed quoniam utraque formula etiam valores fractos praebere potest (nisi $bb - ac = 1$), opus est ut eos valores ipsius z, qui tum ipsum x tum ipsum y integrum reddunt, a reliquis in utraque formula separemus; attamen sufficit primam solam considerare, quum pro altera prorsus eadem methodus adhibenda sit.

Quoniam $\mathfrak{A}$, $\mathfrak{B}$ inter se primi sunt, duos numeros $\mathfrak{a}$, $\mathfrak{b}$ ita determinare licebit, ut fiat $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$. Quo facto habetur

$$(\mathfrak{a}x + \mathfrak{b}y)(bb - ac) = z + \mathfrak{a}(ed - be) + \mathfrak{b}(ae - bd)$$

unde statim patet, omnes valores ipsius z qui valores integros ipsorum x, y producere possint, necessario numero $\mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ sec. mod. $bb - ac$ congruos, sive sub formula $(bb - ac)z' + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ contentos esse debere, designante z' indefinite numerum integrum. Hinc facile loco formulae [1] obtinemus sequentem

$$x = \mathfrak{A}z' + \mathfrak{b} \times \frac{\mathfrak{A}(\mathfrak{b}d - \mathfrak{a}e) - \mathfrak{B}(\mathfrak{b}e - \mathfrak{a}d)}{bb - ac}$$

$$y = \mathfrak{B}z' - \mathfrak{a} \times \frac{\mathfrak{A}(\mathfrak{b}d - \mathfrak{a}e) - \mathfrak{B}(\mathfrak{b}e - \mathfrak{a}d)}{bb - ac}$$

quam aut pro omnibus valoribus ipsius z' aut pro nullo valores integros ipsorum x, y praebere manifestum est, et quidem casus prior semper locum habebit, quando $\mathfrak{A}(\mathfrak{b}d - \mathfrak{a}e)$ et $\mathfrak{B}(\mathfrak{b}e - \mathfrak{a}d)$ sec. mod. $bb - ac$ sunt congrui, posterior quando sunt incongrui. — Prorsus eodem modo tractanda erit formula [2], solutionesque in integris (si quas praebere potest) a reliquis separandae.

219.

Quando $bb - ac = 0$, forma $axx + 2bxy + cyy$ exhiberi poterit ita: $m(\alpha x + \mathfrak{G}y)^2$, ubi m, α, $\mathfrak{G}$ sunt integri (art. 215). Ponatur $\alpha x + \mathfrak{G}y = z$, transitque aequatio proposita in hanc:

$$mzz + 2dx + 2ey + f = 0$$

unde et ex $z = \alpha x + \mathfrak{G}y$, deducitur

$$x = \frac{\mathfrak{G}mzz + 2ez + \mathfrak{G}f}{2\alpha e - 2\mathfrak{G}d}, \quad y = \frac{\alpha mzz + 2dz + \alpha f}{2\mathfrak{G}d - 2\alpha e}$$

Iam patet, nisi fuerit $\alpha e = \mathfrak{G}d$ (quem casum statim seorsim considerabimus), valores ipsorum x, y, ex his formulis deductos tribuendo ipsi z valorem quemcunque, aequationi propositae satisfacere; quare nihil superest, nisi ut eos valores ipsius z determinare doceamus, ex quibus valores integri ipsorum x, y sequantur.

Quoniam $\alpha x + \mathfrak{G}y = z$, necessario pro z numeri *integri* tantum accipi possunt; praeterea vero manifestum est, si aliquis valor ipsius z tum ipsum x tum ipsum y integrum reddat, omnes valores ipsius z illi secundum modulum $2\alpha e - 2\mathfrak{G}d$ congruos itidem valores integros producere. Quodsi itaque pro z omnes numeri integri a 0 usque ad $2\alpha e - 2\mathfrak{G}d - 1$ (quando $\alpha e - \mathfrak{G}d$ est positivus) aut ad $2\mathfrak{G}d - 2\alpha e - 1$ (quando $\alpha e - \mathfrak{G}d$ est negativus) incl. substituuntur, et pro nullo horum valorum tum x tum y integri fiunt, nullus omnino valor ipsius z valores integros ipsorum x, y producet, aequatioque proposita in integris nullo modo poterit resolvi; si vero quidam ex illis valoribus ipsius z ipsis x, y valores integros conciliant, puta hi ζ, ζ', ζ'' etc. (quos etiam per solutionem congruentiarum secundi gradus ex principiis sect. IV invenire licet); *omnes* solutiones prodi-

bunt ponendo $z = (2\alpha e - 2\delta d)v + \zeta$, $z' = (2\alpha e - 2\delta d)v + \zeta'$ etc., designante v indefinite omnes numeros integros.

229.

Pro eo quem exclusimus casu, ubi $\alpha e = \delta d$, methodum peculiarem indagare oportet. Supponamus, α, δ inter se primos esse, quod licere ex art. 215. I constat, eritque $\frac{d}{\alpha} = \frac{e}{\delta}$ numerus integer (art. 19), quem statuemus $= h$. Tunc aequatio proposita hanc induit formam:

$$(m\alpha x + m\delta y + h)^2 - hh + mf = 0$$

manifestoque adeo rationaliter solvi nequit, nisi $hh - mf$ fuerit numerus quadratus. Sit $hh - mf = kk$, patetque aequationi propositae sequentes duas aequivalere:

$$m\alpha x + m\delta y + h + k = 0, \quad \text{et} \quad m\alpha x + m\delta y + h - k = 0$$

i. e. quamlibet solutionem aequationis propositae etiam alterutri harum aequationum satisfacere, et vice versa. Aequatio prior manifesto in integris solvi nequit, nisi $h + k$ per m fuerit divisibilis, similiterque posterior solutionem in integris non admittet, nisi $h - k$ per m fuerit divisibilis. Hae vero conditiones ad resolubilitatem utriusque aequationis sufficiunt (quia α, δ inter se primi esse supponuntur), omnesque solutiones secundum regulas notas exhiberi poterunt.

221.

Casum in art. 217 consideratum (quia omnium difficillimus est) exemplo illustramus. Proposita sit aequatio $xx + 8xy + yy + 2x - 4y + 1 = 0$. Ex hac primo per introductionem aliarum incognitarum $p = 15x - 9$, $q = 15y + 6$ derivatur aequatio $pp + 8pq + qq = -540$. Huius autem solutiones omnes in integris, contineri inveniuntur sub quatuor formulis sequentibus:

$$\begin{aligned} p &= 6t, & q &= -24t - 90u \\ p &= 6t, & q &= -24t + 90u \\ p &= -6t, & q &= 24t - 90u \\ p &= -6t, & q &= 24t + 90u \end{aligned}$$

denotantibus t, u indefinite omnes numeros integros positivos aequationi

$tt - 15uu = 1$ satisfacientes, quos complectitur formula:

$$t = \tfrac{1}{2}\big((4 + \sqrt{15})^n + (4 - \sqrt{15})^n\big)$$
$$u = \tfrac{1}{2\sqrt{15}}\big((4 + \sqrt{15})^n - (4 - \sqrt{15})^n\big)$$

si n indefinite omnes numeros integros positivos (inclusa etiam cifra) designat. Quamobrem omnes valores ipsorum x, y contenti erunt sub formulis his:

$$\begin{aligned} x &= \tfrac{1}{5}(2t+3), & y &= -\tfrac{1}{5}(8t+30u+2) \\ x &= \tfrac{1}{5}(2t+3), & y &= -\tfrac{1}{5}(8t-30u+2) \\ x &= \tfrac{1}{5}(-2t+3), & y &= \tfrac{1}{5}(8t-30u-2) \\ x &= \tfrac{1}{5}(-2t+3), & y &= \tfrac{1}{5}(8t+30u-2) \end{aligned}$$

Praeceptis autem nostris rite applicatis, reperietur, ut valores *integri* prodeant, in formula prima et secunda eos valores ipsorum t, u accipi debere, qui proveniant ex indice n *pari*; in tertia quartaque vero eos, qui ex *impari* n obtineantur. — Solutiones simplicissimae habentur hae: $x = 1, -1, -1$; $y = -2, 0, 12$ resp.

Ceterum observare convenit, solutionem problematis in artt. praecc. explicati plerumque per multifaria artificia abbreviari posse, praesertim quantum ad exclusionem solutionum inutilium *i. e.* fractiones implicantium pertinet; sed haec ne nimis longi fiamus hoc loco praeterire coacti sumus.

Annotationes historicae.

222.

Quoniam complura ex iis quae hucusque pertractavimus etiam ab aliis geometris considerata sunt, horum merita silentio praeterire non possumus. De *formarum aequivalentia* disquisitiones generales instituit ill. La Grange, *Nouv. Mém. de l'Ac. de Berlin*, 1773 *p.* 263 et 1775 *p.* 323 sqq., ubi imprimis docuit, pro quovis determinante dato multitudinem finitam formarum dari ita comparatarum, ut quaevis forma illius determinantis alicui ex ipsis aequivalens sit, adeoque omnes formas determinantis dati in classes distribui posse. Postea clar. Le Gendre plures proprietates elegantes huius classificationis ad maximam partem per inductionem detexit, quas infra trademus demonstrationibusque muniemus. Ceterum distinctionem aequivalentiae propriae et impropriae, cuius usus maxime in disquisitionibus subtilioribus conspicuus est, nemo hucusque attigerat.

Problema famosum in art. 216 sqq. explicatum ill. La Grange primus com-

plete resolvit, *Hist. de l'Ac. de Berlin*, 1767 *p.* 165 et 1768 *p.* 181 sqq. Exstat solutio (sed minus completa) etiam in *Suppl. ad Euleri Algebram* iam saepius laudatis. Iam antea ill. Euler idem argumentum aggressus fuerat, *Comm. Petr. T.* VI *p.* 175; *Comm. Nov. T.* IX *p.* 3; *Ibid. T.* XVIII *p.* 185 sqq., sed investigationem suam eo semper restrinxit, ut ex aliqua solutione, quam iam cognitam esse supponit, aliae deriventur; praetereaque ipsius methodi in paucis tantummodo casibus *omnes* solutiones suppeditare valent (vid. La Grange *Hist. de l'Ac. de Berlin* 1767, *p.* 237). Quum ultima harum trium commentt. recentioris dati sit quam solutio La Grangiana, quae problema omni generalitate amplectitur nihilque hoc respectu desiderandum relinquit: Euler tunc temporis (Tomus XVIII Commentariorum pertinet ad annum 1773, et a. 1774 est publicatus) illam solutionem nondum novisse videtur. Ceterum solutio nostra (perinde ut omnia reliqua quae in hac sectione hactenus tradidimus), principiis omnino diversis est superstructa.

Quae ab aliis, Diophanto, Fermatio etc. huc pertinentia sunt tradita, casus maxime speciales spectant; quare quum eorum quae praesertim memoratu digna visa sunt, iam supra mentio facta sit, sigillatim omnia enarrare supersedemus.

* * *

Quae hactenus de formis secundi gradus exposuimus, pro primis tantum elementis huius doctrinae sunt habenda: innixius hanc disquisitionem persequentibus campus se aperuit nobis vastissimus, ex quo ea quae attentione imprimis digna videntur, in sequentibus excerpemus. Namque argumentum hoc tam fertile est, ut permulta alia, quae iam nunc invenire nobis contigit, brevitatis gratia silentio praeterire oporteat: multo vero plura sine dubio adhuc latent novosque conatus exspectant. Ceterum in limine harum investigationum statim adnotare convenit, formas determinantis 0 inde exclusas esse, nisi contrarium moneatur.

DISQUISITIONES ULTERIORES DE FORMIS.

Distributio formarum determinantis dati in classes.

223.

Iam supra (artt. 175, 195, 211) ostendimus, proposito numero quocunque integro D (sive positivo sive negativo) assignari posse multitudinem finitam formarum F, F', F'' etc. determinantis D, ita comparatarum, ut quaevis forma determinantis D proprie aequivalens sit alicui ex illis et quidem unicae tantum. Omnes igitur formae determinantis D (quarum multitudo est infinita) secundum illas formas *classificari* poterunt, formando scilicet e complexu omnium formarum formae F proprie aequivalentium classem primam; e formis quae formae F' proprie aequivalent, secundam etc.

Ex singulis classibus formarum determinantis dati D, forma aliqua eligi et tamquam *forma repraesentans* totius classis considerari poterit. Per se quidem prorsus arbitrarium est, quaenam forma ex quaque classe accipiatur, attamen ea semper praeferenda erit, quae reliquas *simplicitate* superare videtur. Simplicitas formae alicuius (a, b, c) manifesto ex magnitudine numerorum a, b, c aestimanda est, meritoque forma (a', b', c') minus simplex dicetur quam (a, b, c) si $a' > a$, $b' > b$, $c' > c$. Sed hinc res nondum determinatur penitus, arbitrioque nostro relinquitur *e. g.*, utram ex formis $(17, 0, -45)$, $(5, 0, -153)$ pro simpliciori habere malimus. Plerumque tamen e re erit, sequentem normam observare:

I. Quando determinans D est negativus, adoptentur formae reductae in singulis classibus contentae tamquam formae repraesentantes; ubi vero in eadem classe duae formae reductae reperiuntur (quae erunt oppositae, art. 172), recipiatur ea, cuius terminus medius positivus.

II. Quando determinans D est positivus non-quadratus, evolvatur periodus formae alicuius reductae in classe proposita contentae, in qua aut duae formae ancipites invenientur aut nulla (art. 187).

1) In casu priori sint formae ancipites hae: (A, B, C), (A', B', C'); residua minima numerorum B, B' secundum modulos A, A' resp. M, M' (quae positive accipi poterunt nisi sunt $= 0$); denique $\frac{D - MM}{A} = N$, $\frac{D - M'M'}{A'} = N'$. His ita factis, ex formis $(A, M, -N)$, $(A', M', -N')$ ea quae simplicissima videtur, pro forma repraesentante accipiatur. In hoc iudicio forma cuius terminus medius $= 0$, praeferatur; quando vero terminus medius aut in utraque aut in neutra est 0, ea quae terminum primum minorem habet, alteri praehabenda, et quando termini primi magnitudine sunt aequales signis diversi, signum negativum positivo postponendum.

2) Quando vero nulla forma anceps in tota periodo habetur, eligatur ex omnibus periodi formis ea quae terminum primum sine respectu signi minimum

habet, ita quidem, ut si duae formae in eadem periodo occurrant, in quarum altera idem terminus primus signo positivo affectus sit in altero negativo, posterior priori postponatur. Sit haec forma (A, B, C), deducaturque ex ipsa eodem modo ut in casu praec. forma alia $(A, M, -N)$ (puta, accipiendo pro M residuum absolute minimum ipsius B secundum mod. A, et faciendo $N = \frac{D-MM}{A}$): haec demum pro repraesentante adoptetur.

Quodsi vero eveniret, ut idem terminus primus minimus A pluribus periodi formis communis sit, omnes hae formae eo quo praescripsimus modo tractandae et ex formis prodeuntibus ea cuius terminus medius quam minimus evadit tamquam forma repraesentans assumenda erit.

Ita *e. g.* pro $D = 305$ habetur periodus inter alias haec: $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$, ex qua primo eligitur forma $(7, 16, -7)$, hinc que secundo deducitur forma repraesentans $(7, 2, -43)$.

III. Quando determinans est positivus quadratus $= kk$, eruatur forma reducta $(A, k, 0)$ in classe proposita contenta et, si $A < k$ aut $= k$, pro forma repraesentante ipsa recipiatur; si vero $A > k$, assumatur illius loco forma $(A - 2k, k, 0)$, cuius terminus primus erit negativus, sed minor quam k.

Ex. Hoc modo omnes formae determinantis -235 distribuuntur in classes sedecim, quarum repraesentantes erunt: $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$, octoque aliae a praecedentibus in solis signis terminorum externorum diversae $(-1, 0, -235)$, $(-2, 1, -118)$ etc.

Omnes formae determinantis 79 in sex classes discedunt, quarum repraesentantes $(1, 0, -79)$, $(3, 1, -26)$, $(3, -1, -26)$, $(-1, 0, 79)$, $(-3, 1, 26)$, $(-3, -1, 26)$.

224.

Per hanc itaque classificationem formae quae proprie aequivalentes sunt, a reliquis omnino segregabuntur. Duae formae eiusdem determinantis D, si ex eadem classe sunt, proprie aequivalentes erunt; quivis numerus per unam repraesentabilis etiam per alteram repraesentari poterit; et si numerus quicunque M per formam priorem ita repraesentari potest, ut indeterminatae valores inter se

primos habeant, idem numerus per alteram formam eodem modo repraesentari poterit, et quidem ita, ut utraque repraesentatio ad eundem valorem expressionis $\sqrt{D} \pmod{M}$ pertineat. Si vero duae formae ad classes diversas pertinent, proprie aequivalentes non erunt; a repraesentabilitate numeri alicuius dati per unam ad repraesentabilitatem eiusdem numeri per alteram concludi nequit; contra, si numerus M per alteram repraesentari potest ita ut valores indeterminatarum inter se primi sint, statim certi sumus, nullam similem repraesentationem eiusdem numeri per formam alteram dari, quae ad eundem valorem expr. $\sqrt{D} \pmod{M}$ pertineat (V. artt. 167, 168).

Contra utique fieri potest, ut formae duae F, F', e classibus diversis K, K' improprie aequivalentes sint, in quo casu *quaevis* forma ex altera classe *cuivis* formae ex altera improprie aequivalebit; quaevis forma ex K formam sibi oppositam habebit in K', classesque ipsae K, K' *oppositae* dicentur. Ita in exemplo primo art. praec. classis tertia formarum det. -235 quartae, septima octavae opposita est; in ex. secundo classis secunda tertiae, quinta sextae. Propositis itaque duabus formis quibuscunque e classibus oppositis, quivis numerus M qui per alteram repraesentari potest, etiam per alteram poterit; quod, si in altera fit per valores indeterminatarum inter se primos, in altera perinde fieri poterit, ita tamen, ut hae duae repraesentationes ad valores oppositos expr. $\sqrt{D} \pmod{M}$ pertineant. — Ceterum regulae supra traditae pro electione formarum repraesentantium ita sunt constitutae, ut classes oppositae formas repraesentantes oppositas semper nanciscantur.

Denique dantur etiam classes *sibi ipsis oppositae*. Scilicet si forma aliqua simul cum forma opposita in eadem classe continetur, facile perspicitur, omnes formas huius classis tum proprie tum improprie inter se aequivalentes esse, oppositasque suas secum habere. Hanc indolem quaevis classis habebit, in qua forma anceps continetur, et vice versa in quavis classe sibi ipsi opposita necessario forma anceps reperietur (art. 163, 165), quamobrem *classis anceps* nuncupabitur. Ita inter classes formarum determinantis -235 octo ancipites habentur, quarum repraesentantes sunt $(1, 0, 235)$, $(2, 1, 118)$, $(5, 0, 47)$, $(10, 5, 26)$, $(-1, 0, -235)$, $(-2, 1, -118)$, $(-5, 0, -47)$, $(-10, 5, -26)$; inter classes formarum determinantis 79 duae, quarum repraesentantes $(1, 0, -79)$, $(-1, 0, 79)$. — Ceterum si formae repraesentantes secundum regulas nostras determinatae sunt, classes ancipites nullo negotio inde cognosci poterunt. Scilicet pro determinante positivo

non-quadrato classis anceps certo formam repraesentantem ancipitem nanciscitur (art. 194); pro determinante negativo forma repraesentans classis ancipitis aut ipsa anceps erit, aut talis cuius termini externi sunt aequales (art. 172); denique pro determinante positivo quadrato per art. 210 facile diiudicatur, an forma repraesentans sibi ipsi improprie aequivalens sit adeoque classis, quam repraesentat, anceps.

225.

Iam supra (art. 175) ostendimus, in forma (a, b, c) determinantis negativi terminos externos eadem signa habere tum inter se tum cum terminis externis cuiusvis aliae formae illi aequivalentis. Si a, c sunt positivi, formam (a, b, c) *positivam* vocabimus, nec non totam classem in qua (a, b, c) continetur et quae e solis formis positivis constabit, *classem positivam* dicemus. Contra (a, b, c) erit *forma negativa*, et in *classe negativa* contenta, si a, c sunt negativi. Per formam positivam numeri negativi, per negativam positivi repraesentari nequeunt. Si forma (a, b, c) est repraesentans alicuius classis positivae, forma $(-a, b, -c)$ repraesentans classis negativae erit, unde sequitur, multitudinem classium positivarum multitudini negativarum aequalem esse, et, simul ac illae fuerint assignatae, etiam has haberi. Quocirca in disquisitionibus super formis determinantis negativi plerumque sufficit classes positivas considerare, quippe quarum proprietates ad classes negativas facile transferuntur.

Ceterum distinctio haec unice in formis determinantis negativi locum habet; per formas determinantis positivi sine discrimine numeri positivi et negativi repraesentari possunt, quin adeo haud raro duae formae tales (a, b, c), $(-a, b, -c)$ in hoc casu ad eandem classem sunt referendae.

Distributio classium in ordines.

226.

Formam quamcunque (a, b, c) *primitivam* vocamus, si numeri a, b, c divisorem communem non habent; alioquin dicitur *derivata*, et quidem, posito numerorum a, b, c divisore communi maximo $= m$, forma (a, b, c) erit *derivata e forma primitiva* $(\frac{a}{m}, \frac{b}{m}, \frac{c}{m})$. Ex hac definitione statim liquet, omnes formas, quarum determinans per nullum quadratum (praeter 1) divisibilis sit, necessario primitivas esse. Porro ex art. 161 patet, si in aliqua classe data formarum determinantis D forma primitiva inveniatur, omnes formas huius classis primitivas fore, in quo

casu classis ipsa *primitiva* dicetur. Porro manifestum est, si forma aliqua F determinantis D derivata sit ex forma primitiva f determinantis $\frac{D}{mm}$, classesque in quibus formae F, f resp. contineantur, sint K, k, omnes formas e classe K derivatas fore e classe primitiva k; quocirca classem K ipsam *ex classe primitiva k derivatam* in hoc casu vocabimus.

Si (a, b, c) est forma primitiva, neque vero a, c simul pares (*i. e.* si aut uterque impar aut saltem alteruter), facile intelligitur, non modo a, b, c, sed etiam $a, 2b, c$ divisorem communem habere non posse, in quo casu forma (a, b, c) dicitur *proprie primitiva* sive simpliciter *forma propria*. Si vero (a, b, c) est forma primitiva, numeri a, c autem ambo pares, patet, numeros $a, 2b, c$ divisorem communem 2 habere (qui simul erit maximus), vocabiturque (a, b, c) *forma improprie primitiva*, sive simpliciter *forma impropria**). In hoc casu b necessario erit impar (alioquin enim (a, b, c) non esset forma primitiva); quare erit $bb \equiv 1 \pmod 4$ adeoque quoniam ac per 4 divisibilis, determinans $bb - ac \equiv 1 \pmod 4$. Formae impropriae itaque tantummodo pro determinante formae $4n+1$, si est positivus, vel formae $-(4n+3)$, si est negativus, locum habent. — Ex art. 161 autem perspicuum est, si in classe aliqua data forma proprie primitiva inveniatur, omnes formas huius classis proprie primitivas esse; contra classem quae formam improprie primitivam implicet ex solis formis improprie primitivis constare. Quamobrem classis ipsa in casu priori *proprie primitiva* seu simpliciter *propria*; in posteriori *improprie primitiva* seu *impropria* appellabitur. Ita *e. g.* inter classes positivas formarum determinantis -235 sex sunt propriae, puta quarum repraesentantes $(1, 0, 235)$, $(1, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$, $(13, -5, 20)$, totidemque inter negativas; binae vero inter utrasque impropriae. — Classes formarum determinantis 79 (utpote numeri formae $4n+3$) omnes sunt propriae.

Si forma (a, b, c) est derivata, et quidem e primitiva $(\frac{a}{m}, \frac{b}{m}, \frac{c}{m})$, haec aut proprie primitiva aut improprie esse poterit. In casu priori m erit divisor communis maximus etiam numerorum $a, 2b, c$; in posteriori horum numerorum div. comm. max. erit $2m$. Hinc intelligitur distinctio inter *formam e forma proprie primitiva derivatam* et *formam ex improprie primitiva derivatam*; nec non (quoniam propter art. 161 omnes formae eiusdem classis hoc respectu perinde se habent)

*) Hos terminos *proprie* et *improprie* ideo hic elegimus, quia alii magis idonei non occurrebant, quod admonemus, ne quis inter hanc significationem eamque qua inde ab art. 157 usi sumus, nexum occultum quaerat, qui nullus adest. Ceterum ambiguitas certe hinc non est metuenda.

inter *classem derivatam e classe proprie primitiva* et *classem ex impropria primitiva derivatam*.

Per has distinctiones fundamentum primum nacti sumus, cui distributionem omnium classium formarum determinantis dati in varios *ordines* superstruere possumus. Classes duas, quarum repraesentantes sunt formae (a, b, c), (a', b', c') in *eundem ordinem* coniiciemus, si *tum* numeri a, b, c eundem divisorem communem maximum habent ut a', b', c', *tum* $a, 2b, c$ eundem ut $a', 2b', c'$; si vero aut alterutra aut utraque harum conditionum locum non habet, classes ad *ordines diversos* referentur. Hinc statim patet, omnes classes proprie primitivas unum ordinem constituere; omnes classes improprie primitivas, alium; si mm est quadratum determinantem D metiens, classes derivatae e classibus proprie primitivis determinantis $\frac{D}{mm}$ formabunt ordinem peculiarem, aliumque classes derivatae e classibus improprie primitivis determinantis $\frac{D}{mm}$ etc. Si forte D per nullum quadratum (praeter 1) divisibilis est, ordines classium derivatarum non aderunt adeoque aut unus tantum ordo dabitur (quando $D \equiv 2$ vel 3 secundum mod. 4), puta ordo classium proprie primitivarum, aut duo (quando $D \equiv 1 \pmod 4$) scilicet O. classium proprie primitivarum et O. cl. impr. primitivarum. Per principia calculi combinationum haud difficile conditur regula sequens generalis: Si supponitur $D = D' \, 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \ldots$, ita ut D' nullum factorem quadraticum implicet, et a, b, c etc. sint numeri primi impares diversi (ad quam formam quivis numerus redigi potest faciendo $\mu = 0$, quando D per 4 non est divisibilis; et α, β, γ etc. omnes $= 0$, sive quod eodem redit omittendo factores $a^{2\alpha}, b^{2\beta}, c^{2\gamma}$ etc., quando D per nullum quadratum impar dividi potest): habebuntur aut ordines

$$(\mu+1)(\alpha+1)(\beta+1)(\gamma+1)\ldots$$

nempe quando $D' \equiv 2$ vel $3 \pmod 4$; aut ordines

$$(\mu+2)(\alpha+1)(\beta+1)(\gamma+1)\ldots$$

quando $D' \equiv 1 \pmod 4$. Sed demonstrationem huius regulae supprimimus, quoniam neque difficilis neque hic adeo necessaria est.

Ex. 1. Pro $D = 45 = 5.3^2$ habentur sex classes, quarum repraesentantes $(1, 0, -45)$, $(-1, 0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3, 0, -15)$, $(6, 3, -6)$. Hae distribuuntur in quatuor ordines, scilicet O. I comprehendet duas classes proprias quarum repr. $(1, 0, -45)$, $(-1, 0, 45)$; O. II continebit duas classes improprias, quarum repr. $(2, 1, -22)$, $(-2, 1, 22)$; O. III continebit unam classem derivatam e propria determinantis 5, puta cuius repr. $(3, 0, -15)$; O. IV constabit ex una classe derivata ex impropria det. 5, puta cuius repr. $(6, 3, -6)$.

Ex. 2. Classes positivae determinantis $-99 = -11.3^2$ inter quatuor ordines distribuentur: O. I complectetur classes proprie primitivas sequentes *): $(1, 0, 99)$, $(4, 1, 25)$, $(4, -1, 25)$, $(5, 1, 20)$, $(5, -1, 20)$, $(9, 0, 11)$; O. II continebit classes improprias $(2, 1, 50)$, $(10, 1, 10)$; O. III classes derivatas e propriis determinantis -11, $(3, 0, 33)$, $(9, 3, 12)$, $(9, -3, 12)$; O. IV classem unicam derivatam ex impropria det. -11, $(6, 3, 18)$. — Classes negativae huius determinantis prorsus eodem modo in ordines distribui poterunt.

Observamus, *classes oppositas semper ad eundem ordinem referri*, cuius theorematis ratio nullo negotio perspicitur.

227.

Ex his diversis ordinibus imprimis ordo classium proprie primitivarum maximam attentionem meretur. Nam singulae classes derivatae a certis classibus primitivis (determinantis minoris) originem trahunt, ex quarum consideratione ea quae ad illas spectant plerumque sponte sequuntur. Infra autem docebimus, quamlibet classem improprie primitivam simili modo quasi associatam esse aut unicae classi proprie primitivae aut tribus (eiusdem determinantis). Porro pro determinantibus negativis classes negativas praeterire licebit, quippe quibus singulis certae classes positivae semper respondent. Ut itaque naturam classium proprie primitivarum profundius penetremus, ante omnia differentiam certam essentialem explicabimus, secundum quam totus ordo classium propriarum in plura *genera* subdividi potest. Quoniam hoc argumentum gravissimum hactenus nondum attigimus, res ab integro nobis erit repetenda.

Ordinum partitio in genera.

228.

Theorema. *Per formam quamcunque proprie primitivam F repraesentari possunt infinite multi numeri per numerum primum quemcunque datum p non divisibiles.*

Dem. Si forma $F = axx + 2bxy + cyy$, manifestum est, p omnes tres numeros $a, 2b, c$ simul metiri non posse. Iam quando a per p non est divisi-

*) Adhibendo brevitatis caussa formas repraesentantes pro classibus ipsis quarum vice funguntur.

bilis, patet, si pro x assumatur numerus quicunque per p non divisibilis, pro y vero numerus per p divisibilis, valorem formae F fieri non divisibilem per p; quando c per p non est divisibilis, idem obtinetur tribuendo ipsi x valorem divisibilem ipsique y valorem non divisibilem; denique quando tum a tum c per p sunt divisibiles, adeoque $2b$ non divisibilis, forma F valorem per p non divisibilem induet tribuendo tum ipsi x tum ipsi y valores quoscunque per p non divisibiles. Q. E. D.

Manifestum est, theorema etiam pro formis *improprie primitivis* locum habere, si modo non fuerit $p = 2$.

Quoniam plures huiusmodi conditiones simul consistere possunt, ut idem numerus per quosdam numeros primos datos divisibilis sit, per alios non divisibilis (v. art. 32): facile perspicitur, numeros x, y infinite multis modis ita determinari posse, ut forma primitiva $axx + 2bxy + cyy$ valorem per quotcunque numeros primos datos non divisibilem adipiscatur, a quibus unice excludendus est 2, quoties forma est improprie primitiva. Hinc patet, theorema generalius ita proponi posse: *Per formam quamcunque primitivam repraesentari possunt infinite multi numeri, qui ad numerum quemcunque datum (imparem, quando forma est improprie primitiva) sint primi.*

229.

Theorema. *Sit F forma primitiva determinantis D, p numerus primus ipsum D metiens: tum numeri per p non divisibiles qui per formam F repraesentari possunt, in eo convenient, ut vel omnes sint residua quadratica ipsius p, vel omnes non-residua.*

Dem. Sit $F = (a, b, c)$; m, m' duo numeri quicunque per p non divisibiles qui per formam F repraesentari possunt, scilicet

$$m = agg + 2bgh + chh, \quad m' = ag'g' + 2bg'h' + ch'h'$$

Tum erit

$$mm' = (agg' + b(gh' + hg') + chh')^2 - D(gh' - hg')^2$$

quare mm' quadrato congruus erit secundum modulum D, adeoque etiam secundum p, i. e. mm' erit residuum quadraticum ipsius p. Hinc sequitur, aut utrumque m, m' esse residuum quadraticum ipsius p, aut utrumque non-residuum. Q. E. D.

Simili modo probatur, quando determinans D per 4 sit divisibilis, omnes numeros impares per F repraesentabiles vel esse $\equiv 1$, vel omnes $\equiv 3 \pmod 4$. Scilicet productum e duobus numeris talibus in hoc casu semper erit residuum quadr. ipsius 4, adeoque $\equiv 1 \pmod 4$; quare vel uterque erit $\equiv 1$, vel uterque $\equiv 3$.

Denique quando D per 8 est divisibilis, productum e duobus numeris quibuscunque imparibus, qui per F repraesentari possunt, erit R. Q. ipsius 8 et proin $\equiv 1 \pmod 8$. Quare in hoc casu omnes numeri impares per F repraesentabiles vel erunt $\equiv 1$, vel omnes $\equiv 3$, vel omnes $\equiv 5$, vel omnes $\equiv 7 \pmod 8$.

Ita *e. g.* quum per formam $(10, 3, 17)$ repraesentari possit numerus 10 qui est N. R. ipsius 7: omnes numeri per 7 non divisibiles, qui per formam illam repraesentari possunt, non-residua ipsius 7 erunt. — Quum -3 per formam $(-3, 1, 49)$ repraesentabilis et sec. mod. 4 sit $\equiv 1$, omnes numeri impares per formam hanc repraesentabiles perinde se habebunt.

Ceterum, si ad propositum praesens necessarium esset, facile demonstrare possemus, numeros per formam F repraesentabiles ad nullum numerum primum qui ipsum D non metiatur, talem relationem fixam habere, sed promiscue tum residua tum non-residua numeri cuiusvis primi ipsum D non metientis per formam F repraesentari posse. Contra respectu numerorum 4 et 8 analogon quoddam etiam in aliis casibus locum habet, quos praeterire non possumus.

I. *Quando determinans D formae primitivae F est $\equiv 3 \pmod 4$: omnes numeri impares, per formam F repraesentabiles, erunt vel $\equiv 1$, vel omnes $\equiv 3 \pmod 4$.* Si enim m, m' sunt duo numeri per F repraesentabiles, productum mm' eodem modo ut supra sub formam $pp - Dqq$ redigi poterit. Quando itaque uterque m, m' est impar, necessario alter numerorum p, q par erit, alter impar adeoque alterum quadratorum $pp, qq, \equiv 0$, alterum $\equiv 1 \pmod 4$. Unde facile deducitur, $pp - Dqq$ certo esse $\equiv 1 \pmod 4$, adeoque aut utrumque $m, m', \equiv 1$, aut utrumque $\equiv 3 \pmod 4$. Ita *e. g.* per formam $(10, 3, 17)$ alii numeri impares quam qui sunt formae $4n + 1$ repraesentari nequeunt.

II. *Quando determinans D formae primitivae F est $\equiv 2 \pmod 8$: omnes numeri impares, per formam F repraesentabiles, erunt vel partim $\equiv 1$ partim $\equiv 7$, vel partim $\equiv 3$ partim $\equiv 5 \pmod 8$.* Ponamus enim m, m' esse duos numeros

impares per F repraesentabiles, quorum igitur productum mm' sub formam $pp - Dqq$ redigi poterit. Quando ergo uterque m, m' est impar, necessario p impar esse debebit (quia D par), adeoque $pp \equiv 1 \pmod 8$; qq vero erit vel $\equiv 0$ vel $\equiv 1$ vel $\equiv 4$, et proin Dqq vel $\equiv 0$ vel $\equiv 2$. Hinc $mm' \equiv pp - Dqq$ fit vel $\equiv 1$ vel $\equiv 7 \pmod 8$; si itaque m est vel $\equiv 1$ vel $\equiv 7$, etiam m' erit vel $\equiv 1$ vel $\equiv 7$; si vero m est vel $\equiv 3$ vel $\equiv 5$, etiam m' erit vel $\equiv 3$ vel $\equiv 5$. *E. g.* omnes numeri impares per formam $(3, 1, 5)$ repraesentabiles sunt aut $\equiv 3$ aut $\equiv 5 \pmod 8$, nullique numeri formae $8n+1$ aut $8n+7$ per formam illam repraesentari possunt.

III. *Quando determinans D formae primitivae F est $\equiv 6 \pmod 8$: per formam hanc repraesentari possunt numeri impares vel tales tantum qui sunt $\equiv 1$ et $\equiv 3 \pmod 8$, vel tales tantum qui sunt $\equiv 5$ et $\equiv 7 \pmod 8$.* Demonstrationem praecedenti (in II) omnino similem quisque nullo negotio evolvere poterit. — Ita *e. g.* per formam $(5, 1, 7)$ unice tales numeri impares possunt repraesentari qui sunt aut $\equiv 5$ aut $\equiv 7 \pmod 8$.

230.

Omnes igitur numeri qui per formam primitivam datam F determinantis D repraesentari possunt, relationem fixam habebunt ad singulos divisores primos ipsius D (per quos quidem ipsi non sunt divisibiles), numeri impares vero qui per F possunt repraesentari, in quibusdam casibus etiam ad numeros 4 et 8 relationem fixam habebunt, scilicet ad 4, quoties D aut $\equiv 0$ aut $\equiv 3 \pmod 4$, et ad 8, quoties D aut $\equiv 0$, aut $\equiv 2$ aut $\equiv 6 \pmod 8$ *). Talem relationem ad singulos hos numeros, *characterem* seu *characterem particularem* formae F vocabimus sequentique modo exprimemus: Quando sola residua quadratica numeri primi p per formam F repraesentari possunt, tribuemus ipsi characterem Rp, in casu opposito characterem Np; similiter scribemus 1, 4, quando alii numeri impares per formam F repraesentari nequeunt nisi qui sunt $\equiv 1 \pmod 4$, unde statim liquet quales characteres exprimantur per signa 3, 4; 1, 8; 3, 8; 5, 8; 7, 8. Denique formis per quas numeri impares tales soli repraesentari possunt qui sec.

*) Pro determinantibus per 8 divisibilibus relatio ad numerum 4 negligi potest, quoniam in hoc casu sub relatione ad 8 iam est contenta.

mod. 8 sunt vel $\equiv 1$ vel $\equiv 7$, tribuemus characterem 1 *et* 7, 8; ex quo significatio characterum 3 *et* 5, 8; 1 *et* 3, 8; 5 *et* 7, 8 sponte sequitur.

Characteres singuli formae primitivae datae (a, b, c) determinantis D semper ex uno saltem numerorum a, c (qui manifesto per formam illam ambo sunt repraesentabiles) cognosci possunt. Nam quoties p est divisor primus ipsius D, certe unus numerorum a, c per p non erit divisibilis; si enim uterque per p divisibilis esset, p etiam ipsum $bb (= D + ac)$ metiretur, et proin etiam ipsum b, *i. e.* forma (a, b, c) non esset primitiva. Simili modo in iis casibus, ubi forma (a, b, c) ad numerum 4 vel 8 relationem fixam habet, certo ad minimum unus numerorum a, c impar erit, ex quo igitur relatio illa deprehendi poterit. Ita *e. g.* character formae $(7, 0, 23)$ respectu numeri 23 e numero 7 concluditur $N23$, eiusdem formae character respectu numeri 7 habetur ex numero 23 puta $R7$; denique character huius formae respectu numeri 4, puta 3, 4, vel e numero 7 vel e numero 23 colligi potest.

Quoniam omnes numeri qui per formam aliquam F in classe K contentam repraesentari possunt, etiam per quamlibet aliam formam huius classis sunt repraesentabiles: manifesto singuli characteres formae F omnibus reliquis formis huius classis quoque competent, quapropter illos tamquam characteres totius classis considerare licebit. Singuli itaque characteres classis cuiuslibet primitivae datae ex ipsius forma repraesentante cognoscuntur. Classes oppositae semper characteres omnes eosdem habebunt.

231.

Complexus *omnium* characterum particularium formae vel classis datae constituet characterem integrum huius formae vel classis. Ita *e. g.* character integer formae $(10, 3, 17)$, vel totius classis quam repraesentat erit 1, 4; $N7$; $N23$. Simili modo character integer formae $(7, 1, -17)$ erit 7, 8; $R3$; $N5$, nam character particularis 3, 4 in hoc casu omittitur quia in characterе 7, 8 iam est contentus. — Ex hoc fonte petimus subdivisionem totius ordinis classium proprie primitivarum (positivarum quando det. est negativus) determinantis dati in plura *genera* diversa, referendo omnes classes, quae eundem characterem integrum habent, ad genus idem; quarumque characteres integri diversi sunt, ad genera diversa. Singulis vero generibus eos characteres integros tribuemus, quos classes sub ipsis contentae habent. Ita *e. g.* pro determinante -161 habentur sedecim

classes positivae proprie primitivae, quae sequenti modo in quatuor genera distribuuntur:

Character	Classium formae repraesentantes
$1,4;\ R7;\ R23$	$(1, 0, 161)$, $(2, 1, 81)$, $(9, 1, 18)$, $(9, -1, 18)$
$1,4;\ N7;\ N23$	$(5, 2, 33)$, $(5, -2, 33)$, $(10, 3, 17)$, $(10, -3, 17)$
$3,4;\ R7;\ N23$	$(7, 0, 23)$, $(11, 2, 15)$, $(11, -2, 15)$, $(14, 7, 15)$
$3,4;\ N7;\ R23$	$(3, 1, 54)$, $(3, -1, 54)$, $(6, 1, 27)$, $(6, -1, 27)$

De multitudine characterum integrorum diversorum, qui quidem a priori sunt possibiles, teneantur sequentia.

I. Quando determinans D per 8 est divisibilis, respectu numeri 8 quatuor characteres particulares diversi sunt possibiles; numerus 4 nullum characterem peculiarem suppeditat (annot. ad art. praec.). Praeterea respectu singulorum divisorum primorum imparium ipsius D bini characteres dantur; quare si illorum multitudo est m, dabuntur omnino 2^{m+2} characteres integri diversi (statuendo $m = 0$, quoties D est potestas binaria).

II. Quando det. D per 8 non est divisibilis, sed tamen per 4, insuperque per m numeros primos impares: omnino habebuntur 2^{m+1} characteres integri diversi.

III. Quando det. D est par neque vero per 4 divisibilis, erit vel $\equiv 2$ (mod. 8) vel $\equiv 6$. In casu priori dabuntur duo characteres particulares respectu numeri 8 puta 1 *et* 7, 8, atque 3 *et* 5, 8; in casu posteriori totidem. Posita igitur multitudine divisorum primorum imparium ipsius D, $= m$: habebuntur omnino 2^{m+1} characteres integri diversi.

IV. Quando D est impar, erit vel $\equiv 1$ vel $\equiv 3$ (mod. 4). In casu posteriori respectu numeri 4 duo characteres diversi dantur, qualis relatio in casu priori in characterem integrum non ingreditur. Quare designante m idem ut ante, in casu priori dabuntur 2^m, in posteriori 2^{m+1} characteres integri diversi.

Probe vero notandum est, hinc neutiquam sequi, totidem genera revera

dari quot characteres diversi a priori sint possibiles. In exemplo quidem nostro horum semissi tantum revera classes sive genera respondent; nullaeque classes positivae dantur, quibus characteres $1,4;\ R7;\ N23$ vel $1,4;\ N7;\ R23$; vel $3,4;\ R7;\ R23$ vel $3,4;\ N7;\ N23$ competant. De quo argumento gravissimo infra fusius agetur.

Formae $(1, 0, -D)$, quae haud dubie inter omnes formas determinantis D pro simplicissima habenda est, nomen *formae principalis* abhinc tribuemus; classem totam in qua illa reperitur, *classem principalem* vocabimus; denique genus totum in quo classis principalis contenta est, *genus principale* dicetur. Probe itaque distinguendae sunt forma principalis, forma e classe principali et forma e genere principali; nec non classis principalis et classis e genere principali. His denominationibus semper utemur, etiamsi forte pro determinante aliquo aliae classes praeter principalem, vel alia genera praeter genus principale non dentur, uti *e. g.* evenit plerumque, quando D est numerus primus positivus formae $4n + 1$.

232.

Quamquam ea quae de formarum characteribus explicata sunt proxime eum in finem sunt allata, ut subdivisio ordinis *positivi proprie primitivi* inde petatur: tamen nihil impedit quominus eadem etiam ad formas classesque negativas aut ad improprie primitivas applicentur, atque tum ordo improprie primitivus positivus, tum ordo proprie primitivus negativus, tum ordo improprie primitivus negativus ex eodem principio in genera subdividantur. Ita postquam *e. g.* ordo proprie primitivus formarum determinantis 145 in duo genera sequentia subdivisus est

$R5,\ R29$	$(1, 0, -145)$, $(5, 0, -29)$
$N5,\ N29$	$(3, 1, -48)$, $(3, -1, -48)$

etiam ordo improprie primitivus perinde in duo genera subdividi potest:

$R5,\ R29$	$(4, 1, -36)$, $(4, -1, -36)$
$N5,\ N29$	$(2, 1, -72)$, $(10, 5, -12)$

vel, sicuti classes positivae formarum determinantis -129 in quatuor genera distribuuntur:

1, 4; $R3$; $R43$	(1, 0, 129), (10, 1, 13), (10, −1, 13)
1, 4; $N3$; $N43$	(2, 1, 65), (5, 1, 26), (5, −1, 26)
3, 4; $R3$; $N43$	(3, 0, 43), (7, 2, 19), (7, −2, 19)
3, 4; $N3$; $R43$	(6, 3, 23), (11, 5, 14), (11, −5, 14)

etiam classes negativae in quatuor ordines discedunt

3, 4; $N3$; $N43$	(−1, 0, −129), (−10, 1, −13), (−10, −1, −13)
3, 4; $R3$; $R43$	(−2, 1, −65), (−5, 1, −26), (−5, −1, −26)
1, 4; $N3$; $R43$	(−3, 0, −43), (−7, 2, −19), (−7, −2, −19)
1, 4; $R3$; $N43$	(−6, 3, −23), (−11, 5, −14), (−11, −5, −14)

Attamen quum systema classium negativarum systemati positivarum semper tam simile evadat, plerumque superfluum videbitur illud seorsim construere. Ordinem improprie primitivum autem ad proprie primitivum reducere infra docebimus.

Tandem quod attinet ad ordines derivatos: pro harum subdivisione regulae novae non sunt necessariae. Quum enim quivis ordo derivatus ex aliquo ordine primitivo (determinantis minoris) originem trahat, illiusque classes singulae ad singulas huius sponte referantur: manifesto subdivisio ordinis derivati e subdivisione ordinis primitivi peti poterit.

233.

Si forma (primitiva) $F = (a, b, c)$ ita est comparata, ut inveniri possint duo numeri g, h tales ut fiat $gg \equiv a$, $gh \equiv b$, $hh \equiv c$ secundum modulum datum m, dicemus formam illam esse residuum quadraticum numeri m atque $gx+hy$ valorem expressionis $\sqrt{(axx+2bxy+cyy)}\,(\mathrm{mod.}\,m)$, sive brevius (g, h) valorem expr. $\sqrt{(a, b, c)}$ vel $\sqrt{F}\,(\mathrm{mod.}\,m)$. Generalius, si multiplicator M, ad modulum m primus, eius est indolis ut fieri possit

$$gg \equiv aM, \quad gh \equiv bM, \quad hh \equiv cM \pmod{m}$$

dicemus $M \times (a, b, c)$ sive MF esse res. quadr. ipsius m, atque (g, h) valorem expressionis $\sqrt{M(a, b, c)}$ vel $\sqrt{MF}\,(\mathrm{mod.}\,m)$. Ita e.g. forma (3, 1, 54) est res. quadr. ipsius 23 atque (7, 10) valor expr. $\sqrt{(3, 1, 54)}\,(\mathrm{mod.}\,23)$; similiter (2, −4) valor expr. $\sqrt{5}\,(10, 3, 17)\,(\mathrm{mod.}\,23)$. Usus harum definitionum infra ostendetur: hic notentur propositiones sequentes:

I. Si $M(a, b, c)$ est R. Q. numeri m, hic determinantem formae (a, b, c) metietur. Si enim (g, h) est valor expressionis $\sqrt{M(a, b, c)}\,(\mathrm{mod.}\,m)$, sive

$$gg \equiv aM, \quad gh \equiv bM, \quad hh \equiv cM \pmod{m}$$

erit $bbMM - acMM \equiv 0$, sive $(bb-ac)MM$ per m divisibilis. Quoniam autem M ad m primus esse supponitur, etiam $bb-ac$ per m divisibilis erit.

II. Si $M(a, b, c)$ est R. Q. ipsius m, atque m aut numerus primus aut potestas numeri primi, puta $= p^n$: character particularis formae (a, b, c) respectu numeri p erit vel Rp vel Np, prout M est residuum vel non-residuum ipsius p. Hoc statim inde sequitur, quod tum aM tum cM est residuum ipsius m sive ipsius p, atque ad minimum unus numerorum a, c per p non divisibilis (art. 230).

Simili modo, si (manentibus reliquis) $m = 4$, erit vel 1, 4 vel 3, 4 character part. formae (a, b, c), prout $M \equiv 1$ vel $\equiv 3$; nec non si $m = 8$ vel altior potestas numeri 2. erit 1, 8; 3, 8; 5, 8; 7, 8 char. part. formae (a, b, c), prout $M \equiv 1; 3; 5; 7 \pmod{8}$ resp.

III. Vice versa si m est numerus primus aut numeri primi imparis potestas $= p^n$, determinantem $bb-ac$ metiens, atque M vel residuum vel non-residuum ipsius p, prout character formae (a, b, c) respectu ipsius p est Rp vel Np resp., erit $M(a, b, c)$ resid. quadr. ipsius m. Quando enim a per p non est divisibilis, aM erit res. ipsius p adeoque etiam ipsius m; si itaque g est valor expr. $\sqrt{aM}\,(\mathrm{mod.}\,m)$, h valor expr. $\frac{bg}{a}\,(\mathrm{mod.}\,m)$, erit $gg \equiv aM$; $ah \equiv bg$, adeoque

$$agh \equiv bgg \equiv abM \quad \text{et} \quad gh \equiv bM$$

denique

$$ahh \equiv bgh \equiv bbM \equiv bbM - (bb-ac)M \equiv acM$$

adeoque $hh \equiv cM$, i. e. (g, h) valor expr. $\sqrt{M(a, b, c)}$. Quando vero a per m est divisibilis, certo c non erit; unde facile perspicitur, eadem resultare, si pro h assumatur valor expr. $\sqrt{cM}\,(\mathrm{mod.}\,m)$, pro g valor expr. $\frac{bh}{c}\,(\mathrm{mod.}\,m)$.

Simili modo demonstratur, si m fuerit $= 4$ ipsumque $bb-ac$ metiatur, numerusque M accipiatur vel $\equiv 1$ vel $\equiv 3$, prout 1, 4 vel 3, 4 fuerit char. part.

formae (a, b, c): fore $M(a, b, c)$ res. qu. ipsius m. Nec non, si m fuerit $= 8$ vel altior potestas ipsius 2, per quam $bb - ac$ divisibilis sit, atque M accipiatur $\equiv 1; 3; 5; 7 \pmod 8$, prout character part. formae (a, b, c) respectu numeri 8 postulet: $M(a, b, c)$ fore res. qu. ipsius m.

IV. Si determinans formae (a, b, c) est $= D$, atque $M(a, b, c)$ res. qu. ipsius D, omnes characteres particulares formae (a, b, c) tum respectu singulorum divisorum primorum imparium ipsius D, tum respectu numeri 4 vel numeri 8 (si ipsum D metiuntur) ex numero M statim cognosci possunt. Ita *e. g.* quum $3(20, 10, 27)$ sit resid. qu. ipsius 440, scilicet $(150, 9)$ valor expr. $\sqrt{3}(20, 10, 27)$ sec. mod. 440, atque $3N5$, $3R11$: characteres formae $(20, 10, 27)$ sunt $3, 8; N5; R11$. Soli characteres particulares respectu numerorum 4 et 8, quoties determinantem non metiuntur, nexum necessarium cum numero M non habent.

V. Vice versa, si numerus M ad D primus omnes characteres particulares formae (a, b, c) in se complectitur (exceptis characteribus respectu numerorum 4, 8, quando ipsum D non metiuntur): erit $M(a, b, c)$ res. qu. ipsius D. Nam ex III patet, si D sub formam $\pm A^\alpha B^\beta D^\gamma \ldots$ redigatur, ita ut A, B, C etc. sint numeri primi diversi, fore $M(a, b, c)$ resid. qu. singulorum $A^\alpha, B^\beta, C^\gamma$ etc. Si igitur valor expr. $\sqrt{M}(a, b, c)$ secundum mod. A^α, est $(\mathfrak{A}, \mathfrak{A}')$; secundum mod. B^β, $(\mathfrak{B}, \mathfrak{B}')$; sec. mod. C^γ, $(\mathfrak{C}, \mathfrak{C}')$ etc. numerique g, h ita determinantur ut sit $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc.; $h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ etc. secundum modulos $A^\alpha, B^\beta, C^\gamma$ etc. resp. (art. 32): facile perspicietur, fore $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ secundum omnes modulos $A^\alpha, B^\beta, C^\gamma$ etc. adeoque etiam secundum modulum D qui illorum est productum.

VI. Propter has rationes numeri tales ut M vocabuntur *numeri characteristici* formae (a, b, c), poteruntque per V plures huiusmodi numeri nullo negotio inveniri, simulac omnes characteres particulares huius formae sunt eruti; simplicissimi autem tentando plerumque evolvuntur facillime. Manifestum est, si M sit numerus characteristicus formae primitivae datae determinantis D, omnes numeros, ipsi M secundum mod. D congruos, fore numeros characteristicos eiusdem formae; formas in eadem classe, sive etiam in classibus diversis ex eodem genere, contentas eosdem numeros characteristicos habere, quamobrem quivis numerus

characteristicus formae datae etiam toti classi et generi tribui potest; denique semper esse numerum characteristicum formae classis et generis principalis, sive quamlibet formam e genere principali esse residuum determinantis sui.

VII. Si (g, h) est valor expr. $\sqrt{M}(a, b, c) \pmod m$, atque $g' \equiv g$, $h' \equiv h \pmod m$: erit etiam (g', h') valor eiusdem expressionis. Tales valores pro *aequivalentibus* haberi possunt; contra si (g, h), (g', h') sunt valores eiusdem expr. $\sqrt{M}(a, b, c)$, neque tamen simul $g' \equiv g$, $h' \equiv h \pmod m$, *diversi* sunt censendi. Manifesto quoties (g, h) est valor talis expressionis, etiam $(-g, -h)$ erit, facileque demonstratur, hos valores semper esse diversos nisi $m = 2$. Aeque facile demonstratur, expressionem $\sqrt{M}(a, b, c) \pmod m$ plures valores diversos quam duos tales (oppositos) habere non posse, quando m sit aut numerus primus impar aut numeri primi imparis potestas aut $= 4$; quando vero m sit $= 8$ aut altior potestas numeri 2, quatuor omnino dari. Hinc facile deducitur per VI, si determinans D formae (a, b, c) sit $= \pm 2^\alpha A^\alpha B^\beta \ldots$, designantibus A, B etc. numeros primos impares diversos quorum multitudo $= n$, atque M numerus characteristicus illius formae: dari omnino vel 2^n vel 2^{n+1} vel 2^{n+2} valores diversos expr. $\sqrt{M}(a, b, c) \pmod D$, prout μ vel < 2 vel $= 2$ vel > 2. Ita *e. g.* habentur sedecim valores expr. $\sqrt{7}(12, 6, -17) \pmod{240}$, puta $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Demonstrationem ampliorem quum ad sequentia non sit adeo necessaria, brevitatis gratia non apponimus.

VIII. Denique observamus, si duarum formarum acquivalentium (a, b, c), (a', b', c') determinans sit D, numerus characteristicus M, priorque transeat in posteriorem per substitutionem $\alpha, \beta, \gamma, \delta$: ex quovis valore expr. $\sqrt{M}(a, b, c)$ ut (g, h) sequi valorem expr. $\sqrt{M}(a', b', c')$, puta $(\alpha g + \gamma h, \beta g + \delta h)$. Demonstrationem quisque nullo negotio eruere poterit.

De compositione formarum.

234.

Postquam haec de formis in classes genera et ordines distribuendis praemisimus, proprietatesque generales quae ex his distinctionibus statim defluunt explicavimus, ad aliud argumentum gravissimum transimus a nemine hucusque

attactum, de formarum *compositione*. In cuius disquisitionis limine, ne posthac demonstrationum seriem continuam interrumpere oporteat, statim intercalamus

LEMMA. *Habentur quatuor series numerorum integrorum*

$$a, a', a'' \ldots a^{n}; \quad b, b', b'' \ldots b^{n}; \quad c, c', c'' \ldots c^{n}; \quad d, d', d'' \ldots d^{n}$$

ex aeque multis (puta $n+1$) terminis constantes, atque ita comparatae, ut

$$cd' - dc', \quad cd'' - dc'' \text{ etc.}, \quad c'd'' - d'c'' \text{ etc. etc.}$$

respective sint

$$= k(ab' - ba'), \quad k(ab'' - ba'') \text{ etc.}, \quad k(a'b'' - b'a'') \text{ etc. etc.}$$

sive generaliter

$$c^{\lambda} d^{\mu} - d^{\lambda} c^{\mu} = k(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})$$

*denotante k numerum integrum datum; λ, μ integros quoscunque inaequales inter 0 et n incl. quorum maior μ *); praetereа omnes $a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu}$ divisorem communem non habent. Tunc inveniri possunt quatuor numeri integri $\alpha, \vartheta, \gamma, \delta$ tales, ut sit*

$$\alpha a + \vartheta b = c, \quad \alpha a' + \vartheta b' = c', \quad \alpha a'' + \vartheta b'' = c'' \text{ etc.}$$
$$\gamma a + \delta b = d, \quad \gamma a' + \delta b' = d', \quad \gamma a'' + \delta b'' = d'' \text{ etc.}$$

sive generaliter

$$\alpha a^{\nu} + \vartheta b^{\nu} = c^{\nu}, \quad \gamma a^{\nu} + \delta b^{\nu} = a^{\nu}$$

quo facto erit

$$\alpha\delta - \vartheta\gamma = k$$

Quum per hyp. numeri $ab' - ba'$, $ab'' - ba''$ etc. $a'b'' - b'a''$ etc. (quorum multitudo erit $= \frac{1}{2}(n+1)n$) divisorem communem non habeant, inveniri poterunt totidem alii numeri integri, per quos illis resp. multiplicatis productorum summa fiat $= 1$ (art. 40). Designentur hi multiplicatores per $(0,1)$, $(0,2)$ etc. $(1,2)$ etc., sive generaliter multiplicator ipsius $a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu}$ per (λ, μ), ita ut sit

$$\Sigma(\lambda, \mu)(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu}) = 1$$

(Per literam Σ denotamus aggregatum omnium valorum expressionis, cui praefixa

*) Considerando a tamquam a^0, b tamquam b^0 etc. — Ceterum manifesto eadem aequatio valebit quoque quando $\lambda = \mu$ aut $\lambda > \mu$.

est, qui oriuntur tribuendo ipsis λ, μ omnes valores inaequales inter 0 et n, ita ut sit $\mu > \lambda$). Quo facto si statuitur

$$\Sigma(\lambda, \mu)(c^{\lambda} b^{\mu} - b^{\lambda} c^{\mu}) = \alpha, \quad \Sigma(\lambda, \mu)(a^{\lambda} c^{\mu} - c^{\lambda} a^{\mu}) = \vartheta$$
$$\Sigma(\lambda, \mu)(d^{\lambda} b^{\mu} - b^{\lambda} d^{\mu}) = \gamma, \quad \Sigma(\lambda, \mu)(a^{\lambda} d^{\mu} - d^{\lambda} a^{\mu}) = \delta$$

hi $\alpha, \vartheta, \gamma, \delta$ proprietatibus praescriptis erunt praediti.

Dem. I. Denotante ν numerum quemcunque integrum inter 0 et n, erit

$$\begin{aligned} \alpha a^{\nu} + \vartheta b^{\nu} &= \Sigma(\lambda, \mu)(c^{\lambda} b^{\mu} a^{\nu} - b^{\lambda} c^{\mu} a^{\nu} + a^{\lambda} c^{\mu} b^{\nu} - c^{\lambda} a^{\mu} b^{\nu}) \\ &= \tfrac{1}{k} \Sigma(\lambda, \mu)(c^{\lambda} d^{\mu} c^{\nu} - d^{\lambda} c^{\mu} c^{\nu}) \\ &= \tfrac{1}{k} c^{\nu} \Sigma(\lambda, \mu)(c^{\lambda} d^{\mu} - d^{\lambda} c^{\mu}) \\ &= c^{\nu} \Sigma(\lambda, \mu)(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu}) = c^{\nu} \end{aligned}$$

Et per calculum similem eruitur

$$\gamma a^{\nu} + \delta b^{\nu} = d^{\nu}. \quad Q.\ E.\ P.$$

II. Quoniam igitur

$$c^{\lambda} = \alpha a^{\lambda} + \vartheta b^{\lambda}, \quad c^{\mu} = \alpha a^{\mu} + \vartheta b^{\mu}$$

fit

$$c^{\lambda} b^{\mu} - b^{\lambda} c^{\mu} = \alpha(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})$$

similique modo

$$a^{\lambda} c^{\mu} - c^{\lambda} a^{\mu} = \vartheta(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})$$
$$d^{\lambda} b^{\mu} - b^{\lambda} d^{\mu} = \gamma(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})$$
$$a^{\lambda} d^{\mu} - d^{\lambda} a^{\mu} = \delta(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})$$

ex quibus formulis valores ipsorum α, ϑ, γ, δ multo facilius erui possunt, si modo λ, μ ita accipiuntur, ut $a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu}$ non sit $= 0$, quod certo fieri poterit, quia omnes $a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu}$ per hyp. divisorem communem non habent, adeoque *omnes* $= 0$ esse nequeunt. — Ex iisdem aequationibus deducitur, multiplicando primam per quartam, secundam per tertiam et subtrahendo,

$$(\alpha\delta - \vartheta\gamma)(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})^2 = (a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})(c^{\lambda} d^{\mu} - d^{\lambda} c^{\mu}) = k(a^{\lambda} b^{\mu} - b^{\lambda} a^{\mu})^2$$

unde necessario

$$\alpha\delta - \vartheta\gamma = k. \quad Q.\ E.\ S.$$

235.

Si forma $$AXX+2BXY+CYY...F$$ transit in productum e duabus formis

$$axx+2bxy+cyy...f, \text{ et } a'x'x'+2b'x'y'+c'y'y'...f'$$

per substitutionem talem

$$X = pxx'+p'xy'+p''yx'+p'''yy'$$
$$Y = qxx'+q'xy'+q''yx'+q'''yy'$$

(quod brevitatis causa in sequentibus semper ita exprimemus: Si F transit in ff' per substitutionem $p, p', p'', p'''; q, q', q'', q'''$*)), dicemus simpliciter, formam F *transformabilem* esse in ff'; si insuper haec transformatio ita est comparata, ut sex numeri

$$pq'-qp', \; pq''-qp'', \; pq'''-qp''', \; p'q''-q'p'', \; p'q'''-q'p''', \; p''q'''-q''p'''$$

divisorem communem non habeant: formam F e formis f, f' *compositam* vocabimus.

Inchoabimus hanc disquisitionem a suppositione generalissima, formam F in ff' transire per substitutionem $p, p', p'', p'''; q, q', q'', q'''$ et quae inde sequantur evolvemus. Manifesto huic suppositioni ex asse aequivalebunt sequentes novem aequationes (*i. e.* simulac hae aequationes locum habent, F per substitutionem dictam transibit in ff', et vice versa):

$$App + 2Bpq + Cqq = aa' \quad [1]$$
$$Ap'p' + 2Bp'q' + Cq'q' = ac' \quad [2]$$
$$Ap''p'' + 2Bp''q'' + Cq''q'' = ca' \quad [3]$$
$$Ap'''p''' + 2Bp'''q''' + Cq'''q''' = cc' \quad [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \quad [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \quad [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' \quad [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' \quad [8]$$
$$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb' \quad [9]$$

*) In hac igitur designatione ad ordinem tum coefficientium p, p' etc. tum formarum f, f' probe respicere oportet. Facile autem perspicietur, si ordo formarum f, f' convertatur ut prior fiat posterior, coefficientes p', q' cum his p'', q'' commutandos esse, reliquos suo quemlibet loco manere.

Sint determinantes formarum F, f, f' resp. D, d, d'; divisores communes maximi numerorum $A, 2B, C$; $a, 2b, c$; $a', 2b', c'$ resp. M, m, m' (quos omnes positive acceptos supponimus). Porro determinentur sex numeri integri $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ ita ut sit

$$\mathfrak{A}a+2\mathfrak{B}b+\mathfrak{C}c = m, \quad \mathfrak{A}'a'+2\mathfrak{B}'b'+\mathfrak{C}'c' = m'$$

Denique designentur numeri

$$pq'-qp', \; pq''-qp'', \; pq'''-qp''', \; p'q''-q'p'', \; p'q'''-q'p''', \; p''q'''-q''p'''$$

resp. per P, Q, R, S, T, U, sitque ipsorum divisor communis maximus positive acceptus $= k$. — Iam ponendo

$$Ap''' + B(pq''' + qp'') + Cqq''' = bb' + \Delta \quad [10]$$

fit ex aequ. 9

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \quad [11]$$

Ex his undecim aequationibus 1...11, sequentes novas evolvimus*):

$$DPP = d'aa \quad [12]$$
$$DP(R-S) = 2d'ab \quad [13]$$
$$DPU = d'ac - (\Delta\Delta - dd'). \quad [14]$$
$$D(R-S)^2 = 4d'bb + 2(\Delta\Delta - dd') \quad [15]$$
$$D(R-S)U = 2d'bc \quad [16]$$
$$DUU = d'cc \quad [17]$$
$$DQQ = da'a' \quad [18]$$
$$DQ(R+S) = 2da'b' \quad [19]$$
$$DQT = da'c' - (\Delta\Delta - dd') \quad [20]$$
$$D(R+S)^2 = 4db'b' + 2(\Delta\Delta - dd') \quad [21]$$
$$D(R+S)T = 2db'c' \quad [22]$$
$$DTT = dc'c' \quad [23]$$

Hinc rursus deducuntur hae duae:

*) Origo harum aequationum haec est: 12 ex 5.5 — 1.2; 13 ex 5.9 — 1.7 — 2.6; 14 ex 10.11 — 6.7; 15 ex 5.8 + 5.8 + 10.10 + 11.11 — 1.4 — 2.3 — 6.7 — 6.7; 16 ex 8.9 — 3.7 — 4.6; 17 ex 8.8 — 3.4. Deductio sex reliquarum eodem modo adornatur, si modo aequationes 2, 5, 7 cum aequationibus 3, 6, 8 resp. commutantur, et reliquae 1, 4, 9..10, 11 eodem loco deinceps retinentur, puta 18 ex 6.6 — 1.3 etc.

$$0 = 2d'aa(\Delta\Delta - dd')$$

$$0 = (\Delta\Delta - dd')^2 - 2d'ac(\Delta\Delta - dd')$$

scilicet prior ex 12.15 — 13.13, posterior ex 14.14 — 12.17; unde facile perspicitur, necessario esse $\Delta\Delta - dd' = 0$, sive sit $a = 0$, sive non sit $= 0$ *). Supponemus itaque, in aequatt. 14, 15, 20, 21 ad dextram deleri $\Delta\Delta - dd'$.

Iam statuendo

$$\mathfrak{A}P + \mathfrak{B}(R-S) + \mathfrak{C}U = m'n'$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R+S) + \mathfrak{C}'T = m'n$$

(ubi n, n' etiam fractiones evadere posse probe notandum, etsi $m'n'$, $m'n$ necessario sint integri): facile ex aequatt. 12...17 deducitur

$$Dmm'n'n' = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'mm$$

similiterque ex aequ. 18...23

$$Dm'm'nn = d(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'm'$$

Erit igitur $d = Dnn$, $d' = Dn'n'$, unde nanciscimur CONCLUSIONEM PRIMAM: *Determinantes formarum F, f, f' necessario inter se habent rationem quadratorum;* et SECUNDAM: *D semper metitur numeros $dm'm'$, $d'mm$.* Patet itaque, D, d, d' eadem signa habere, nullamque formam in productum ff' transformabilem esse posse, cuius determinans maior sit quam divisor communis maximus numerorum $dm'm'$, $d'mm$.

Multiplicentur aequationes 12, 13, 14 resp. per $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$; similiterque per eosdem numeros aequatt. 13, 15, 16, et 14, 16, 17; addantur terna producta, dividaturque summa per Dmn', scripto pro d', $Dn'n'$. Tunc prodit

$$P = an', \quad R - S = 2bn', \quad U = cn'$$

Simili modo multiplicatis aequationibus 18, 19, 20 nec non 19, 21, 22 et 20, 22, 23 resp. per $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, obtinetur

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n$$

*) Haec derivatio aequationis $\Delta\Delta = dd'$ ad institutum praesens sufficit; alioquin analysin elegantiorem sed hic nimis prolixam tradere possemus, directe deducendo ex aequationibus 1...11 hanc $0 = (\Delta\Delta - dd')^2$.

Hinc habetur CONCLUSIO TERTIA: *Numeri a, $2b$, c proportionales sunt numeris P, $R-S$, U, positaque illorum ratione ad hos ut 1 ad n', erit n' radix quadrata ex $\frac{d'}{D}$; similiterque numeri a', $2b'$, c' ad Q, $R+S$, T eandem rationem habent, quae si ponitur esse ut 1 ad n, erit n radix quadrata ex $\frac{d}{D}$.*

Ceterum quantitates n, n' radices vel positivae vel negativae ex $\frac{d}{D}$, $\frac{d'}{D}$ esse possunt, unde distinctionem petimus, quae primo aspectu sterilis videbitur, sed cuius usus in sequentibus sufficienter apparebit. Scilicet dicemus, in transformatione formae F in ff' formam f accipi *directe* quando n' est positiva, *inverse* quando n negativa; similiterque f' accipi directe vel inverse, prout n' positiva vel negativa. Accedente autem conditione ut k sit $= 1$, forma F *vel* ex utraque forma f, f' directe composita, *vel* ex utraque inverse *vel* ex f directe et ex f' inverse, *vel* ex f inverse et ex f' directe dicetur, prout vel n, n' ambae sunt positivae, vel ambae negativae, vel prior positiva posterior negativa, vel prior negativa posterior positiva. Ceterum quisque facile intelliget, has relationes ab ordine quo formae f, f' collocantur (vid. annot. prim. ad art. praes.) non pendere.

Porro observamus, divisorem maximum communem numerorum P, Q, R, S, T, U puta k metiri numeros mn', $m'n$ (uti ex valoribus supra stabilitis manifestum est) adeoque quadratum kk ipsos $mmn'n'$, $m'm'nn$, atque Dkk ipsos $d'mm$, $dm'm'$. Sed et vice versa quivis divisor communis ipsorum mn', $m'n$ metietur ipsum k. Sit enim e talis divisor, qui manifesto etiam numeros an', $2bn'$, cn', $a'n$, $2b'n$, $c'n$ metietur, *i.e.* numeros P, $R-S$, U, Q, $R+S$, T et proin etiam ipsos $2R$ et $2S$. Iam si $\frac{2R}{e}$ esset numerus impar, etiam $\frac{2S}{e}$ impar esse deberet (quoniam summa et differentia sunt pares) adeoque etiam productum impar. Hoc autem productum fit $= \frac{4}{ee}(b'b'nn - bbn'n') = \frac{4}{ee}(d'nn + a'c'nn - dn'n' - acn'n') = \frac{4}{ee}(a'c'nn - acn'n')$ adeoque par, quia e ipsos $a'n$, $c'n$, an', cn' metitur. Quare $\frac{2R}{e}$ necessario erit par, et proin R nec non S per e divisibilis. Quoniam igitur e omnes sex P, Q, R, S, T, U metitur, metietur etiam ipsorum divisorem communem maximum k. Q. E. D. — Hinc concluditur, k esse divisorem communem maximum numerorum mn', $m'n$; unde facile perspicietur, *Dkk fore divisorem communem maximum numerorum $dm'm'$, $d'mm$.* Quae est CONCLUSIO QUARTA. Patet itaque, quoties F ex f et f' composita sit, D fore divisorem communem maximum, numerorum $dm'm'$, $d'mm$, et vice versa; quae proprietas etiam tamquam definitio formae compositae adoptari potuisset. Forma igitur composita e

formis f, f' determinantem maximum possibilem inter omnes formas in productum ff' transformabiles habet.

Antequam ulterius progredi possimus, ante omnia valorem ipsius Δ accuratius definire oportet, quem quidem ostendimus esse $= \sqrt{dd'} = \sqrt{DDnn'n'}$, sed cuius *signum* hinc nondum determinatur. Ad hunc finem ex aequatt. fundamentalibus 1—11 eruimus $DPQ = \Delta aa'$ (quae aequ. obtinetur ex 5.6—1.11), adeoque $Daa'nn' = \Delta aa'$, unde, nisi aliquis numerorum a, a' est $= 0$, fit $\Delta = Dnn'$. Sed prorsus simili modo ex aequatt. fundd. octo aliae deduci possunt, in quibus ad laevam Dnn' ad dextram Δ multiplicati habeantur per $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc' *), unde facile concluditur propterea quod neque omnes $a, 2b, c$, neque omnes $a', 2b', c'$ possunt esse $= 0$, in omnibus casibus fieri $\Delta = Dnn'$, adeoque Δ idem signum habere ut D, d, d' vel oppositum, prout n, n' eadem signa habeant vel diversa.

Porro observamus, numeros aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', $2bb'+2\Delta$, $2bb'-2\Delta$ omnes per mm' divisibiles esse. De novem prioribus hoc per se manifestum est, de duobus reliquis autem simili modo demonstrari potest ut antea ostendimus R et S per e divisibiles esse. Scilicet patet, $4bb'+4\Delta$ et $4bb'-4\Delta$ per mm' divisibiles esse (quoniam $4\Delta = \sqrt{16dd'}$ atque $4d$ per mm, $4d'$ per $m'm'$ divisibilis, adeoque $16dd'$ per $mmm'm'$ et 4Δ per mm') et differentiam quotientium parem; productum ex quotientibus facile demonstratur esse par, unde uterque quotiens par, et $2bb'+2\Delta$, $2bb'-2\Delta$ per mm' divisibiles.

Iam ex undecim aequationibus fundamentalibus facile deducuntur sex sequentes:

$$\begin{aligned}
APP &= aa'q'q' - 2ab'q'q' + ac'qq \\
AQQ &= aa'q''q'' - 2ba'q''q'' + ca'qq \\
ARR &= aa'q'''q''' - 2(bb'+\Delta)qq''' + cc'qq \\
ASS &= ac'q''q'' - 2(bb'-\Delta)q'q'' + ca'q'q' \\
ATT &= ac'q'''q''' - 2bc'q'q''' + cc'q'q' \\
AUU &= ca'q'''q''' - 2cb'q''q''' + cc'q''q''
\end{aligned}$$

Hinc sequitur, omnes APP, AQQ etc. divisibiles esse per mm', unde facile derivatur, quoniam kk divisor communis maximus numerorum PP, QQ, RR etc., etiam Akk per mm' divisibilem esse. Substitutis autem pro $a, 2b, c$, $a', 2b', c'$ valoribus suis $\frac{P}{n'}$ etc. sive $\frac{1}{n'}(pq'-qp')$ etc., transibunt in sex alias aequationes, in quibus ad dextram habebuntur producta ex quantitate $\frac{1}{nn'}(q'q''-qq''')$ in PP, QQ, RR etc. Calculum facillimum lectoribus relinquimus. Hinc sequitur (quoniam omnes PP, QQ etc. esse $= 0$ nequeunt) $Ann' = q'q''-qq'''$.

*) Analysin quam lectores facile detegere poterunt brevitatis caussa supprimere oportet.

Simili modo ex aequationibus fundamentalibus derivantur sex aliae aequationes, a praecedentibus in eo tantummodo discrepantes, quod pro A ubique habetur C et pro q, q', q'', q''' resp. p, p', p'', p''', quas ipsas brevitatis caussa non adscribimus. Hinc eodem modo sequitur, Ckk per mm' divisibilem esse atque $Cnn' = p'p''-pp'''$.

Denique ex eodem fonte petuntur sex aequationes hae:

$$\begin{aligned}
BPP &= -aa'p'q' + ab'(pq'+qp') - ac'pq \\
BQQ &= -aa'p''q'' + ba'(pq''+qp'') - ca'pq \\
BRR &= -aa'p'''q''' + (bb'+\Delta)(pq'''+qp''') - cc'pq \\
BSS &= -ac'p''q'' + (bb'-\Delta)(p'q''+q'p'') - ca'p'q' \\
BTT &= -ac'p'''q''' + bc'(p'q'''+q'p''') - cc'p'q' \\
BUU &= -ca'p'''q''' + cb'(p''q'''+q''p''') - cc'p''q''
\end{aligned}$$

unde perinde ut ante concluditur, $2Bkk$ divisibilem esse per mm' atque $2Bnn' = pq'''+qp'''-p'q''-q'p''$.

Quoniam itaque Akk, $2Bkk$, Ckk per mm' sunt divisibiles, facile perspicietur, etiam Mkk per mm' divisibilem esse debere. Ex aequationibus fundamentalibus autem colligitur, M metiri ipsos aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', adeoque etiam ipsos am', $2bm'$, cm' (qui sunt divisores comm. max. trium primorum mediorum et ultimorum resp.); denique etiam ipsum mm' qui est horum div. comm. max. Hinc patet, in eo casu ubi forma F ex formis f, f' composita est sive $k = 1$, necessario esse $M = mm'$. Quae est CONCLUSIO QUINTA.

Si div. comm. max. numerorum A, B, C est $\mathfrak{M}$, hic erit vel $= M$ (quando forma F est proprie primitiva vel ex proprie primitiva derivata) vel $= \frac{1}{2}M$ (quando F est forma improprie primitiva vel ex improprie prim. derivata); similiter designando divisores comm. max. numerorum a, b, c; a', b', c' resp. per $\mathfrak{m}$, $\mathfrak{m}'$ erit $\mathfrak{m}$ vel $= m$ vel $= \frac{1}{2}m$, et $\mathfrak{m}'$ vel $= m'$ vel $= \frac{1}{2}m'$. Iam patet, $\mathfrak{m}\mathfrak{m}$ metiri ipsum d', $\mathfrak{m}'\mathfrak{m}'$ ipsum d', adeoque $\mathfrak{m}\mathfrak{m}\mathfrak{m}'\mathfrak{m}'$ ipsum dd' sive $\Delta\Delta$, et $\mathfrak{m}\mathfrak{m}'$ ipsum Δ.

Hinc ex sex ultimis aequationibus pro BPP etc. sequitur, $\mathfrak{m}\mathfrak{m}'$ metiri ipsum Bkk, adeoque (quum etiam ipsos Akk, Ckk metiatur) etiam ipsum $\mathfrak{M}kk$. Quoties igitur F ex f, f' composita est, metietur $\mathfrak{m}\mathfrak{m}'$ ipsum $\mathfrak{M}$. Quando itaque in hoc casu utraque f, f' est proprie primitiva vel ex proprie primitiva derivata sive $\mathfrak{m}\mathfrak{m}' = mm' = M$, erit $\mathfrak{M} = M$, sive F similis forma. Quando vero, in eadem suppositione, aut utraque f, f' aut alterutra saltem est improprie primitiva vel ex improprie primitiva derivata, *e. g.* forma f; ex aequationibus fundamentalibus sequitur, aa', $2ab'$, ac', ba', $2bb'$, bc', ca', $2cb'$, cc' per $\mathfrak{M}$ divisibiles esse adeoque etiam am', bm', cm' et hinc quoque $\mathfrak{m}m' = \frac{1}{2}mm' = \frac{1}{2}M$; unde necessario in hoc casu erit $\mathfrak{M} = \frac{1}{2}M$, sive etiam forma F vel impr. prim. vel ex impr. prim. derivata. Quae efficiunt CONCLUSIONEM SEXTAM.

Tandem observamus, si novem aequationes

$$an' = P, \quad 2bn' = R - S, \quad cn' = U$$
$$a'n = Q, \quad 2b'n = R + S, \quad c'n = T$$
$$Ann' = q'q'' - qq''', \quad 2Bnn' = pq''' + qp''' - p'q'' - q'p'', \quad Cnn' = p'p'' - pp'''$$

quas, quoniam in sequentibus saepius ad ipsas revenire oportebit, per Ω designabimus) locum habere *supponantur*, spectatis adeo ipsis n, n' tamquam incognitis, quarum tamen neutra $= 0$: per substitutionem facile confirmari, etiam aequationes fundamentales $1 \ldots 9$ necessario veras esse sive formam (A, B, C) per substitutionem p, p', p'', p'''; q, q', q'', q''' in productum e formis $(a, b, c)(a', b', c')$ transire; praetereaque esse

$$bb - ac = nn(BB - AC), \quad b'b' - a'c' = n'n'(BB - AC)$$

Calculum quem hic apponere nimis prolixum foret lectorum industriae committimus.

236.

PROBLEMA. *Propositis duabus formis quarum determinantes aut aequales sunt aut saltem rationem quadratorum inter se habent: invenire formam ex illis compositam.*

Sol. Sint formae componendae $(a, b, c) \ldots f$, $(a', b', c') \ldots f'$; harum determinantes d, d'; divisores communes maximi numerorum a, $2b$, c; a', $2b'$, c' resp. m, m'; divisor comm. maximus numerorum $dm'm'$, $d'mm$ eodem signo ut d, d'

affectus D. Tunc $\frac{dm'm'}{D}$, $\frac{d'mm}{D}$ erunt numeri positivi inter se primi ipsorumque productum, quadratum; quare ipsi erunt quadrata (art. 21). Hinc $\sqrt{\frac{d}{D}} : \sqrt{\frac{d'}{D}}$ erunt quantitates rationales quas ponemus $= n$, n', et quidem accipiemus pro n valorem positivum vel negativum, prout forma f in compositionem vel directe vel inverse ingredi debet, similiterque signum ipsius n' ex ratione qua f'' in compositionem ingredi debet, determinabimus. Erunt itaque mn', $m'n$ numeri integri inter se primi; n et n' autem etiam fractiones esse possunt. His ita factis, observamus, an', cn', $a'n$, $c'n$, $bn' + b'n$, $bn' - b'n$ esse integros, quod de quatuor prioribus per se manifestum est (quum $an' = \frac{a}{m}mn'$ etc.); de duobus reliquis eodem modo probatur ut in art. praec. demonstratum fuit, R et S per e divisibiles esse.

Iam accipiantur quatuor numeri integri $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$ ad libitum, ea sola conditione, ut quatuor quantitates in aequatione sequente (I) ad laevam positae non omnes simul $= 0$ fiant, ponaturque

$$\begin{aligned} \mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}'''(bn' + b'n) &= \mu q \quad \ldots\ldots \text{(I)} \\ -\mathfrak{Q}an' + \mathfrak{Q}''c'n - \mathfrak{Q}''(bn' - b'n) &= \mu q' \\ \mathfrak{Q}'''cn' - \mathfrak{Q}a'n + \mathfrak{Q}'(bn' - b'n) &= \mu q'' \\ -\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q}(bn' + b'n) &= \mu q''' \end{aligned}$$

ita ut q, q', q'', q''' fiant integri divisorem communem non habentes, quod obtinetur accipiendo pro μ divisorem communem maximum quatuor numerorum, qui in his aequationibus sunt ad laevam. Tunc igitur per art. 40 inveniri poterunt quatuor numeri integri $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ tales ut fiat

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

Quo facto determinentur numeri p, p', p'', p''' per aequationes sequentes:

$$\begin{aligned} \mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}'''(bn' + b'n) &= p \quad \ldots\ldots \text{(II)} \\ -\mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}''(bn' - b'n) &= p' \\ \mathfrak{P}'''cn' - \mathfrak{P}a'n + \mathfrak{P}'(bn' - b'n) &= p'' \\ -\mathfrak{P}''cn' - \mathfrak{P}'c'n - \mathfrak{P}(bn' + b'n) &= p''' \end{aligned}$$

Tandem ponatur

$$q'q'' - qq''' = Ann', \quad pq''' + qp''' - p'q'' - q'p'' = 2Bnn', \quad p'p'' - pp''' = Cnn'$$

Tunc A, B, C erunt numeri integri formaque $(A, B, C) \ldots F$ ex formis f, f' composita.

Dem. I. Ex aequatt. I nullo negotio confirmantur sequentes quatuor aequationes:

$$\begin{aligned} 0 &= q'cn' - q''c'n - q'''(bn' - b'n) \quad \ldots\ldots\ldots \text{(III)} \\ 0 &= qcn' + q'''an' - q''(bn' + b'n) \\ 0 &= q''an' + qc'n - q'(bn' + b'n) \\ 0 &= q''an' - q'an - q(bn' - b'n) \end{aligned}$$

II. Iam ponamus, numeros integros $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \mathfrak{N}, \mathfrak{N}'$ ita determinatos esse ut fiat

$$\begin{aligned} \mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m \\ \mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' &= m' \\ \mathfrak{N}m'n + \mathfrak{N}'mn' &= 1 \end{aligned}$$

Tunc erit

$$\mathfrak{A}a\mathfrak{N}n' + 2\mathfrak{B}b\mathfrak{N}n' + \mathfrak{C}c\mathfrak{N}n' + \mathfrak{A}a'\mathfrak{N}n + 2\mathfrak{B}b'\mathfrak{N}n + \mathfrak{C}c'\mathfrak{N}n = 1$$

Hinc atque ex aequatt. (III) facile confirmatur, si statuatur

$$\begin{aligned} -q'\mathfrak{A}\mathfrak{N} - q''\mathfrak{A}\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N} + \mathfrak{B}\mathfrak{N}) &= \mathfrak{q} \\ q\mathfrak{A}\mathfrak{N} - q'''\mathfrak{C}\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N} - \mathfrak{B}\mathfrak{N}) &= \mathfrak{q}' \\ -q'''\mathfrak{C}\mathfrak{N} + q\mathfrak{A}\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N} - \mathfrak{B}\mathfrak{N}) &= \mathfrak{q}'' \\ q''\mathfrak{C}\mathfrak{N} + q'\mathfrak{C}\mathfrak{N} + q(\mathfrak{B}\mathfrak{N} + \mathfrak{B}\mathfrak{N}) &= \mathfrak{q}''' \end{aligned}$$

fore

$$\begin{aligned} \mathfrak{q}an' + \mathfrak{q}''a'n + \mathfrak{q}'''(bn' + b'n) &= q \quad \ldots\ldots \text{(IV)} \\ -\mathfrak{q}an' + \mathfrak{q}''c'n - \mathfrak{q}''(bn' - b'n) &= q' \\ \mathfrak{q}'''cn' - \mathfrak{q}a'n + \mathfrak{q}'(bn' - b'n) &= q'' \\ -\mathfrak{q}''cn' - \mathfrak{q}'c'n - \mathfrak{q}(bn' + b'n) &= q''' \end{aligned}$$

Quoties $\mu = 1$, hae aequationes non sunt necessariae, sed ipsarum loco aequationes (I), quibus omnino analogae sunt, retineri possunt. Quodsi nunc ex aequatt. II, IV valores ipsorum Ann', $2Bnn'$, Cnn' (*i. e.* numerorum $qq'' - qq'''$ etc.) evolvuntur, et quae mutuo se destruunt delentur: invenietur, singulorum

partes esse vel producta ex integris in nn', vel ex integris in $dn'n'$ vel ex integris in $d'nn$, insuperque omnes partes constituentes ipsius $2Bnn'$ implicare factorem 2. Hinc concluditur (quoniam $dn'n' = d'nn$, et proin $\frac{dn'n'}{nn'} = \frac{d'nn}{nn'} = \sqrt{dd'}$ sunt integri), A, B, C esse numeros integros. *Q. E. P.*

III. Substituendo ex aequatt. (II) valores ipsorum p, p', p'', p''', facile comprobatur adiumento aequatt. (III) et huius

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

esse

$$\begin{aligned} pq' - qp' &= an', \quad pq''' - qp''' - p'q'' + q'p'' = 2bn', \quad p''q''' - q''p''' = cn' \\ pq'' - qp'' &= a'n, \quad pq''' - qp''' + p'q'' - q'p'' = 2b'n, \quad p'q''' - q'p''' = c'n \end{aligned}$$

quae aequationes identicae sunt cum sex prioribus (Ω) art. praec.; tres reliquae autem iam per hyp. locum habent. Quare (*ibid. sub fin.*) forma F transibit in ff' per substitutionem p, p', p'', p'''; q, q', q'', q'''; ipsiusque determinans erit $= D$, sive aequalis divis. comm. max. numerorum $dm'm'$, $d'mm$, quamobrem per concl. quartam art. praec. F ex f, f' composita erit. *Q. E. S.* Denique facile perspicietur, F ex f, f' *ita* compositam esse ut praescriptum sit, quum signa quantitatum n, n' iam ab initio rite sint determinata.

237.

THEOREMA. *Si forma F in productum e duabus formis f, f' est transformabilis, atque forma f'' formam f''' implicat: F etiam in productum e formis f, f''' transformabilis erit.*

Dem. Retineantur pro formis F, f, f' omnia signa art. 235; forma f'' sit $= (a'', b'', c'')$, transeatque f' in f''' per substitutionem $\alpha, \beta, \gamma, \delta$. Tunc nullo negotio perspicietur, F transire in ff''' per substitutionem

$$\begin{aligned} &\alpha p + \gamma p', \quad \beta p + \delta p', \quad \alpha p'' + \gamma p''', \quad \beta p'' + \delta p''' \\ &\alpha q + \gamma q', \quad \beta q + \delta q', \quad \alpha q'' + \gamma q''', \quad \beta q'' + \delta q''' \quad \textit{Q. E. D.} \end{aligned}$$

Positis brevitatis caussa coefficientibus

$$\alpha p + \gamma p', \ \beta p + \delta p' \text{ etc.} = \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''; \quad \Omega, \Omega', \Omega'', \Omega'''$$

numeroque $\alpha\delta - \beta\gamma = e$: ex aequatt. Ω art. 235 facile confirmatur, esse

$$\begin{aligned}
\mathfrak{P}\Omega' - \Omega\mathfrak{P}' &= a'e \\
\mathfrak{P}\Omega''' - \Omega\mathfrak{P}''' - \mathfrak{P}'\Omega'' + \Omega'\mathfrak{P}'' &= 2b'e \\
\mathfrak{P}''\Omega''' - \Omega''\mathfrak{P}''' &= c'e \\
\mathfrak{P}\Omega'' - \Omega\mathfrak{P}'' = \alpha\alpha a'n + 2\alpha\gamma b'n + \gamma\gamma c'n &= a''n \\
\mathfrak{P}\Omega''' - \Omega\mathfrak{P}''' + \mathfrak{P}'\Omega'' - \Omega'\mathfrak{P}'' &= 2b''n \\
\mathfrak{P}'\Omega''' - \Omega'\mathfrak{P}''' &= c''n \\
\Omega'\Omega'' - \Omega\Omega''' &= A'n'e \\
\mathfrak{P}\Omega''' + \Omega\mathfrak{P}''' - \mathfrak{P}'\Omega'' - \Omega'\mathfrak{P}' &= 2B'n'e \\
\mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= C'n'e
\end{aligned}$$

Iam designato determinante formae f'' per d'', erit e radix quadrata ex $\frac{d''}{d'}$, et quidem positiva vel negativa, prout forma f' formam f'' vel proprie vel improprie implicat. Quare $n'e$ erit radix quadrata ex $\frac{d''}{D}$; unde patet, novem aequationes praecedentes aequationibus Ω art. 235 prorsus analogas esse, formamque f in transformatione formae F in ff'' eodem modo accipi, ut in transformatione formae F in ff'; formam f'' vero in illa vel eodem modo ut f' in hac, vel opposito, prout f' ipsam f'' proprie implicet vel improprie.

238.

Theorema. *Si forma F sub forma F' est contenta atque in productum e formis f, f' transformabilis: etiam forma F' in idem productum transformabilis erit.*

Dem. Retentis pro formis F, f, f' iisdem signis ut supra et supponendo formam F' transire in F per substitutionem $\alpha, \beta, \gamma, \delta$, facile perspicietur, F' per substitutionem

$$\begin{array}{cccc} \alpha p + \beta q, & \alpha p' + \beta q', & \alpha p'' + \beta q'', & \alpha p''' + \beta q''' \\ \gamma p + \delta q, & \gamma p' + \delta q', & \gamma p'' + \delta q'', & \gamma p''' + \delta q''' \end{array}$$

idem fieri quod F per substitutionem p, p', p'', p'''; q, q', q'', q''', adeoque F' per substitutionem illam transire in ff'. *Q. E. D.*

Praeterea per similem calculum ut in art. praec. facile confirmatur, F' eodem modo in ff' transformabilem fore ut F, quando F' ipsam F proprie implicet; quando vero F improprie sub F' contenta sit, transformationes formae F in ff' et formae F' in ff' oppositas fore respectu utriusque formae f, f', scilicet

quae ex his formis in alteram transformationem directe ingrediatur, in altera accipi inverse.

Ex combinatione theorematis praesentis cum theor. art. praec. obtinemus sequens generalius: *Si forma F in productum ff' est transformabilis, atque formae f, f' resp. implicant formas g, g', forma F vero sub forma G contenta est: G in productum gg' transformabilis erit.* Nam per theor. art. praes. G transformabilis erit in ff', hinc per theor. art. praec. in fg' et per idem theor. etiam in gg'. Porro patet, si omnes tres formae f, f', G formas g, g', F proprie implicent, G eodem modo in gg' transformabilem fore respectu formarum g, g', ut F in ff' respectu formarum f, f'; idem evenire, si illae tres implicationes omnes sint impropriae; denique aeque facile determinari poterit, *quomodo* G in gg' transformabilis sit, si ex illis implicationibus aliqua duabus reliquis sit dissimilis.

Si formae F, f, f' formis G, g, g' resp. sunt aequivalentes, hae eosdem determinantes habebunt ut illae, et quod pro formis f, f' sunt numeri m, m', idem erunt pro formis g, g' (art. 161). Hinc nullo negotio per conclus. quartam art. 235 deducitur, in hocce casu G ex g, g' *compositam* fore, si F ex f, f' composita sit, et quidem formam g in compositionem illam eodem modo ingredi, ut f in hanc, quando F ipsi G eodem modo aequivaleat, ut f ipsi g, et contra; similiterque g' in compositione priori vel eodem modo vel opposito accipiendam ut f' in posteriori, prout aequivalentia formarum f', g' aequivalentiae formarum F, G similis sit vel dissimilis.

239.

Theorema. *Si forma F ex formis f, f' composita est: quaevis alia forma in productum ff' eodem modo transformabilis ut F, ipsam F proprie implicabit.*

Dem. Retentis pro F, f, f' omnibus signis art. 235, aequationes Ω etiam hic locum habebunt. Ponamus formam $F' = (A', B', C')$, cuius determinans $= D'$, transire in productum ff' per substitutionem $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \mathfrak{p}'''$; $\mathfrak{q}, \mathfrak{q}', \mathfrak{q}'', \mathfrak{q}'''$ designemusque numeros

$$\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}', \quad \mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'', \quad \mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''', \quad \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'', \quad \mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}''', \quad \mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''$$

resp. per

$$P', Q', R', S', T', U'$$

Tunc habebuntur novem aequationes ipsis Ω omnino similes puta

$$P' = a\mathfrak{n}', \quad R - S' = 2b\mathfrak{n}', \quad U' = c\mathfrak{n}'$$
$$Q' = a'\mathfrak{n}, \quad R + S' = 2b'\mathfrak{n}, \quad T' = c'\mathfrak{n}$$
$$\mathfrak{q}\mathfrak{q}'' - \mathfrak{q}\mathfrak{q}''' = A'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}'$$

quas per Ω' designabimus. Quantitates $\mathfrak{n}$, $\mathfrak{n}'$ hic erunt radices quadratae ex $\frac{d}{D'}$, $\frac{d'}{D'}$ et quidem iisdem signis resp. affectae ut n, n'; si igitur radix quadrata ex $\frac{D}{D'}$ positive accepta (quae erit numerus integer) statuitur $= k$, erit $\mathfrak{n} = ku$, $\mathfrak{n}' = ku'$. Hinc et ex aequatt. senis prioribus in Ω et Ω' manifestum est, fore

$$P' = kP, \quad Q' = kQ, \quad R' = kR$$
$$S' = kS, \quad T' = kT, \quad U' = kU$$

Quare per lemma art. 234 determinari poterunt quatuor numeri integri $\alpha, \beta, \gamma, \delta$ tales ut fiat

$$\alpha p + \beta q = \mathfrak{p}, \quad \gamma p + \delta q = \mathfrak{q}$$
$$\alpha p' + \beta q' = \mathfrak{p}', \quad \gamma p' + \delta q' = \mathfrak{q}' \text{ etc.}$$

atque

$$\alpha\delta - \beta\gamma = k$$

Substitutis his valoribus ipsorum $\mathfrak{p}, \mathfrak{q}, \mathfrak{p}', \mathfrak{q}'$ etc. in aequatt. tribus ultimis Ω', facile confirmatur adiumento aequationum $\mathfrak{n} = k\mathfrak{n}$, $\mathfrak{n}' = k\mathfrak{n}'$ triumque ultimarum Ω, fore

$$A'\alpha\alpha + 2B'\alpha\gamma + C'\gamma\gamma = A$$
$$A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B$$
$$A'\beta\beta + 2B'\beta\delta + C'\delta\delta = C$$

quapropter forma F' per substitutionem $\alpha, \beta, \gamma, \delta$ (quae propria erit, quoniam $\alpha\delta - \beta\gamma = k$ est positivus) transibit in F, *i. e.* formam F proprie implicabit. *Q. E. D.*

Si itaque F' e formis f, f' etiam composita est (eodem modo ut F ex iisdem), formae F, F' eundem determinantem habebunt, eruntque adeo proprie aequivalentes. Generalius, si forma G e formis g, g' eodem modo composita est ut

F ex f, f' resp., formaeque g, g' ipsis f, f' proprie aequivalent: formae F, G proprie aequivalebunt.

Quum is casus ubi ambae formae componendae compositionem directe ingrediuntur, simplicissimus sit, ad ipsumque reliqui facile reducantur, illum solum in sequentibus contemplabimur, ita ut si forma aliqua simpliciter dicatur e duabus aliis composita, semper subintelligere oporteat, ex utraque illam proprie esse compositam*). Eadem restrictio valebit, quoties forma in productum e duabus aliis transformabilis dicetur.

240.

THEOREMA. *Si e formis f, f' composita est forma F; ex F et f'' forma $\mathfrak{F}$; ex f, f'' forma F'; ex F' et f' forma $\mathfrak{F}'$: formae $\mathfrak{F}, \mathfrak{F}'$ proprie aequivalentes erunt.*

Dem. I. Sit

$$f = axx + 2bxy + cyy$$
$$f' = a'x'x' + 2b'x'y' + c'y'y'$$
$$f'' = a''x''x'' + 2b''x''y'' + c''y''y''$$
$$F = AXX + 2BXY + CYY$$
$$F' = A'X'X' + 2B'X'Y' + C'Y'Y'$$
$$\mathfrak{F} = \mathfrak{A}\mathfrak{X}\mathfrak{X} + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}\mathfrak{Y}$$
$$\mathfrak{F}' = \mathfrak{A}'\mathfrak{X}'\mathfrak{X}' + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'\mathfrak{Y}'$$

determinantes harum septem formarum resp. $d, d', d'', D, D', \mathfrak{D}, \mathfrak{D}'$, qui omnes eadem signa et rationem quadratorum inter se habebunt. Porro sit m divisor communis maximus numerorum $a, 2b, c$, similemque significationem habeant m', m'', M relative ad formas f', f'', F. Tum ex concl. 4 art. 235, D erit div. comm. max. numerorum $dm'm'$, $d'mm$ adeoque $Dm''m''$ div. comm. max. numerorum $dm'm'm''m''$, $d'mmm''m''$; $M = mm'$; $\mathfrak{D}$ div. comm. max. num. $Dm''m''$, $d''MM$, sive numerorum $Dm''m''$, $d''mmm'm'$. Hinc concluditur, $\mathfrak{D}$ esse div. comm. max. trium numerorum $dm'm'm''m''$, $d'mmm''m''$, $d''mmm'm'$; ex simili autem ratione $\mathfrak{D}'$ eorundem trium numerorum divisor communis maximus erit; quare quum $\mathfrak{D}, \mathfrak{D}'$ eadem signa habeant, erit $\mathfrak{D} = \mathfrak{D}'$, sive formae $\mathfrak{F}, \mathfrak{F}'$ eundem determinantem habebunt.

*) Similiter ut in compositione rationum (quae cum compositione formarum magnam analogiam habet) subintelligi solet, rationes componendas directe accipiendas esse nisi ubi contrarium monetur.

II. Iam transeat F in ff' per substitutionem

$$X = px'+p'y'+p''yx'+p'''yy'$$
$$Y = qx'+q'y'+q''yx'+q'''yy'$$

atque $\mathfrak{F}$ in Ff'' per substitutionem

$$\mathfrak{X} = \mathfrak{p}X''+\mathfrak{p}'Y''+\mathfrak{p}''YX''+\mathfrak{p}'''YY''$$
$$\mathfrak{Y} = \mathfrak{q}X''+\mathfrak{q}'Y''+\mathfrak{q}''YX''+\mathfrak{q}'''YY''$$

designenturque radices quadratae positivae ex $\frac{d}{D}, \frac{d'}{D}, \frac{D}{\mathfrak{D}}, \frac{d''}{\mathfrak{D}}$ per $n, n', \mathfrak{N}, \mathfrak{n}''$. Tunc per art. 235 habebuntur decem et octo aequationes, quarum semissis altera ad transformationem formae F in ff' pertinebit, altera ad transformationem formae $\mathfrak{F}$ in Ff''. Prima erit $pq'-qp' = an'$, ad cuius instar facile formari poterunt reliquae brevitatis gratia hic omittendae. Ceterum quantitates $n, n', \mathfrak{N}, \mathfrak{n}''$ rationales quidem erunt, sed non necessario numeri integri.

III. Si valores ipsorum X, Y in valoribus ipsorum $\mathfrak{X}$, $\mathfrak{Y}$ substituuntur prodit substitutio talis:

$$\begin{aligned}\mathfrak{X} = {} & (1)xx'x''+(2)xx'y''+(3)xy'x''+(4)xy'y'' \\ & +(5)yx'x''+(6)yx'y''+(7)yy'x''+(8)yy'y'' \\ \mathfrak{Y} = {} & (9)xx'x''+(10)xx'y''+(11)xy'x''+(12)xy'y'' \\ & +(13)yx'x''+(14)yx'y''+(15)yy'x''+(16)yy'y''\end{aligned}$$

per quam manifesto $\mathfrak{F}$ transibit in productum $ff'f''$. Coefficiens (1) erit $= p\mathfrak{p}+q\mathfrak{p}''$; valores quindecim reliquorum non apponimus, quippe quos quisque nullo negotio evolvet. Designemus numerum $(1)(10)-(2)(9)$ per $(1,2)$, numerum $(1)(11)-(3)(9)$ per $(1,3)$, et generaliter $(g)(8+h)-(h)(8+g)$ per (g,h), supponendo g, h esse integros inaequales inter 1 et 16, quorum maior h *); hoc modo omnino viginti et octo signa habebuntur. Iam denotatis radicibus quadratis positivis ex $\frac{d}{\mathfrak{D}}, \frac{d'}{\mathfrak{D}}$ per $\mathfrak{n}, \mathfrak{n}'$, (quae erunt $= n\mathfrak{N}, n'\mathfrak{N}$), eruentur sequentes 28 aequationes:

*) Horum signorum significatio praesens non est confundenda cum ea, in qua in art. 234 accepta erant; nam numeri per haec signa *hic* expressi apprime respondent iis, qui in art. 234 per numeros similibus signis *illic* denotatos multiplicabantur.

$(1,2) = aa'\mathfrak{n}''$	$(3,5) = a''b'\mathfrak{n}-a''b\mathfrak{n}'$
$(1,3) = aa''\mathfrak{n}'$	$(3,6) = bb'\mathfrak{n}''+b'b''\mathfrak{n}-bb''\mathfrak{n}'-\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$
$(1,4) = ab'\mathfrak{n}''+ab''\mathfrak{n}'$	$(3,7) = a''c\mathfrak{n}$
$(1,5) = a'a''\mathfrak{n}$	$(3,8) = bc\mathfrak{n}''+b''c\mathfrak{n}$
$(1,6) = a'b\mathfrak{n}''+ab''\mathfrak{n}$	$(4,5) = b'b''\mathfrak{n}-bb'\mathfrak{n}''-bb''\mathfrak{n}'+\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$
$(1,7) = a''b\mathfrak{n}'+a'b''\mathfrak{n}$	$(4,6) = b'c''\mathfrak{n}-bc''\mathfrak{n}'$
$(1,8) = bb'\mathfrak{n}''+bb''\mathfrak{n}'+b'b''\mathfrak{n}+\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$	$(4,7) = b''c\mathfrak{n}-bc'\mathfrak{n}''$
$(2,3) = ab''\mathfrak{n}'-ab'\mathfrak{n}''$	$(4,8) = cc''\mathfrak{n}$
$(2,4) = ac''\mathfrak{n}'$	$(5,6) = ca'\mathfrak{n}''$
$(2,5) = a'b''\mathfrak{n}-a'b\mathfrak{n}''$	$(5,7) = ca''\mathfrak{n}'$
$(2,6) = a'c''\mathfrak{n}$	$(5,8) = b'c\mathfrak{n}''+b''c\mathfrak{n}'$
$(2,7) = bb''\mathfrak{n}'+b'b''\mathfrak{n}-bb'\mathfrak{n}''-\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$	$(6,7) = b''c\mathfrak{n}'-b'c\mathfrak{n}''$
$(2,8) = bc''\mathfrak{n}'+b'c''\mathfrak{n}$	$(6,8) = cc''\mathfrak{n}'$
$(3,4) = ac'\mathfrak{n}''$	$(7,8) = cc'\mathfrak{n}''$

quas per Φ designabimus, novemque aliae:

$$\begin{aligned}(10)(11)-(9)(12) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\ (1)(12)-(2)(11)-(3)(10)+(4)(9) &= 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\ (2)(3)-(1)(4) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\ -(9)(16)+(10)(15)+(11)(14)-(12)(13) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\ (1)(16)-(2)(15)-(3)(14)+(4)(13) & \\ +(5)(12)-(6)(11)-(7)(10)+(8)(9) &= 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\ -(1)(8)+(2)(7)+(3)(6)-(4)(5) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\ (14)(15)-(13)(16) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\ (5)(16)-(6)(15)-(7)(14)+(8)(13) &= 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\ (6)(7)-(5)(8) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}\end{aligned}$$

quas designabimus per Ψ *).

IV. Originem omnium harum 37 aequationum deducere nimis prolixum foret: sufficiet quasdam confirmavisse, ad quarum instar reliquae haud difficulter demonstrari poterunt.

*) Observare convenit, 18 alias aequationes his Ψ similes erui posse, in quibus ad dextram loco factorum $a, 2b, c$ habeantur $a', 2b', c'$; $a'', 2b'', c''$: sed has quum ad institutum nostrum non sint necessariae, omittimus.

1) Habetur

$$\begin{aligned}(1,2) &= (1)(10)-(2)(9)\\ &= (\mathfrak{p}\mathfrak{q}'-\mathfrak{q}\mathfrak{p}')pp+(\mathfrak{p}\mathfrak{q}'''-\mathfrak{q}\mathfrak{p}'''-\mathfrak{p}'\mathfrak{q}''+\mathfrak{q}'\mathfrak{p}'')pq+(\mathfrak{p}''\mathfrak{q}'''-\mathfrak{q}''\mathfrak{p}''')qq\\ &= \mathfrak{n}''(App+2Bpq+Cqq) = \mathfrak{n}''aa'\end{aligned}$$

quae est aequ. prima.

2) Fit

$$(1,3) = (1)(11)-(3)(9) = (\mathfrak{p}\mathfrak{q}''-\mathfrak{q}\mathfrak{p}'')(pq'-qp') = a''\mathfrak{R}a\mathfrak{n}' = aa''\mathfrak{n}'$$

aequ. secunda.

3) Erit

$$\begin{aligned}(1,8) &= (1)(16)-(8)(9)\\ &= (\mathfrak{p}\mathfrak{q}'-\mathfrak{q}\mathfrak{p}')pp'''+(\mathfrak{p}\mathfrak{q}'''-\mathfrak{q}\mathfrak{p}''')pq'''-(\mathfrak{p}'\mathfrak{q}''-\mathfrak{q}'\mathfrak{p}'')qp'''+(\mathfrak{p}''\mathfrak{q}'''-\mathfrak{q}''\mathfrak{p}''')qq'''\\ &= \mathfrak{n}''(App'''+B(pq'''+qp''')+Cqq''')+b''\mathfrak{R}(pq'''-qp''')\\ &= \mathfrak{n}''(bb'+\sqrt{dd'})+b''\mathfrak{R}(b'n+bn')\text{ *)}\\ &= \mathfrak{n}''bb'+\mathfrak{n}'bb''+\mathfrak{n}b'b''+\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''\end{aligned}$$

aequatio octava in Φ. Aequationes reliquas lectoribus confirmandas linquimus.

V. Ex aequatt. Φ sequitur, viginti octo numeros $(1,2)$, $(1,3)$ etc. nullum divisorem communem habere, sequenti modo. Primo observamus, viginti septem producta e ternis factoribus, quorum primus vel $\mathfrak{n}$, secundus aliquis numerorum a', $2b'$, c', tertiusque aliquis numerorum a'', $2b''$, c''; vel primus $\mathfrak{n}'$, secundus aliquis e numeris a, $2b$, c, tertius aliquis numerorum a'', $2b''$, c''; vel denique primus $\mathfrak{n}''$, secundus aliquis numerorum a, $2b$, c tertiusque aliquis e numeris a', $2b'$, c' — singula haec viginti septem producta propter aequatt. Φ aequalia esse vel alicui ex viginti octo numeris $(1,2)$, $(1,3)$ etc. vel plurium summae aut differentiae (*e.g.* $\mathfrak{n}a'a''=(1,5)$, $2\mathfrak{n}a'b''=(1,6)+(2,5)$, $4\mathfrak{n}b'b''=(1,8)+(2,7)+(3,6)+(4,5)$, et sic de reliquis); quamobrem si hi numeri divisorem communem habent, hic necessario etiam omnia illa producta metiri deberet. Hinc vero facile deducitur adiumento art. 40 et per methodum saepius in praecedentibus adhibitam, eundem divisorem etiam numeros $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$ metiri debere, adeoque horum

*) Hoc sequitur ex aequ. 10 art. 235 et sqq. Quantitas radicalis $\sqrt{dd'}$ fit $= Dnn' = \mathfrak{D}nn'\mathfrak{R}\mathfrak{R} = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

quadrata quae sunt $\frac{dm'm''m'''}{\mathfrak{D}}$, $\frac{d'mm''m'''}{\mathfrak{D}}$, $\frac{d''mm'm'}{\mathfrak{D}}$ per illius quadratum divisibilia esse, *Q. E. A.*, quoniam per I trium numeratorum divisor communis maximus est $\mathfrak{D}$, adeoque quadrata ipsa divisorem communem habere nequeunt.

VI. Haec omnia pertinent ad transformationem formae $\mathfrak{F}$ in $ff'f'''$; et ex transformationibus formae F in ff' formaeque $\mathfrak{F}$ in Ff''' deducta sunt. Sed prorsus simili modo e transformationibus formae F' in ff''' formaeque $\mathfrak{F}'$ in $F'f''$ derivabitur transformatio formae $\mathfrak{F}'$ in $ff'f'''$ talis:

$$\begin{aligned}\mathfrak{X}' &= (1)'x'x''+(2)'x'y''+(3)'y'x''+\text{ etc.}\\ \mathfrak{Y}' &= (9)'x'x''+(10)'x'y''+(11)'y'x''+\text{ etc.}\end{aligned}$$

(designando omnes coefficientes similiter ut in transformatione formae $\mathfrak{F}$ in $ff'f''$, singulisque distinctionis caussa lineolam affigendo), ex qua perinde ut ante 28 aequationes ipsis Φ analogae deducentur, quas per Φ' designabimus, novemque aliae ipsis Ψ analogae, quas exprimemus per Ψ'. Scilicet denotando

$$(1)'(10)'-(2)'(9)' \text{ per } (1,2)', \quad (1)'(11)'-(3)'(9)' \text{ per } (1,3)'$$

aequationes Φ' erunt

$$(1,2)' = aa'\mathfrak{n}'', \quad (1,3)' = aa''\mathfrak{n}', \text{ etc.}$$

aequationes Ψ' autem

$$(10)'(11)'-(9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{R}', \text{ etc.}$$

(Evolutionem uberiorem brevitatis gratia lectoribus relinquimus; ceterum periti novum calculum ne necessarium quidem esse, sed analysin primam per analogiam facile huc transferri posse invenient). Quibus ita factis, ex Φ et Φ' statim sequitur

$$(1,2) = (1,2)', \quad (1,3) = (1,3)', \quad (1,4) = (1,4)', \quad (2,3) = (2,3)', \text{ etc.}$$

hinc vero et inde quod omnes $(1,2)$, $(1,3)$, $(2,3)$ etc. divisorem communem (per V) non habent, adiumento lemmatis art. 234 concluditur, quatuor numeros integros α, $\vec{\alpha}$, γ, δ ita determinari posse, ut fiat

$$\begin{aligned}&\alpha(1)'+\vec{\alpha}(9)' = (1), \quad \alpha(2)'+\vec{\alpha}(10)' = (2), \quad \alpha(3)'+\vec{\alpha}(11)' = (3), \text{ etc.}\\ &\gamma(1)'+\delta(9)' = (9), \quad \gamma(2)'+\delta(10)' = (10), \quad \gamma(3)'+\delta(11)' = (11), \text{ etc.}\end{aligned}$$

atque $\alpha\delta-\vec{\alpha}\gamma = 1$.

VII. Hinc atque substituendo ex tribus aequatt. primis Ψ valores ipsorum $a\mathfrak{A}, a\mathfrak{B}, a\mathfrak{C}$ et ex tribus aequ. primis Ψ' valores ipsorum $b\mathfrak{A}, a\mathfrak{B}, a\mathfrak{C}$ facile confirmatur fore

$$\begin{aligned} a(\mathfrak{A}\alpha\alpha + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma\gamma) &= a\mathfrak{A}' \\ a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) &= a\mathfrak{B}' \\ a(\mathfrak{A}\beta\beta + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta\delta) &= a\mathfrak{C}' \end{aligned}$$

unde, nisi $a = 0$, manifesto sequitur, formam $\mathfrak{F}$ transire in $\mathfrak{F}'$ per substitutionem propriam $\alpha, \beta, \gamma, \delta$. — Adhibendo autem loco trium aequationum primarum in Ψ et Ψ' tres sequentes, facile confirmabuntur tres aequationes modo traditis omnino similes, in quibus loco factoris a ubique invenitur b; unde patet, eandem conclusionem etiamnum valere, si modo non sit $b = 0$. Denique adhibendo tres ultimas aequationes Ψ, Ψ' invenietur eodem modo, conclusionem veram esse, nisi $c = 0$. Quocirca, quum certo omnes a, b, c simul $= 0$ esse nequeant, necessario forma $\mathfrak{F}$ per subst. $\alpha, \beta, \gamma, \delta$ transibit in $\mathfrak{F}'$, adeoque huic formae proprie aequivalebit. *Q. E. D.*

241.

Talem formam ut $\mathfrak{F}$ vel $\mathfrak{F}'$, quae oritur, si una trium formarum datarum componitur cum ea quae ex compositione duarum reliquarum resultat, *ex his tribus formis compositam* vocabimus, patetque ex art. pracc., nihil hic interesse, quonam ordine tres formae componantur. Simili modo propositis quotcunque formis f, f', f'', f''' etc. (quarum determinantes rationem quadratorum inter se habere debent), si forma f componitur cum f', resultans cum f'', quae hinc oritur cum f''' etc.: forma quae ad finem huius operationis prodit *ex omnibus formis* f, f', f'', f''' etc. composita dicetur. Facile vero demonstratur, etiam hic arbitrarium esse, quonam ordine formae componantur; *i. e.* quocunque ordine hae formae componantur, formas ex compositione oriundas semper proprie aequivalentes esse. — Porro manifestum est, si formis f, f', f'' etc. proprie aequivaleant formae g, g', g'' etc. resp., formam compositam ex his proprie aequivalentem fore formae ex illis compositae.

242.

Propositiones praecedentes formarum compositionem maxima universalitate complectuntur; progredimur iam ad applicationes magis particulares, per quas illarum ordinem interrumpere noluimus. Ac primo quidem resumemus problema art. 236, quod per conditiones sequentes limitabimus: *primo* ut formae componendae eundem determinantem habeant, sive sit $d = d'$; *secundo* ut m, m' sint inter se primi; *tertio* ut forma quaesita directe ex utraque f, f' composita sit. Hinc etiam mm, $m'm'$ inter se primi erunt; quare divisor communis maximus numerorum $dm'm'$, $d'mm$ *i. e.* D fiet $= d = d'$, atque $n = n' = 1$. Quatuor quantitates $\mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}'''$, quae ad libitum assumi possunt, statuemus $= -1, 0, 0, 0$ resp., quod semper licebit unico casu excepto, ubi $a, a', b+b'$ simul sunt $= 0$, ad quem igitur hic non respiciemus; manifesto autem hic casus occurrere nequit nisi in formis determinantis positivi quadrati. Tunc patet, μ fieri divisorem communem maximum numerorum $a, a', b+b'$; numeros $\mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ ita accipi debere ut fiat

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b+b') = \mu$$

ipsum $\mathfrak{P}$ vero omnino arbitrarium esse. Hinc provenit, substituendo l. c. pro p, q, p', q' etc. valores suos:

$$A = \tfrac{aa'}{\mu\mu}, \quad B = \tfrac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

C autem per aequationem $AC = BB - D$ poterit determinari, si modo non simul a et $a' = 0$.

In hac igitur solutione valor ipsius A non pendet a valoribus ipsorum $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ (qui infinitis modis diversis determinari possunt); B autem alios valores obtinebit tribuendo his numeris alios valores, operaeque pretium est investigare, quomodo omnes valores ipsius B inter se connexi sint. Ad hunc finem observamus

I. Quomodocunque determinentur $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$, valores ipsius B inde prodeuntes omnes congruos esse secundum modulum A. Ponamus, si statuatur

$$\mathfrak{P} = \mathfrak{p}, \quad \mathfrak{P}' = \mathfrak{p}', \quad \mathfrak{P}'' = \mathfrak{p}'', \quad \mathfrak{P}''' = \mathfrak{p}''', \quad \text{fieri} \quad B = \mathfrak{P}$$

faciendo autem

$$\mathfrak{P} = \mathfrak{p} + \mathfrak{d}, \quad \mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}', \quad \mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}'', \quad \mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}''', \quad \text{prodire} \quad B = \mathfrak{B} + \mathfrak{D}$$

Tunc igitur erit

$$a\mathfrak{d}+a'\mathfrak{d}''+(b+b')\mathfrak{d}''' = 0, \quad aa'\mathfrak{d}+ab'\mathfrak{d}'+a'b\mathfrak{d}''+(bb'+D)\mathfrak{d}''' = \mu\mathfrak{D}$$

Multiplicando aequationis posterioris partem primam per $a\mathfrak{p}'+a'\mathfrak{p}''+(b+b')\mathfrak{p}'''$, secundam per μ, et subtrahendo a producto primo quantitatem

$$(ab'\mathfrak{p}'+a'b\mathfrak{p}''+(bb'+D)\mathfrak{p}''')(a\mathfrak{d}+a'\mathfrak{d}''+(b+b')\mathfrak{d}''')$$

quae propter aequationem priorem manifesto erit $=0$, habebitur evolutione facta et sublatis quae se destruunt

$$aa'(\mu\mathfrak{d}+((b'-b)\mathfrak{p}''+c'\mathfrak{p}''')\mathfrak{d}'+((b-b')\mathfrak{p}'+c\mathfrak{p}''')\mathfrak{d}''-(c'\mathfrak{p}'+c\mathfrak{p}'')\mathfrak{d}''') = \mu\mu\mathfrak{D}$$

unde manifesto $\mu\mu\mathfrak{D}$ per aa', sive $\mathfrak{D}$ per $\frac{aa'}{\mu\mu}$ *i. e.* per A divisibilis erit, atque

$$\mathfrak{B} \equiv \mathfrak{B}+\mathfrak{D} \pmod{A}$$

II. Si valores $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \mathfrak{p}'''$ ipsorum $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ reddant $B=\mathfrak{B}$, inveniri posse alios valores horum numerorum, ex quibus B nanciscatur valorem quemcunque datum ipsi $\mathfrak{B}$ secundum mod. A congruum, puta $\mathfrak{B}+kA$. Primo observamus, quatuor numeros $\mu, c, c', b-b'$ divisorem communem habere non posse; nam si quem haberent, hic metiretur sex numeros $a, a', b+b', c, c', b-b'$ adeoque tum ipsos $a, 2b, c$, tum ipsos $a', 2b', c'$ et proin etiam ipsos m, m', qui per hyp. inter se sunt primi. Quamobrem quatuor numeri integri h, h', h'', h''' poterunt assignari tales ut fiat

$$h\mu+h'c+h''c'+h'''(b-b') = 1$$

Quo facto si statuitur

$$kh = \mathfrak{d}, \qquad k(h''(b+b')-h'''a') = \mu\mathfrak{d}'$$
$$k(h'(b+b')+h'''a) = \mu\mathfrak{d}'', \qquad -k(h'a+h''a) = \mu\mathfrak{d}'''$$

patet, ipsos $\mathfrak{d}, \mathfrak{d}', \mathfrak{d}'', \mathfrak{d}'''$ esse integros; porro facile confirmatur, fieri

$$a\mathfrak{d}'+a'\mathfrak{d}''+(b+b')\mathfrak{d}''' = 0$$
$$aa'\mathfrak{d}+ab'\mathfrak{d}'+a'b\mathfrak{d}''+(bb'+D)\mathfrak{d}''' = \frac{aa'k}{\mu}(\mu h+ch'+c'h''+(b-b')h''') = \mu kA$$

Ex aequatione priori patet, etiam $\mathfrak{p}+\mathfrak{d}, \mathfrak{p}'+\mathfrak{d}', \mathfrak{p}''+\mathfrak{d}'', \mathfrak{p}'''+\mathfrak{d}'''$ esse valores ipsorum $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$; ex posteriori, hos valores producere $B=\mathfrak{B}+kA$. *Q. E. D.*

Hinc perspicuum est, B semper ita determinari posse ut iaceat inter 0 et $A-1$ incl., siquidem A est positivus; vel inter 0 et $-A-1$ si A negativus.

213.

Ex aequationibus

$$\mathfrak{P}a+\mathfrak{P}''a'+\mathfrak{P}'''(b+b') = \mu, \quad B = \frac{1}{\mu}(\mathfrak{P}aa'+\mathfrak{P}ab'+\mathfrak{P}'a'b+\mathfrak{P}'''(bb'+D))$$

deducitur

$$B = b+\frac{a}{\mu}(\mathfrak{P}a'+\mathfrak{P}'(b'-b)-\mathfrak{P}'''c) = b'+\frac{a'}{\mu}(\mathfrak{P}a+\mathfrak{P}''(b-b')-\mathfrak{P}'''c')$$

quare

$$B \equiv b \pmod{\tfrac{a}{\mu}}, \text{ et } B \equiv b' \pmod{\tfrac{a'}{\mu}}$$

Quoties $\frac{a}{\mu}$, $\frac{a'}{\mu}$ inter se primi sunt, inter 0 et $A-1$ (sive inter 0 et $-A-1$ quando A est negativus) unicus tantum numerus iacebit qui secundum mod. $\frac{a}{\mu}$ sit $\equiv b$, et $\equiv b'$ sec. mod. $\frac{a'}{\mu}$; qui si statuitur $=B$ atque $\frac{BB-D}{A} = C$, palam est, (A, B, C) e formis (a, b, c), (a', b', c') compositam fore. In hoc itaque casu ad inventionem formae compositae ad numeros $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ non amplius oportet respicere.*). Ita *e. g.* si quaeritur forma e formis $(10, 3, 11)$, $(15, 2, 7)$ composita, erunt $a, a', b+b'$ resp. $=10, 15, 5$; $\mu=5$; hinc $A=6$; $B\equiv 3 \pmod 2$ et $\equiv 2 \pmod 3$, unde $B=5$ atque $(6, 5, 21)$ forma quaesita. — Ceterum conditio ut $\frac{a}{\mu}$, $\frac{a'}{\mu}$ inter se primi sint, omnino aequivalet huic, ut numeri duo a, a' divisorem communem maiorem non habeant quam tres $a, a', b+b'$, sive, quod eodem redit, ut divisor communis maximus numerorum a, a' etiam numerum $b+b'$ metiatur. Notentur imprimis sequentes casus particulares:

1) Propositis duabus formis (a, b, c), (a', b', c') eiusdem determinantis D ita comparatis ut divisor comm. max. numerorum a, $2b$, c primus sit ad div. comm. max. num. a', $2b'$, c', atque a primus ad a': forma ex his composita (A, B, C) invenitur faciendo $A=aa'$, $B\equiv b \pmod a$ et $\equiv b' \pmod{a'}$, $C=\frac{BB-D}{A}$. Hic casus semper locum habet, quando altera formarum componendarum est forma principalis, puta $a=1$, $b=0$, $c=-D$. Tunc erit $A=a'$, B statui poterit

*) Quod semper efficitur adhibendo congruentias

$$\frac{aB}{\mu} \equiv \frac{ab'}{\mu}, \quad \frac{a'B}{\mu} \equiv \frac{a'b}{\mu}, \quad \frac{(b+b')B}{\mu} \equiv \frac{bb'+D}{\mu} \pmod A$$

$= b'$, unde fiet $C = c'$; quare *ex forma principali et quacunque alia forma eiusdem determinantis composita est haec forma ipsa.*

2) Si duae formae *oppositae* proprie primitivae sunt componendae, puta (a, b, c) et $(a, -b, c)$, erit $\mu = a$. Hinc facile perspicitur, formam principalem $(1, 0, -D)$ ex illis esse compositam.

3) Propositis quotcunque formis proprie primitivis, (a, b, c), (a', b', c'), (a'', b'', c'') etc. eiusdem determinantis D, quarum termini antecedentes a, a', a'' etc. sunt numeri inter se primi, forma (A, B, C) ex illis omnibus composita invenitur, statuendo A aequalem producto ex omnibus a, a'; a'' etc.; B congruum ipsis b, b', b'' etc. secundum modulos a, a', a'' etc. resp.; $C = \frac{BB-D}{A}$. Facile enim perspicietur, ex duabus formis (a, b, c), (a', b', c') compositam fore formam $(aa', B, \frac{BB-D}{aa'})$; ex hac atque (a'', b'', c'') formam $(aa'a'', B, \frac{BB-D}{aa'a''})$ etc. — Vice versa

4) Proposita forma proprie primitiva (A, B, C) determinantis D, si terminus A in factores quotcunque inter se primos a, a', a'' etc. resolvitur; numeri b, b', b'' etc. ipsi B vel aequales vel saltem sec. mod. a, a', a'' etc. resp. congrui accipiuntur, atque fit $ac = bb - D$, $a'c' = b'b' - D$, $a''c'' = b''b'' - D$ etc.: forma (A, B, C) composita erit e formis (a, b, c), (a', b', c'), (a'', b'', c''), sive *in has formas resolubilis.* Nullo negotio probatur, eandem propositionem adhucdum valere, etiamsi forma (A, B, C) sit improprie primitiva vel derivata. Hoc itaque modo quaelibet forma in alias eiusdem determinantis resolvi potest, quarum termini antecedentes omnes sint vel numeri primi vel numerorum primorum potestates. Talis resolutio saepenumero commode applicari potest, si ex pluribus formis datis componenda est una. Ita *e. g.* si quaeritur forma composita e formis $(3, 1, 134)$, $(10, 3, 41)$, $(15, 2, 27)$, resolvatur secunda in has $(2, 1, 201)$, $(5, -2, 81)$, tertia in has $(3, -1, 134)$, $(5, 2, 81)$, patetque, formam ex quinque formis $(3, 1, 134)$, $(2, 1, 201)$, $(5, -2, 81)$, $(3, -1, 134)$, $(5, 2, 81)$ compositam, quocunque ordine accipiantur, etiam ex tribus datis compositam fore. At ex compositione primae cum quarta oritur forma principalis $(1, 0, 401)$; eadem provenit ex compositione tertiae cum quinta; quare ex compositione cunctarum conflatur forma $(2, 1, 201)$.

5) Propter rei utilitatem operae pretium est, hanc methodum adhuc amplius explicare. Ex observatione praecedente manifestum est, problema, quotcunque formas datas proprie primitivas eiusdem determinantis componere, reduci posse ad compositionem formarum, quarum termini initiales sint potestates numerorum primorum (nam numerus primus tamquam sui ipsius potestas prima considerari potest). Quamobrem eum imprimis casum contemplari convenit, ubi duae formae proprie primitivae (a, b, c), (a', b', c') sunt componendae, in quibus a et a' sunt potestates *eiusdem* numeri primi. Sit itaque $a = h^\varkappa$, $a' = h^\lambda$ designante h numerum primum, supponamusque (quod licet), $\varkappa$ non esse minorem quam λ. Erit itaque h^λ div. comm. max. numerorum a, a', qui si insuper ipsum $b + b'$ metitur, habebitur casus initio huius art. consideratus, eritque (A, B, C) ex propositis composita si statuitur $A = h^{\varkappa-\lambda}$, $B \equiv b \pmod{h^{\varkappa-\lambda}}$ et $\equiv b' \pmod 1$, quae conditio posterior manifesto omitti potest; $C = \frac{BB-D}{A}$. Si vero h^λ ipsum $b + b'$ non metitur, necessario div. comm. max. horum numerorum et ipse erit potestas ipsius h, sit igitur $= h^\nu$, eritque $\nu < \lambda$ (statui debet $\nu = 0$, si forte h^λ et $b + b'$ inter se primi sunt). Si itaque $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ ita determinantur, ut fiat

$$\mathfrak{P}h^\varkappa + \mathfrak{P}'h^\lambda + \mathfrak{P}''(b + b') = h^\nu$$

$\mathfrak{P}$ vero ad libitum assumitur, forma (A, B, C) ex datis erit composita, si statuitur

$$A = h^{\varkappa+\lambda-2\nu}, \quad B = b + h^{\varkappa-\nu}(\mathfrak{P}h^\lambda - \mathfrak{P}(b - b') - \mathfrak{P}''c), \quad C = \frac{BB-D}{A}$$

Sed facile perspicitur, in hoc casu etiam $\mathfrak{P}'$ ad libitum assumi posse, quare statuendo $\mathfrak{P} = \mathfrak{P}' = 0$, fit

$$B = b - \mathfrak{P}''ch^{\varkappa-\nu}$$

sive generaliter

$$B = kA + b - \mathfrak{P}''ch^{\varkappa-\nu}$$

designante k numerum arbitrarium (art. praec.). In hanc formulam simplicissimam solus $\mathfrak{P}''$ ingreditur, qui est valor expr. $\frac{h^\nu}{b+b'} \pmod{h^\lambda}$ *). Si *e. g.* quaeritur forma composita ex $(16, 3, 19)$ et $(8, 1, 37)$, est $h = 2$, $\varkappa = 4$, $\lambda = 3$, $\nu = 2$.

*) sive expr. $\frac{-1}{\frac{b+b'}{h^\nu}} \pmod{h^{\lambda-\nu}}$ unde $B \equiv b - \frac{ch^{\varkappa-\nu}}{\frac{b+b'}{h^\nu}} \equiv \frac{(D+bb')\,z\,h^\nu}{(b+b')\,z\,h^\nu} \pmod A$

Hinc $A = 8$, $\mathfrak{P}''$ valor expr. $\frac{1}{4}(\mathrm{mod.}\ 8)$, qualis est 1, unde $B' = 8k - 73$, adeoque faciendo $k = 9$, $B = -1$ atque $C = 37$, sive $(8, -1, 37)$ forma quaesita.

Propositis itaque formis quotcunque, quarum termini initiales omnes sunt potestates numerorum primorum, circumspiciendum erit, num aliquarum termini antecedentes sint potestates *eiusdem* numeri primi, atque hae inter se respective per regulam modo traditam componendae. Hac ratione prodibunt formae, quarum termini primi etiamnum erunt potestates numerorum primorum, sed omnino diversorum; forma itaque ex his composita per observ. tertiam definiri poterit. *E. g.* propositis formis $(3, 1, 47)$, $(4, 0, 35)$, $(5, 0, 28)$, $(16, 2, 9)$, $(9, 7, 21)$, $(16, 6, 11)$, ex prima et quinta conflatur forma $(27, 7, 7)$; ex secunda et quarta confit $(16, -6, 11)$, ex hac et sexta $(1, 0, 140)$, quae negligi potest. Supersunt itaque $(5, 0, 28)$, $(27, 7, 7)$, ex quibus producitur $(135, -20, 4)$, cuius loco assumi potest proprie aequivalens $(4, 0, 35)$. Haec itaque est resultans ex compositione sex propositarum.

Ceterum ex hoc fonte plura alia artificia in applicatione utilia hauriri possunt; sed ne nimis longi fiamus, uberiorem huius rei tractationem supprimimus, ad alia difficiliora properantes.

244.

Si per formam aliquam f repraesentari potest numerus a, per formam f' numerus a', atque forma F in ff' est transformabilis: nullo negotio perspicitur, productum aa' per formam F repraesentabile fore. Hinc statim sequitur, quando determinantes harum formarum sint negativi, formam F positivam fore, si vel utraque f, f' sit positiva vel utraque negativa; contra F fieri negativam, si altera formarum f, f' sit positiva altera negativa. Subsistamus in eo imprimis casu, quem in art. praec. consideravimus, ubi F ex f, f' composita est, atque f, f' et F eundem determinantem D habent. Supponamus insuper, repraesentationes numerorum a, a' per formas f, f' fieri per valores indeterminatarum inter se primos, atque priorem pertinere ad valorem b expressionis $\sqrt{D}\ (\mathrm{mod.}\ a)$, posteriorem ad valorem b' expr. $\sqrt{D}\ (\mathrm{mod.}\ a')$, ponaturque $bb - D = ac$, $b'b' - D = a'c'$. Tunc per art. 168 formae (a, b, c), (a', b', c') proprie aequivalebunt formis f, f'; quare F etiam ex illis duabus formis composita erit. Sed ex iisdem formis composita erit forma (A, B, C), si, posito numerorum $a, a', b + b'$ divisore communi maximo $= \mu$, statuitur $A = \frac{aa'}{\mu\mu}$, $B \equiv b'$ et b' sec. modulos $\frac{a}{\mu}, \frac{a'}{\mu}$, resp.,

$AC = BB - D$; quare haec forma proprie aequivalebit formae F. Iam per formam $Axx + 2Bxy + Cyy$ repraesentatur numerus aa', faciendo $x = \mu$, $y = 0$, quorum valorum divisor comm. max. est μ; quare aa' etiam per formam F repraesentari poterit ita ut valores indeterminatarum habeant divisorem communem maximum μ (art. 166). Quoties igitur evadit $\mu = 1$, aa' per formam F repraesentari poterit tribuendo indeterminatis valores inter se primos, repraesentatioque haec pertinebit ad valorem B expr. $\sqrt{D}\ (\mathrm{mod.}\ aa')$, ipsis b, b' secundum modulos a, a' resp. congruum. Conditio $\mu = 1$ semper locum habet, quando a, a' inter se primi sunt; generaliter autem, quando div. comm. max. ipsorum a, a' ad $b + b'$ est primus.

Compositio ordinum.

245.

Theorema. *Si forma f ad eundem ordinem referenda est ut g, similiterque f' est ex eodem ordine ut g': forma F ex f, f' composita eundem determinantem habebit ex eodemque ordine erit ut forma G ex g, g' composita.*

Dem. Sint formae $f, f', F = (a, b, c)$, (a', b', c'), (A, B, C) resp., ipsarumque determinantes $= d, d', D$. Porro sit numerorum $a, 2b, c$ div. comm. max. $= m$; numerorum a, b, c div. comm. max. $= \mathfrak{m}$; similesque significationes habeant $m', \mathfrak{m}'$ respectu formae f', et $M, \mathfrak{M}$ respectu formae F. Tunc ordo formae f determinabitur per numeros $d, m, \mathfrak{m}$, unde iidem numeri etiam pro forma g valebunt; eadem ratione numeri $d', m', \mathfrak{m}'$ idem erunt pro forma g' quod sunt pro forma f'. Iam per art. 235, numeri $D, M, \mathfrak{M}$ determinati sunt per $d, d', m, m', \mathfrak{m}, \mathfrak{m}'$; scilicet erit D divisor communis maximus ipsorum $dm'm'$, $d'mm$; $M = mm'$; atque $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (si simul $m = \mathfrak{m}$, $m' = \mathfrak{m}'$) vel $= 2\mathfrak{m}\mathfrak{m}'$ (si $m = 2\mathfrak{m}$, aut $m' = 2\mathfrak{m}'$). Quae proprietates ipsorum $D, M, \mathfrak{M}$, quum inde sequantur, quod F ex f, f' composita est: facile perspicitur, D, M et $\mathfrak{M}$ etiam pro forma G valere, adeoque G esse ex eodem ordine ut F. Q. E. D.

Ex hac ratione ordinem in quo est forma F, compositum dicemus ex ordinibus in quibus sunt formae f, f'. Ita *e. g.* ex duobus ordinibus proprie primitivis semper compositus est similis ordo; ex proprie primitivo et improprie primitivo, improprie primitivus. — Simili modo intelligendum est, si ordo aliquis ex pluribus aliis ordinibus compositus vocabitur.

Compositio generum.

246.

PROBLEMA. *Propositis duabus formis primitivis quibuscunque f, f', ex quarum compositione oritur F; ex generibus ad quae pertinent f, f' definire genus ad quod referenda erit F.*

Sol. I. Considceremus primo eum casum ubi ad minimum una formarum f, f' e. g. prior est proprie primitiva, designemusque determinantes formarum f, f', F per d, d', D. Tunc D erit divisor communis maximus numerorum dm'^2, d', ubi m' est aut 1 aut 2, prout forma f' est proprie aut improprie primitiva; F autem in casu illo pertinebit ad ordinem proprie primitivum, in hoc ad improprie primitivum. Iam genus formae F definietur per ipsius characteres particulares, nempe tum respectu singulorum divisorum primorum imparium ipsius D, tum, pro quibusdam casibus, respectu numerorum 4 aut 8. Hos igitur singulos determinare oportebit.

1°. Si p est divisor quicunque primus impar ipsius D, necessario etiam ipsos d, d' metietur, adeoque etiam inter characteres formarum f, f' occurrent ipsarum relationes ad p. Iam si per f repraesentari potest numerus a, per f' numerus a': productum aa' repraesentari poterit per F. Si itaque tum per f, tum per f' repraesentari possunt residua quadratica ipsius p (per p non divisibilia), etiam per F residua quadratica ipsius p repraesentari poterunt, *i. e.* si utraque f, f' habet characterem Rp, forma F eundem characterem habebit. Simili ratione F habebit characterem Rp, si utraque f, f' habet characterem Np; contra F habebit char. Np, si altera formarum f, f' habet Rp, altera Np.

2°. Si in characterem integrum formae F ingreditur relatio ad numerum 4, talis relatio etiam in characteres formarum f, f' ingredi debet. Nam illud tunc tantummodo evenit, quando D est $\equiv 0$ aut $\equiv 3 \pmod 4$. Quando D per 4 est divisibilis, etiam dm'^2 et d' per 4 divisibiles erunt, unde statim patet, f' non posse esse improprie primitivam, adeoque esse $m' = 1$; hinc tum d tum d' per 4 divisibiles erunt, et in utriusque characterem ingredietur relatio ad 4. Quando $D \equiv 3 \pmod 4$, metietur D ipsos d, d'; quotientes erunt quadrata, adeoque etiam d, d' necessario vel $\equiv 0$ vel $\equiv 3 \pmod 4$, et inter characteres ipsarum f, f' relatio ad 4. Hinc eodem modo ut in (1°) sequitur, characterem formae F fore 1,4, si vel utraque f, f' habeat 1,4 vel utraque 3,4; contra characterem formae F fore 3,4, si altera formarum f, f' habeat 1,4, altera 3,4.

3°. Quando D per 8 est divisibilis, etiam d' erit; hinc f' certo proprie primitiva, $m' = 1$ atque etiam d per 8 divisibilis; quare inter characteres formae F aliquis e characteribus 1,8; 3,8; 5,8; 7,8 tunc tantum locum habere potest, si etiam in charactere tum formae f, tum formae f' talis relatio ad 8 adest. Facile autem confirmatur eodem modo ut ante, characterem formae F fore 1,8, si f et f' respectu ipsius 8 eundem habeant; characterem formae F fore 3,8, si altera formarum f, f' habeat 1,8 altera 3,8, vel altera 5,8 altera 7,8; F habere 5,8, si f, f' habeant 1,8 et 5,8 vel 3,8 et 7,8; F habere 7,8, si f et f' habeant vel 1,8 et 7,8, vel 3,8 et 5,8.

4°. Quando est $D \equiv 2 \pmod 8$, erit d' vel $\equiv 0$ vel $\equiv 2 \pmod 8$, hinc $m' = 1$, adeoque etiam d vel $\equiv 0$ vel $\equiv 2 \pmod 8$; attamen uterque d, d' per 8 divisibilis esse nequit, quoniam D est divisor communis *maximus* ipsorum. Quare in eo tantum casu alteruter characterum 1 *et* 7,8; 3 *et* 5,8 formae F tribui debebit, ubi vel vtraque forma f, f' aliquem ex illis habet, vel altera aliquem ex illis, altera aliquem horum 1,8; 3,8; 5,8; 7,8. Hinc facile deducitur, characterem formae F determinari per tabulam sequentem, si character in margine positus pertineat ad alteram formarum f, f', ad alteram vero character in facie:

	1 *et* 7,8 vel 1,8 vel 7,8	3 *et* 5,8 vel 3,8 vel 5,8
1 *et* 7,8	1 *et* 7,8	3 *et* 5,8
3 *et* 5,8	3 *et* 5,8	1 *et* 7,8

5°. Eodem modo probatur, ipsi F tribui non posse alterutrum characterum 1 *et* 3,8; 5 *et* 7,8, nisi etiam aliquis ex iisdem saltem uni formarum f, f' competat, alterique vel aliquis ex iisdem, vel aliquis ex his 1,8; 3,8; 5,8; 7,8.

Et quidem character formae F determinabitur per hanc tabulam, in cuius margine et facie sunt characteres formarum f, f'

	1 *et* 3, 8 vel 1, 8 vel 3, 8	5 *et* 7, 8 vel 5, 8 vel 7, 8
1 *et* 3, 8	1 *et* 3, 8	5 *et* 7, 8
5 *et* 7, 8	5 *et* 7, 8	1 *et* 3, 8

II. Si utraque forma f, f' est improprie primitiva, erit D divisor communis maximus numerorum $4d$, $4d'$, sive $\frac{1}{4}D$ div. comm. maximus numerorum d, d'. Hinc facile sequitur, tum d, tum d', tum $\frac{1}{4}D$ fore $\equiv 1 \pmod 4$. Ponendo autem $F = (A, B, C)$, div. comm. max. numerorum A, B, C erit $= 2$, et div. comm. max. numerorum A, $2B$, C erit 4. Quare F erit forma derivata ex improprie primitiva $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$, cuius determinans erit $\frac{1}{4}D$, et cuius genus determinabit genus formae F. Character autem illius formae, tamquam improprie primitivae, relationes ad 4 vel 8 non implicabit, sed tantummodo relationes ad singulos divisores primos impares ipsius $\frac{1}{4}D$. Iam quum omnes hi divisores manifesto etiam ipsos d, d' metiantur, atque semissis cuiusvis producti duorum factorum, quorum alter per f alter per f' est repraesentabilis, per formam $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$ repraesentari possit: facile perspicietur, characterem huius formae respectu cuiusvis numeri primi imparis p ipsum $\frac{1}{4}D$ metientis fore Rp, *tum* si fuerit $2Rp$ atque formae f, f' respectu ipsius p eundem characterem habeant, *tum* si fuerit $2Np$ atque characteres formarum f, f' respectu ipsius p oppositi; contra characterem illius formae fore Np, *tum* si f, f' habeant characteres aequales respectu ipsius p atque sit $2Np$, *tum* si f, f' habeant oppositos atque sit $2Rp$.

247.

Ex solutione problematis praec. manifestum est, si g sit forma primitiva ex eodem ordine et genere ut f, nec non g' forma primitiva ex eodem ordine et genere ut f': formam ex g et g' compositam ad idem genus pertinere, ad quod pertineat forma ex f et f' composita. Hinc sponte sequitur significatio *generis*

ex duobus aliis generibus (sive etiam pluribus) *compositi*. Porro ibinde patet, si f, f' eundem determinantem habeant atque f sit forma e genere principali, F vero ex f et f' composita: F fore ex eodem genere ut f'; quocirca genus principale in compositione cum aliis generibus eiusdem determinantis semper omitti poterit. Si vero reliquis manentibus f non est e genere principali, f' autem forma primitiva: F certo erit ex alio genere quam f'. Denique si f, f' sunt formae proprie primitivae eiusdem generis, F erit e genere principali; si vero f, f' sunt ambae proprie primitivae eiusdem determinantis, sed e diversis generibus, F ad genus principale pertinere non poterit. Quodsi itaque forma quaecunque proprie primitiva *cum se ipsa* componitur, forma inde resultans, quae etiam proprie primitiva eiusdemque determinantis erit, necessario ad genus principale pertinebit.

248.

Problema. *Propositis duabus formis quibuscunque f, f', e quibus composita est F: e generibus formarum f, f' definire genus formae F.*

Sol. Sit $f = (a, b, c)$, $f' = (a', b', c')$, $F = (A, B, C)$, porro $\mathfrak{m}$ div. comm. max. numerorum a, b, c, atque $\mathfrak{m}'$ div. comm. max. numerorum a', b', c', ita ut f, f' sint derivatae e primitivis $(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}})$, $(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'})$, quas denotabimus per $\mathfrak{f}$, $\mathfrak{f}'$ resp. Iam si saltem una formarum $\mathfrak{f}$, $\mathfrak{f}'$ est proprie primitiva, divisor comm. max. numerorum A, B, C erit $\mathfrak{m}\mathfrak{m}'$, adeoque F derivata e forma primitiva $(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}) \ldots \mathfrak{F}$, unde patet, genus formae F pendere a genere formae $\mathfrak{F}$. Sed facile perspicietur, $\mathfrak{F}$ per eandem substitutionem transire in $\mathfrak{f}\mathfrak{f}'$, per quam F transeat in ff', adeoque $\mathfrak{F}$ ex $\mathfrak{f}$, $\mathfrak{f}'$ esse compositam, ipsiusque genus per problema art. 246 determinari posse. — Si vero utraque $\mathfrak{f}$, $\mathfrak{f}'$ est improprie primitiva, divisor c. m. numerorum A, B, C erit $2\mathfrak{m}\mathfrak{m}'$, formaque $\mathfrak{F}$ etiamnum ex $\mathfrak{f}$, $\mathfrak{f}'$ composita et manifesto e proprie primitiva $(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'})$ derivata. Huius itaque formae genus determinari poterit per art. 246; et quum F ex eadem forma derivata sit, ipsius genus hinc sponte innotescit.

Ex hac solutione manifestum est, theorema in art. praec. pro formis primitivis explicatum, scilicet *si f', g' sint ex iisdem generibus resp. ut f, g, formam ex f', g' compositam ex eodem genere fore, ex quo sit forma ex f, g composita*, generaliter pro formis quibuscunque valere.

Compositio classium.

249.

THEOREMA. *Si formae f, f' sunt ex iisdem ordinibus generibus et classibus ut g, g' resp.: forma ex f et f' composita ex eadem classe erit ut forma ex g et g' composita.*

Ex hoc theoremate (cuius veritas ex art. 239 protinus sequitur) sponte patebit significatio *classis e duabus classibus datis* sive etiam *e pluribus compositae*.

Si classis quaecunque K cum classe principali componitur, classis K ipsa prodibit sive classis principalis in compositione cum aliis classibus eiusdem determinantis negligi potest. Ex compositione duarum classium oppositarum proprie primitivarum semper oritur classis principalis eiusdem determinantis (v. art. 243). Quum itaque quaevis classis anceps sibi ipsa opposita sit: ex compositione cuiusvis classis ancipitis proprie primitivae cum se ipsa classis principalis eiusdem determinantis provenit.

Propositio ultima etiam conversa valet: scilicet *si ex compositione classis proprie primitivae K cum se ipsa provenit classis principalis H eiusdem determinantis, K necessario erit classis anceps.* Si enim K' est classis opposita ipsi K, e tribus classibus K, K, K' composita erit eadem classis quae oritur ex H et K'; ex illis provenit K (quoniam K et K' producunt H, haec cum K ipsam K), ex his K'; quare K cum K' coincidet eritque adeo classis anceps.

Porro notetur propositio haec: *Si classes K, L oppositae sunt classibus K', L' resp.: classis ex K et L composita classi ex K' et L' compositae erit opposita.* Sint formae f, g, f', g' resp. e classibus K, L, K', L'; forma F composita ex f, g, atque F' composita ex f', g'. Quum f' ipsi f, atque g' ipsi g improprie aequivaleant, F autem composita sit ex utraque f, g directe: F etiam ex f', g' composita erit, sed ex utraque inverse. Quare forma quaecunque, quae ipsi F improprie aequivalet, composita erit ex f', g' directe adeoque ipsi F' proprie aequivalebit (artt. 238, 239), unde F, F' improprie aequivalebunt, classesque ad quas pertinent, oppositae erunt.

Hinc sequitur, si classis anceps K cum classe ancipite L componatur, semper prodire classem ancipitem. Nam opposita erit classi, quae composita est e classibus ipsis K, L oppositis, adeoque sibi ipsi, quoniam hae classes sibi ipsae sunt oppositae.

Denique observamus, si propositae sint classes duae quaecunque K, L eiusdem determinantis, quarum prior sit proprie primitiva, semper inveniri posse classem M eiusdem determinantis, ex qua atque K composita sit L. Manifesto hoc obtinetur, accipiendo pro M classem quae composita est ex L atque classe ipsi K opposita; simul perspicietur facillime, hanc classem esse unicam quae hac proprietate sit praedita, sive classes diversas eiusdem det. cum eadem classe pr. prim. compositas producere classes diversas.

Classium compositio commode per signum additionis, $+$, denotari potest, sicuti classium identitas per signum aequalitatis. In his signis propositio modo tradita exhiberi potest ita: Si K' est classis opposita ipsi K, erit $K+K'$ classis principalis eiusdem determinantis, unde $K+K'+L=L$; posita itaque $K'+L=M$, erit $K+M=L$, uti desiderabatur; si vero praeter M alia M' daretur eadem proprietate praedita, sive $K+M'=L$, foret $K+K'+M'=L+K'=M$, unde $M'=M$. — Si plures classes identicae componuntur, hoc (ad instar multiplicationis) denotari potest praefigendo ipsarum numerum, ita ut $2K$ idem designet ut $K+K$, $3K$ idem ut $K+K+K$ etc. Eadem signa etiam ad formas transferri possent, ita ut $(a, b, c)+(a', b', c')$ designaret formam ex (a, b, c), (a', b', c') compositam: sed ne vel species ambiguitatis oriri possit, hac abbreviatione abstinere malumus, praesertim quod tali signo $\sqrt{M}(a, b, c)$ significationem peculiarem iam tribuimus. — Classem $2K$ ex *duplicatione* classis K oriri dicemus, classem $3K$ ex *triplicatione* etc.

250.

Si D est numerus per mm divisibilis (ubi ipsum m positivum supponimus): dabitur ordo formarum determinantis D ex ordine proprie primitivo determinantis $\frac{D}{mm}$ derivatus (sive *duo*, quando D est negativus, nempe positivus et negativus); manifesto forma $(m, 0, -\frac{D}{m})$ ad illum ordinem pertinebit (scilicet ad positivum) meritoque tamquam *forma simplicissima* in eo considerari potest (sicuti $(-m, 0, \frac{D}{m})$ erit simplicissima in ordine negativo quando D neg.). Si insuper est $\frac{D}{mm} \equiv 1 \pmod 4$, dabitur etiam ordo formarum det. D ex improprie primitivo det. $\frac{D}{mm}$ derivatus, ad quem manifesto forma $(2m, m, \frac{mm-D}{2m})$ pertinebit et pro simplicissima in eodem habebitur. (Quando D est neg., rursus duo ordines dabuntur et in negativo forma $(-2m, -m, \frac{D-mm}{2m})$ pro simplicissima habebitur). Ita *e. g.*, si etiam eum casum ubi $m=1$ huc referre lubet, in quatuor ordinibus

formarum det. 45 sequentes erunt simplicissimae $(1, 0, -45)$, $(2, 1, -22)$, $(3, 0, -15)$, $(6, 3, -6)$. Quibus ita intellectis, offert se

PROBLEMA. *Proposita forma quacunque F ex ordine O, invenire formam proprie primitivam (positivam) eiusdem determinantis, ex cuius compositione cum forma in O simplicissima oriatur F.*

Sol. Sit forma $F = (ma, mb, mc)$ derivata e primitiva $f = (a, b, c)$ cuius determinans $= d$, supponamusque *primo*, f esse proprie primitivam. Primo observamus, si forte a ad $2dm$ non sit primus, certo dari alias formas ipsi (a, b, c) proprie aequivalentes, quarum termini primi hac proprietate sint praediti. Nam per art. 228 dantur numeri ad $2dm$ primi per formam illam repraesentabiles; sit talis numerus $a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$, supponamusque, (quod licet), α, γ esse inter se primos; tum, acceptis δ, ζ ita ut fiat $\alpha\zeta - \delta\gamma = 1$, transeat f per substitutionem $\alpha, \delta, \gamma, \zeta$ in formam (a', b', c'), quae illi proprie aequivalebit et proprietate praescripta erit praedita. Iam quum etiam F et $(a'm, b'm, c'm)$ proprie aequivaleant, facile perspicietur, sufficere eum casum considerare ubi a ad $2dm$ sit primus. Tunc (a, bm, cmm) erit forma proprie primitiva (si enim a, $2bm$, cmm divisorem communem haberent, hunc etiam $2dm = 2bbm - 2acm$ implicaret) eiusdem determinantis ut F, confirmaturque facile, F transmutari in productum e forma $(m, 0, -dm)$, quae, nisi F est forma negativa, erit simplicissima ordinis O, in (a, bm, cmm) per substitutionem $1, 0; -b, -cm; 0, m, a, bm$, unde per criterium in obs. 4. art. 235 concluditur, F ex $(m, 0, -dm)$ et (a, bm, cmm) esse compositam. Quando autem F est forma negativa, transibit in productum e forma simplicissima eiusdem ordinis $(-m, 0, dm)$ in positivam $(-a, bm, -cmm)$ per substitutionem $1, 0, b, -cm; 0, -m, -a, bm$, adeoque ex ipsis erit composita.

Secundo, si f est forma improprie primitiva, supponere licebit $\frac{1}{2}a$ ad $2dm$ esse primum; si enim haec proprietas in forma f locum nondum habet, inveniri potest forma ipsi f proprie aequivalens et hac proprietate praedita. Hinc autem sequitur facile, $(\frac{1}{2}a, bm, 2cmm)$ esse formam proprie primitivam eiusdem determinantis ut F; aeque facile confirmatur, F transire in productum e formis

$$(\pm 2m, \pm m, \pm\tfrac{1}{2}(m - dm)), \quad (\pm\tfrac{1}{2}a, bm, \pm 2cmm)$$

per substitutionem

$$1, 0, \tfrac{1}{2}(1 \mp b), -cm; \quad 0, \pm 2m, \pm\tfrac{1}{2}a, (b \pm 1)m$$

ubi signa inferiora accipienda sunt quando F est forma negativa, superiora in casibus reliquis, adeoque ex his duabus formis esse compositam, quarum prior erit simplicissima ordinis O, posterior forma proprie primitiva (positiva).

251.

PROBLEMA. *Propositis duabus formis F, f eiusdem determinantis D et ad eundem ordinem O pertinentibus: invenire formam proprie primitivam determinantis D, quae cum f composita producat F.*

Sol. Sit φ forma simplicissima ordinis O; $\mathfrak{F}$, $\mathfrak{f}$ formae proprie primitivae det. D, quae cum φ compositae producant ipsas F, f resp.; denique f' forma proprie primitiva, quae cum $\mathfrak{f}$ composita producat $\mathfrak{F}$. Tunc forma F composita erit e tribus formis φ, $\mathfrak{f}$, f', sive e duabus f, f'. *Q. E. I.*

Quaevis itaque classis ordinis dati considerari potest tamquam composita ex quacunque classe data eiusdem ordinis et aliqua classe proprie primitiva eiusdem determinantis.

Pro determinante dato in singulis generibus eiusdem ordinis contentae sunt classes aeque multae.

252.

THEOREMA. *Pro determinante dato in singulis generibus eiusdem ordinis contentae sunt classes aeque multae.*

Dem. Pertineant genera G et H ad eundem ordinem, constet G ex n classibus $K, K', K'' \dots K^{n-1}$, sitque L classis aliqua e genere H. Investigetur per art. praec. classis proprie primitiva M eiusdem determinantis, ex cuius compositione cum K prodeat L, designenturque classes quae oriuntur ex compositione classis M cum $K', K'' \dots K^{n-1}$ resp. per $L', L'' \dots L^{n-1}$. Tunc ex obs. ultima art. 249 sequitur, omnes classes $L, L', L'' \dots L^{n-1}$ esse diversas, et per art. 248 omnes pertinebunt ad genus idem, *i. e.* ad genus H. Denique perspicietur facile, H alias classes praeter has continere non posse, quum quaevis classis generis H tamquam composita considerari possit ex M et alia classe eiusdem determinantis, quae necessario semper erit e genere G. Quocirca H perinde ut G continet n classes diversas. *Q. E. D.*

Comparantur multitudines classium in singulis generibus ordinum diversorum contentarum.

253.

Theorema praecedens supponit ordinis identitatem neque ad ordines diversos est extendendum. Ita *e. g.* pro determinante -171 dantur 20 classes positivae, quae reducuntur ad quatuor ordines: in ordine proprie primitivo duo continentur genera, utrumque sex classes complectitur; in ordine impr. primitivo duo genera quatuor classes possident, singula binas; in ordine derivato ex O. proprie prim. det. -19 unicum est genus tres classes complectens; denique O. derivatus ex impr. prim. det. -19 unicum genus habet ex una classe constans; perinde se habent classes negativae. Operae itaque pretium est, in principium generale inquirere, a quo nexus inter multitudines classium in diversis ordinibus pendeat. Supponamus, K, L esse duas classes ex eodem ordine (positivo) O determinantis D, atque M classem proprie primitivam eiusdem det., ex cuius compositione cum K oriatur L, qualis per art. 251 semper potest assignari. Iam in quibusdam casibus fieri potest, ut M sit *unica* classis pr. primitiva, quae cum K composita producat L; in aliis plures classes diversae pr. primitivae exstare possunt hac proprietate praeditae. Supponamus generaliter, dari r huiusmodi classes pr. primitivas, $M, M', M'' \dots M^{r-1}$, quae singulae cum K compositae producant eandem classem L, designemusque illarum complexum per W. Porro sit L' alia classis ordinis O (a classe L diversa), atque N' classis pr. prim. det. D, quae cum L composita efficiat L', designeturque complexus classium $N'+M, N'+M', N'+M'' \dots N'+M^{r-1}$ (quae omnes erunt proprie primitivae et inter se diversae) per W'. Tunc perspicietur facile, K cum classe quacunque ex W' compositam producere L', unde concluditur, W et W' nullam classem communem habere; praeterea nullo negotio comprobatur, nullam classem pr. primitivam in complexu W' non contentam dari, quae cum K composita producat ipsam L'. Eodem modo patet, si L'' sit alia classis ordinis O a classibus L, L' diversa, dari r formas pr. primitivas tum inter se tum a formis W, W' diversas, quae singulae cum K compositae ipsam L'' producant, et perinde res se habebit pro omnibus reliquis classibus ordinis O. Quoniam vero quaevis classis pr. prim. (positiva) determinantis D cum K composita classem ordinis O producit, facile hinc colligitur, si multitudo omnium classium ordinis O sit n, multitudinem omnium classium proprie primitivarum (positivarum) eiusdem determinantis fore rn. Habemus itaque regulam generalem: Denotantibus K, L classes quascunque ordinis O, atque r multitudinem classium proprie primitivarum diversarum eiusdem determinantis, quae singulae cum K compositae ipsam L producunt, multitudo omnium classium in ordine proprie primitivo (positivo) r vicibus maior erit quam multitudo classium ordinis O.

Quum classes K, L in ordine O omnino ad libitum assumi possint, etiam classes identicas accipere licebit, et quidem e re erit ea classe uti, in qua continetur forma huius ordinis simplicissima. Quam itaque pro K et L assumendo, res eo reducta est, ut omnes classes proprie primitivae assignentur, quae cum K compositae ipsam K reproducant. Huc via sternitur per sequens

254.

Theorema. *Si $F = (A, B, C)$ est forma simplicissima ordinis O determinantis D, atque $f = (a, b, c)$ forma proprie primitiva eiusdem determinantis: per hanc formam f repraesentari poterit numerus AA, si F oritur per compositionem formarum f, F; et vice versa F ex se ipsa atque f composita erit, si AA per f repraesentari potest.*

Dem. I. Si F in productum fF transit per substitutionem p, p', p'', p'''; q, q', q'', q'''; ex art. 235 habemus

$$A(aq''q'' - 2bqq'' + cqq) = A^3, \text{ unde } AA = aq''q'' - 2bqq'' + cqq. \quad Q.E.P.$$

II. Si *supponitur*, AA per f repraesentari posse, designentur valores indeterminatarum per quos hoc efficitur per q'', $-q$, sive sit $AA = aq''q'' - 2bqq'' + cqq$. ponaturque

$$q''a - q(b+B) = Ap, \quad -qC = Ap', \quad q''(b-B) - qc = Ap''$$
$$-q''C = Ap''', \quad q''a - q(b-B) = Aq', \quad q''(b+B) - qc = Aq'''$$

Quo facto, facile confirmatur, F transire in productum fF per substitutionem p, p', p'', p'''; q, q', q'', q''', atque adeo ex f et F compositam esse, si modo omnes numeri p, p' etc. sint integri. Iam per descriptionem formae simplicissimae, B est vel 0 vel $\frac{1}{2}A$, adeoque $\frac{2B}{A}$ integer; indidem patet, $\frac{C}{A}$ semper esse integrum. Hinc $q'-p, p', q'''-p'', p'''$ erunt integri, superestque adeo tantummodo, ut probetur p et p'' esse integros. Fit autem

$$pp+\tfrac{2pqB}{A}=a-\tfrac{qqC}{A},\quad p''p''+\tfrac{2p''q''B}{A}=c-\tfrac{q''q''C}{A}$$

quamobrem si $B=0$, fit

$$pp=a-\tfrac{qqC}{A},\quad p''p''=c-\tfrac{q''q''C}{A}$$

et proin p, p'' integri; si vero $B=\frac{1}{2}A$, fit

$$pp+pq=a-\tfrac{qqC}{A},\quad p''p''+p''q''=c-\tfrac{q''q''C}{A}$$

unde aeque facile concluditur, p et p'' in hoc quoque casu esse integros. Ex his colligitur, F ex f et F esse compositam. *Q. E. S.*

255.

Problema itaque eo reductum est, ut omnes classes proprie primitivas determinantis D assignare oporteat, per quarum formas repraesentari potest AA. Manifesto AA repraesentari potest per quamvis formam, cuius terminus primus est vel AA vel quadratum partis aliquotae ipsius A; vice versa autem, si AA repraesentari potest per formam f, tribuendo ipsius indeterminatis valores αe, γe, quorum divisor communis maximus e, forma f per substitutionem $\alpha, \overline{\gamma}, \gamma, \delta$ transibit in formam, cuius terminus primus $\frac{AA}{ee}$, formaque haec proprie aequivalebit formae f, si $\overline{\gamma}, \delta$ ita accipiuntur ut fiat $\alpha\delta-\overline{\gamma}\gamma=1$; unde patet, in quavis classe, per cuius formas repraesentari possit AA, inveniri formas, quarum terminus primus sit AA vel quadratum partis aliquotae ipsius A. Res itaque in eo versatur, ut omnes classes proprie primitivae det. D eruantur, in quibus huiusmodi formae occurrant, quod obtinetur sequenti modo: Sint a, a', a'' etc. omnes divisores (positivi) ipsius A; investigentur omnes valores expr. $\sqrt{D}\,(\mathrm{mod}.aa)$ inter 0 et $aa-1$ incl. siti, qui sint b, b', b'' etc. statuaturque

$$bb-D=aac,\quad b'b'-D=aac',\quad b''b''-D=aac''\text{ etc.}$$

complexus formarum (aa, b, c), (aa, b', c') etc. designetur per V. Tunc facile perspicitur, in quavis classe det. D, in qua occurrat forma, cuius terminus primus aa, etiam aliquam formam ex V contentam esse debere. Simili modo eruantur omnes formae det. D, quarum terminus primus $a'a'$, medius inter 0 et $a'a'-1$ incl. situs, designeturque ipsarum complexus per V'; eademque ratione sit V''

complexus similium formarum quarum terminus primus $a''a''$ etc. Eiiciantur ex V, V', V'' etc. omnes formae, quae non sunt proprie primitivae, reducantur reliquae in classes, et, si forte plures adsint ad eandem classem pertinentes, in singulis classibus una tantum retineatur. Hoc modo omnes classes quaesitae habebuntur, eritque harum multitudo ad unitatem, ut multitudo omnium classium proprie primitivarum (positivarum) ad multitudinem classium in ordine O.

Ex. Sit $D=-531$, atque O ordo positivus derivatus ex ordine improprie primitivo det. -59, in quo forma simplicissima $(6, 3, 90)$ sive $A=6$. Hic a, a', a'', a''' erunt $1, 2, 3, 6$; V continebit formam $(1, 0, 531)$; V' has $(4, 1, 133)$, $(4, 3, 135)$; V'' has $(9, 0, 59)$, $(9, 3, 60)$, $(9, 6, 63)$; denique V''' has $(36, 3, 15)$, $(36, 9, 17)$, $(36, 15, 21)$, $(36, 21, 27)$, $(36, 27, 35)$, $(36, 33, 45)$: sed ex his duodecim formis sex sunt reiiciendae, puta ex V''' secunda et tertia, ex V''' prima, tertia, quarta et sexta, quae omnes sunt formae derivatae; sex reliquae omnes ad classes diversas pertinere inveniuntur. Revera multitudo classium proprie primitivarum (positivarum) det. -531 est 18, multitudoque classium impr. primitivarum (pos.) det. -59 (sive multitudo classium det. -531 ex his derivatarum) 3, adeoque illa ad hanc ut 6 ad 1.

256.

Solutio haec per observationes sequentes generales adhuc magis illustrabitur.

I. Si ordo O est derivatus ex ordine proprie primitivo, metietur AA ipsum D; si vero O est impr. primitivus vel ex impr. prim. derivatus, erit A par, D per $\frac{1}{4}AA$ divisibilis et quotiens $\equiv 1\,(\mathrm{mod}.4)$. Hinc quadratum cuiusvis divisoris ipsius A metietur vel ipsum D, vel saltem ipsum $4D$, et in casu posteriori quotiens semper erit $\equiv 1\,(\mathrm{mod}.4)$.

II. Si aa ipsum D metitur, omnes valores expr. $\sqrt{D}\,(\mathrm{mod}.aa)$, qui quidem inter 0 et $aa-1$ iacent, erunt $0, a, 2a \ldots aa-a$, adeoque a multitudo formarum in V; sed inter has tot tantummodo erunt proprie primitivae, quot numerorum

$$\frac{D}{aa},\ \frac{D}{aa}-1,\ \frac{D}{aa}-4\ldots\frac{D}{aa}-(a-1)^2$$

cum a divisorem communem non habent. Quando $a=1$, V ex unica forma constabit, $(1, 0, -D)$, quae semper erit proprie primitiva. Quando a est 2 vel potestas quaecunque ipsius 2, semissis illorum a numerorum par erunt, semissis impar; quare in V aderunt $\frac{1}{2}a$ formae proprie primitivae. Quando a est alius numerus primus p vel potestas numeri primi p, tres casus sunt distinguendi: scilicet, omnes illi a numeri ad a primi erunt, adeoque omnes formae in V pr. primitivae, si $\frac{D}{aa}$ per p non est divisibilis simulque non residuum quadraticum ipsius p; si vero p ipsum $\frac{D}{aa}$ metitur, in V erunt $\frac{(p-1)a}{p}$ formae pr. primitivae; denique si $\frac{D}{aa}$ est res. quadr. ipsius p per p non divisibile, in V erunt $\frac{(p-2)a}{p}$ formae pr. primitivae. Haec omnia nullo negotio demonstrantur. Generaliter autem posito $a = 2^\nu p^\pi q^\varrho r^\sigma \ldots$, designantibus p, q, r etc. numeros primos impares diversos, multitudo formarum pr. primitivarum in V erit $NPQR\ldots$, ubi statui debet

$$N = 1 \text{ (si } \nu = 0) \text{ vel } N = 2^{\nu-1} \text{ (si } \nu > 0)$$
$$P = p^\pi \text{ (si } \tfrac{D}{aa} \text{ est non-residuum quadr. ipsius } p) \text{ vel}$$
$$P = (p-1)\,p^{\pi-1} \text{ (si } \tfrac{D}{aa} \text{ per } p \text{ est divisibilis) vel}$$
$$P = (p-2)\,p^{\pi-1} \text{ (si } \tfrac{D}{aa} \text{ est res. qu. ipsius } p \text{ per } p \text{ non divisibile)}$$

Q, R etc. autem eodem modo ex q, r etc. sunt definiendi ut P ex p.

III. Si aa ipsum D non metitur, erit $\frac{4D}{aa}$ integer et $\equiv 1 \pmod 4$, valoresque expr. $\sqrt{D} \pmod{aa}$ hi $\frac{1}{2}a, \frac{3}{2}a, \frac{5}{2}a \ldots aa - \frac{1}{2}a$, unde multitudo formarum in V erit a, tot autem inter ipsas erunt proprie primitivae quot ex numeris

$$\frac{D}{aa} - \tfrac{1}{4}, \quad \frac{D}{aa} - \tfrac{3}{4}, \quad \frac{D}{aa} - \tfrac{5}{4}, \quad \ldots \quad \frac{D}{aa} - (a-\tfrac{1}{2})^2$$

ad a sunt primi. Quoties $\frac{4D}{aa} \equiv 1 \pmod 8$, omnes hi numeri erunt pares, adeoque in V nulla forma pr. primitiva; quando autem $\frac{4D}{aa} \equiv 5 \pmod 8$, omnes illi numeri erunt impares, adeoque omnes formae in V pr. primitivae, si a est 2 vel potestas ipsius 2, generaliter autem in hoc casu tot formae pr. primitivae in V erunt, quot illorum numerorum per nullum divisorem primum imparem ipsius a sunt divisibiles. Multitudo haec erit $NPQR\ldots$, si $a = 2^\nu p^\pi q^\varrho r^\sigma \ldots$, ubi statuere oportet $N = 2^\nu$, ipsos P, Q, R etc. autem eodem modo ex p, q, r etc. derivare ut in casu praecedente.

IV. Hoc itaque modo multitudines formarum pr. primitivarum in V, V', V'' etc. definiri possunt; pro aggregato omnium harum multitudinum haud difficulter eruitur sequens regula generalis: Si $A = 2^\nu \mathfrak{A}^\pi \mathfrak{B}^\varrho \mathfrak{C}^\sigma \ldots$, designantibus $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc. numeros primos impares diversos, multitudo totalis omnium formarum pr. primitivarum in V, V', V'' etc. erit $= \frac{Anabc\ldots}{2\mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots}$, ubi statui debet

$n = 1$ (si $\frac{4D}{AA} \equiv 1 \pmod 8$), vel

$n = 2$ (si $\frac{D}{AA}$ integer), vel

$n = 3$ (si $\frac{4D}{AA} \equiv 5 \pmod 8$); porro

$a = \mathfrak{A}$ (si $\mathfrak{A}$ ipsum $\frac{4D}{AA}$ metitur), vel

$a = \mathfrak{A} \pm 1$ (si $\mathfrak{A}$ ipsum $\frac{4D}{AA}$ non metitur, accipiendo signum superius vel inferius prout $\frac{4D}{AA}$ est non-residuum vel res. qu. ipsius $\mathfrak{A}$)

denique b, c etc. eodem modo ex $\mathfrak{B}, \mathfrak{C}$ derivari ut a ex $\mathfrak{A}$. Demonstrationem fusius hic explicare, brevitas non permittit.

V. Iam quod attinet ad multitudinem classium, quas suppeditant formae pr. primitivae in V, V', V'' etc., tres casus sequentes sunt distinguendi.

Primo, quando D est numerus negativus, singulae formae pr. primitivae in V, V' etc. constituent classem peculiarem, sive multitudo ipsa classium quaesitarum exprimetur per formulam in observ. praec. traditam, duobus casibus exceptis, scilicet ubi $\frac{4D}{AA}$ vel $= -4$ vel $= -3$, sive ubi D vel $= -AA$ vel $= -\frac{3}{4}AA$. Ad demonstrationem huius theorematis manifesto ostendi tantummodo debet, fieri non posse, ut duae formae diversae ex V, V', V'' etc. sint proprie aequivalentes. Supponamus itaque, (hh, i, k), $(h'h', i', k')$ esse duas formas diversas pr. primitivas ex V, V', V'' etc. ad eandem classem pertinentes, transeatque prior in posteriorem per substitutionem propriam $\alpha, \delta, \gamma, \delta$; unde habebuntur aequationes

$$\alpha\delta - \delta\gamma = 1, \quad hh\alpha\alpha + 2i\alpha\gamma + k\gamma\gamma = h'h', \quad hh\alpha\delta + i(\alpha\delta + \delta\gamma) + k\gamma\delta = i'$$

Hinc facile concluditur, *primo* γ certo non esse $= 0$ (unde sequeretur, esse $\alpha = \pm 1$, $hh = h'h'$, $i' \equiv i \pmod{hh}$ adeoque formas propositas identicas, contra

hyp.); *secundo*, γ divisibilem esse per divisorem maximum communem numerorum k, k'; (ponendo enim hunc divisorem $= r$, hic manifesto etiam metietur ipsos $2i$, $2i'$, ad k vero erit primus; praeterea rr metietur ipsum $hhk - h'k'k' = ii - i'i'$; unde facile deducitur, r etiam metiri ipsum $i - i'$; habetur autem $\alpha i' - \gamma k' = \alpha i + \gamma k$, unde γk et proin etiam γ divisibilis erit per r); *tertio*, esse $(\alpha hh + \gamma i)^2 - D\gamma\gamma = hh'k'$. Ponendo itaque $\alpha hh + \gamma i = rp$, $\gamma = rq$, p et q erunt integri quorum posterior non $= 0$, atque $pp - Dqq = \frac{hh'k'}{rr}$. Sed $\frac{hh'k'}{rr}$ erit numerus minimus per hh et $h'k'$ simul divisibilis adeoque ipsum AA et proin etiam ipsum $4D$ metietur, quare $\frac{4Drr}{hh'k'}$ erit integer (negativus), quem statuendo $= -e$, erit $pp - Dqq = -\frac{4D}{e}$ sive $4 = (\frac{2rp}{hh'})^2 + eqq$, in qua aequatione pars $(\frac{2rp}{hh'})^2$ tamquam quadratum ipso 4 minus necessario erit vel 0 vel 1. In casu priori erit $eqq = 4$, et $D = -(\frac{hh'}{rq})^2$, unde sequitur, $\frac{4D}{AA}$ esse quadratum signo negativo affectum adeoque certo non $\equiv 1 \pmod 4$, neque adeo O ordinem improprie primitivum neque ex improprie primitivo derivatum. Hinc $\frac{D}{AA}$ erit integer, unde facile deducitur, e per 4 esse divisibilem, $qq = 1$, $D = -(\frac{hh'}{r})^2$ atque etiam $\frac{AA}{D}$ integrum. Hinc necessario erit $D = -AA$ sive $\frac{D}{AA} = -1$, quae est exceptio prima. In casu posteriori erit $eqq = 3$, unde $e = 3$ et $4D = -3(\frac{hh'}{r})^2$; hinc $3(\frac{hh'}{rA})^2$ erit integer, qui, quoniam per quadratum integrum $(\frac{rA}{hh'})^2$ multiplicatus producit 3, non poterit esse alius quam 3; hinc $4D = -3AA$ sive $D = -\frac{3}{4}AA$, quae est exceptio secunda. In omnibus igitur reliquis casibus omnes formae pr. primitivae in V, V', V'' etc. ad classes diversas pertinebunt. — Pro casibus exceptis ea, quae ex disquisitione haud difficili sed hic brevitatis caussa supprimenda resultaverunt, apposuisse sufficiat. Scilicet in priori, ex formis pr. primitivis in V, V', V'' etc. binae semper ad eandem classem pertinebunt, in posteriori ternae, ita ut multitudo omnium classium quaesitarum in illo casu fiat semissis, in hoc triens valoris expressionis in obs. praec. traditae.

Secundo quando D est numerus positivus quadratus: singulae formae pr. primitivae in V, V', V'' etc. sine exceptione classem peculiarem constituunt. Supponamus enim, (hh, i, k), $(h'k', i', k')$ esse duas tales formas diversas proprie aequivalentes, transeatque prior in posteriorem per substitutionem propriam $\alpha, 6, \gamma, \delta$. Tum patet, omnia ratiocinia pro casu praec. adhibita, in quibus non supponatur D esse negativum, etiam hic valere. Designantibus itaque p, q, r

idem ut illic, etiam hic erit $\frac{4Drr}{hh'k'}$ integer, at non amplius negativus sed positivus insuperque quadratus, quo posito $= gg$, erit $(\frac{2rp}{hh'})^2 - ggqq = 4$, *Q. E. A.*, quia differentia duorum quadratorum nequit esse 4, nisi quadratum minus fuerit 0; quamobrem suppositio consistere nequit.

Pro casu *tertio* autem, ubi D est numerus positivus non quadratus, regulam generalem pro comparanda multitudine formarum pr. primitivarum in V, V', V'' etc. cum multitudine classium diversarum inde resultantium hucusque non habemus. Id quidem asserere possumus, hanc vel illi aequalem vel ipsius partem aliquotam esse; quin etiam nexum singularem inter quotientem horum numerorum et valores minimos ipsorum t, u aequationi $tt - Duu = AA$ satisfacientes deteximus, quem hic explicare nimis prolixum foret; an vero possibile sit, illum quotientem in omnibus casibus ex sola inspectione numerorum D, A cognoscere (ut in casibus praecc.), de hac re nihil certi pronunciare possumus. Ecce quaedam exempla, quorum numerum quisque facile augere poterit. Pro $D = 13$, $A = 2$, multitudo formarum pr. prim. in V etc. est 3, quae omnes sunt aequivalentes sive unicam classem efficiunt; pro $D = 37$, $A = 2$, etiam tres formae pr. prim. in V etc. habentur, quae ad tres classes diversas pertinent; pro $D = 588$, $A = 7$, habentur octo formae pr. prim. in V etc. quae efficiunt quatuor classes, pro $D = 867$, $A = 17$ in V etc. sunt 18 formae pr. primitivae, totidem pro $D = 1445$, $A = 17$, sed quae pro illo determinante in duas classes discedunt, pro hoc in sex.

VI. Ex applicatione huius theoriae generalis ad eum casum, ubi O est ordo improprie primitivus, colligitur, multitudinem classium in hoc ordine contentarum fore ad multitudinem omnium classium in ordine proprie primitivo, ut 1 ad multitudinem classium proprie primitivarum diversarum, quas hae tres formae $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ efficiunt. Et quidem hinc resultabit unica classis, quando $D \equiv 1 \pmod 8$, quia in hoc casu forma secunda et tertia sunt improprie primitivae; quando vero $D \equiv 5 \pmod 8$, illae tres formae omnes erunt proprie primitivae totidemque classes diversas producent, si D est negativus, unico casu excepto, ubi $D = -3$, in quo unicam classem constituunt; denique casus ubi D est positivus (formae $8n + 5$) ad eos pertinet, pro quibus regula generalis hactenus desideratur. Id tamen asserere possumus, illas tres formas in hoc casu

vel ad tres classes diversas pertinere vel ad unicam, numquam ad duas; facile enim perspicitur, si formae $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ resp. pertineant ad classes K, K', K'', fore $K+K'=K'$, $K'+K'=K''$, adeoque, si K et K' identicae esse supponantur, etiam K' et K'' identicas fore; simili ratione si K et K'' supponuntur esse identicae, etiam K' et K'' erunt; denique quum sit $K'+K''=K$, ex suppositione, K' et K'' identicas esse, sequitur, etiam K et K'' coincidere; unde colligitur, vel omnes tres classes K, K', K'' esse diversas, vel omnes tres identicas. *E. g.* infra 600 dantur 75 numeri formae $8n+5$, inter quos sunt 16 determinantes pro quibus casus prior locum habet sive multitudo classium in ordine pr. primitivo ter maior est quam in impr. primitivo, puta 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573; pro 59 reliquis casus posterior valet, sive multitudo classium in utroque ordine est aequalis.

VII. Vix opus erit, observare, per disquisitionem praecedentem non solum multitudines classium in ordinibus diversis eiusdem determinantis comparari posse, sed illam etiam ad quosvis determinantes diversos qui rationem quadratorum inter se teneant esse applicabilem. Scilicet designante O ordinem quemcunque det. dmm, O' ordinem det. $dm'm'$, O comparari poterit cum ordine proprie primitivo det. dmm, atque hic cum ordine derivato ex ordine pr. prim. det. d, sive, quod respectu multitudinis classium eodem redit, cum hoc ordine ipso; et cum eodem prorsus simili ratione comparari poterit ordo O'.

De multitudine classium ancipitum.

257.

Inter omnes classes in ordine dato determinantis dati imprimis classes ancipites disquisitionem uberiorem postulant, determinatioque multitudinis harum classium ad multa alia viam nobis aperiet. Sufficit autem, hanc multitudinem in solo ordine pr. primitivo assignare, quum casus reliqui ad hunc facile reduci possint. Hoc negotium ita absolvemus, ut primo omnes formas ancipites pr. primitivas (A, B, C) determinantis propositi D, in quibus vel $B=0$ vel $B=\frac{1}{2}A$, eruere; tunc ex harum multitudine multitudinem omnium classium ancipitum pr. primitivarum det. D invenire doceamus.

I. Omnes formae pr. primitivae $(A, 0, C)$ determinantis D manifesto inveniuntur, accipiendo pro A singulos divisores ipsius D (tum positive tum negative) pro quibus $C=-\frac{D}{A}$ fit primus ad A. Quando itaque $D=1$, duae huiusmodi formae dantur $(1, 0, -1)$, $(-1, 0, 1)$; totidem quando $D=-1$, puta $(1, 0, 1)$, $(-1, 0, -1)$; quando D est numerus primus aut numeri primi potestas (sive signo positivo sive negativo), quatuor dabuntur $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. Generaliter autem, quando D per n numeros primos diversos est divisibilis (inter quos hoc loco etiam 2 in computum ingredi debet): dabuntur omnino 2^{n+1} huiusmodi formae; scilicet posito $D=\pm PQR\ldots$, designantibus P, Q, R etc. numeros primos diversos aut numerorum primorum diversorum potestates, quorum multitudo $=n$, valores ipsius A erunt $1, P, Q, R$ etc. atque producta ex quotcunque horum numerorum; horum valorum multitudo fit per theoriam combinationum 2^n, sed duplicanda est, quoniam singulis valoribus tum signum positivum tum negativum tribuere oportet.

II. Simili modo patet, omnes formas pr. primitivas $(2B, B, C)$ determinantis D obtineri, si pro B accipiantur omnes divisores ipsius D (positive et negative), pro quibus $C=\frac{1}{2}(B-\frac{D}{B})$ fit integer et ad $2B$ primus. Quum itaque C necessario debeat esse impar, adeoque $CC\equiv 1 \pmod 8$, ex $D=BB-2BC=(B-C)^2-CC$ sequitur, D esse vel $\equiv 3 \pmod 4$, quando B impar, vel $\equiv 0 \pmod 8$, quando B par; quoties itaque D alicui numerorum $1, 2, 4, 5, 6$ sec. mod. 8 est congruus, nullae huiusmodi formae dabuntur. Quando $D\equiv 3 \pmod 4$, C fit integer et impar, quicunque divisor ipsius D pro B accipiatur; ne vero C divisorem comm. cum $2B$ habeat, B ita accipi debebit, ut $\frac{D}{B}$ ad B fiat primus; hinc pro $D=-1$ duae formae habentur $(2, 1, 1)$, $(-2, -1, -1)$, generaliterque facile perspicitur, si multitudo omnium numerorum primorum ipsum D metientium sit n, omnino emergere 2^{n+1} formas. — Quando D per 8 est divisibilis, C fit integer, accipiendo pro B divisorem quemcunque parem ipsius $\frac{1}{2}D$; conditioni alteri autem, ut $C=\frac{1}{2}B-\frac{D}{2B}$ ad $2B$ sit primus, satisfit *primo*, accipiendo pro B omnes divisores impariter pares ipsius D, pro quibus $\frac{D}{B}$ cum B divisorem communem non habet, quorum multitudo (habita ratione diversitatis signorum) erit 2^{n+1}, si D per n numeros primos impares diversos divisibilis esse supponitur; *secundo*, accipiendo pro B omnes divisores pariter pares ipsius

$\frac{1}{2}D$, pro quibus $\frac{D}{2^{\mu}B}$ fit primus ad B, quorum multitudo quoque erit 2^{n+1}, ita ut in hoc casu omnino habeantur 2^{n+2} huiusmodi formae. Scilicet ponendo $D = \pm 2^{\mu} PQR\ldots$, designante μ exponentem maiorem quam 2; P, Q, R numeros primos impares diversos aut talium numerorum primorum potestates quorum multitudo n: *tum* pro $\frac{1}{2}B$, *tum* pro $\frac{D}{2^{\mu}B}$ accipi possunt valores 1, P, Q, R etc. productaque ex quotcunque horum numerorum, signo et positivo et negativo.

Ex his omnibus colligitur, si D per n numeros primos impares diversos divisibilis supponatur (statuendo $n = 0$, quando $D = \pm 1$ aut ± 2 aut potestas binarii), multitudinem omnium formarum pr. primitivarum (A, B, C), in quibus B vel 0 vel $\frac{1}{2}A$, fore 2^{n+1} quando D aut $\equiv 1$ aut $\equiv 5 \pmod 8$; 2^{n+2} quando $D \equiv 2, 3, 4, 6$ aut $7 \pmod 8$; denique 2^{n+3} quando $D \equiv 0 \pmod 8$. Quam comparando cum iis quae in art. 231 pro multitudine omnium characterum possibilium formarum primitivarum det. D tradidimus, observamus, illam in omnibus casibus praecise esse duplo hac maiorem. Ceterum manifestum est, quando D sit negativus, inter illas formas totidem positivas affore quot negativas.

258.

Omnes formae in art. praec. erutae manifesto pertinent ad classes ancipites, et vice versa in quavis classe ancipite pr. primitiva det. D saltem una illarum formarum contenta esse debet; in tali enim classe certo adsunt formae ancipites et cuivis formae ancipiti pr. primitivae (a, b, c) det. D aliqua formarum art. praec. aequivalet, scilicet vel

$$(a, 0, -\tfrac{D}{a}) \quad \text{vel} \quad (a, \tfrac{1}{2}a, \tfrac{1}{4}a - \tfrac{D}{a})$$

prout b vel $\equiv 0$ vel $\equiv \frac{1}{2}a \pmod a$. Problema itaque eo reductum est, ut quot classes diversas illae formae constituant, investigemus.

Si forma $(a, 0, c)$ est inter formas art. praec., forma $(c, 0, a)$ inter easdem occurret et ab illa semper erit diversa, unico casu excepto, ubi $a = c = \pm 1$ adeoque $D = -1$, quem aliquantisper seponemus. Quoniam vero hae formae manifesto ad eandem classem pertinent, sufficit unam retinere, et quidem reiiciemus eam, cuius terminus primus est maior quam tertius; eum casum, ubi $a = -c = \pm 1$ sive $D = 1$ quoque seponemus. Hoc modo omnes formas

$(A, 0, C)$ ad semissem reducere possumus, retinendo e binis semper unam; et in omnibus remanentibus erit $A < \sqrt{\pm D}$.

Simili modo si inter formas art. praec. occurrit forma $(2b, b, c)$, inter easdem reperietur

$$(4c - 2b,\ 2c - b, c) = (-\tfrac{2D}{b}, -\tfrac{D}{b}, c)$$

quae illi proprie aequivalens et ab ipsa diversa erit, unico quem seponimus casu excepto, ubi $c = b = \pm 1$ sive $D = -1$. Ex his duabus formis eam retinere sufficit, cuius terminus primus est minor quam terminus primus alterius (magnitudine aequales, signis diversi in hoc casu esse nequeunt); unde patet, etiam omnes formas $(2B, B, C)$ ad semissem reduci posse, e binis unam semper eiiciendo; et in remanentibus esse $B < \frac{D}{B}$ sive $B < \sqrt{\pm D}$. Hoc modo ex omnibus formis art. praec. semissis tantum remanet, quarum complexum per W designabimus, nihilque superest, nisi ut ostendamus, quot classes diversae ex his formis oriantur. Ceterum manifestum est, in eo casu ubi D sit negativus, totidem formas positivas in W affore quot negativas.

I. Quando D est negativus, singulae formae in W pertinebunt ad classes diversas. Nam omnes formae $(A, 0, C)$ erunt reductae; similiter omnes formae $(2B, B, C)$ reductae erunt, praeter eas in quibus $C < 2B$; in tali vero forma erit $2C < 2B + C$; unde (quoniam $B < \frac{D}{B}$ *i. e.* $B < 2C - B$, adeoque $2B < 2C$, sive $B < C$), $2C - 2B < C$ et $C - B < \frac{1}{2}C$ et proin $(C, C - B, C)$, quae manifesto illi aequivalet, forma reducta. Hoc modo totidem formae reductae habentur, quot formae habentur in W, et quum facile perspiciatur, inter illas neque identicas neque oppositas occurrere posse, (unico casu excepto, ubi $C - B = 0$, in quo erit $B = C = \pm 1$, adeoque $D = -1$, quem iam seposuimus): omnes ad classes diversas pertinebunt. Hinc colligitur, multitudinem omnium classium ancipitum pr. primitivarum det. D multitudini formarum in W seu semissi multitudinis formarum art. praec. aequalem esse; in casu excepto autem $D = -1$ per compensationem idem evenit, scilicet duae classes habentur, ad quarum alteram pertinent formae $(1, 0, 1)$, $(2, 1, 1)$, ad alteram hae $(-1, 0, -1)$, $(-2, -1, -1)$. Generaliter itaque pro determinante negativo multitudo omnium classium ancipitum pr. prim. aequalis est multitudini omnium

characterum assignabilium formarum primitivarum huius determinantis; multitudo classium ancipitum pr. prim. positivarum autem semissis erit.

II. Quando D est positivus quadratus $= hh$, haud difficile demonstratur, singulas formas in W ad classes diversas pertinere; sed pro hoc casu ad problematis solutionem adhuc brevius sequenti modo pervenire possumus. Quum per art. 210 in quavis classe ancipite pr. prim. det. hh, neque in ulla alia, contineatur forma reducta una $(a, h, 0)$, in qua a est valor expr. $\sqrt{1} \pmod{2h}$ inter 0 et $2h-1$ incl. situs: perspicuum est, totidem classes ancipites pr. prim. det. hh dari, quot valores expressio illa habeat. Ex art. 105 autem nullo negotio deducitur, multitudinem horum valorum esse 2^n vel 2^{n+1} vel 2^{n+2}, prout h sit impar vel impariter par vel pariter par, sive prout $D \equiv 1$ vel $\equiv 4$ vel $\equiv 0 \pmod 8$, designante n multitudinem divisorum primorum imparium ipsius h sive ipsius D. Hinc colligitur, multitudinem classium ancipitum pr. prim. semper esse semissem multitudinis omnium formarum in art. praec. erutarum, sive multitudini formarum in W vel omnium characterum possibilium aequalem.

III. Quando D est positivus non-quadratus, ex singulis formis (A, B, C) in W contentis alias deducamus (A, B', C'), accipiendo $B' \equiv B \pmod A$ et inter limites $\sqrt{D}$ et $\sqrt{D} \mp A$ (ubi signum superius vel inferius adhibendum, prout A est pos. vel neg.) atque $C' = \frac{B'B'-D}{A}$; designemusque harum complexum per W'. Manifesto hae formae erunt proprie primitivae ancipites det. D, atque omnes inter se diversae: praeterea vero omnes erunt formae reductae. Quando enim $A < \sqrt{D}$, B' manifesto erit $< \sqrt{D}$ atque positivus; praeterea $B' > \sqrt{D} \mp A$ adeoque $A > \sqrt{D} - B'$ et proin A, positive acceptus, certo inter $\sqrt{D} + B'$ et $\sqrt{D} - B'$ situs. Quando vero $A > \sqrt{D}$, non poterit esse $B = 0$ (quippe quas formas eiecimus), sed erit necessario $B = \frac{1}{2}A$; hinc B' magnitudine ipsi $\frac{1}{2}A$ aequalis, signo positivus (quoniam enim $A < 2\sqrt{D}$, $\pm \frac{1}{2}A$ iacebit inter limites ipsi B' assignatos, ipsique B sec. mod. A erit congruus; quare $B' = \pm \frac{1}{2}A$), proin $B' < \sqrt{D}$, unde $2B' < \sqrt{D} + B'$ sive $A < \sqrt{D} + B'$, quamobrem $\pm A$ necessario inter limites $\sqrt{D} + B'$ et $\sqrt{D} - B'$ iacebit. Denique W' omnes formas reductas pr. prim. ancipites det. D continebit; si enim (a, b, c) est huiusmodi forma, erit vel $b \equiv 0$, vel $b \equiv \frac{1}{2}a \pmod a$. In casu priori manifesto non poterit esse $b < a$ neque adeo $a > \sqrt{D}$, quapropter forma $(a, 0, -\frac{D}{a})$ certo contenta

erit in W, et respondens (a, b, c) in W'; in posteriori certo erit $a < 2\sqrt{D}$, adeoque $(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a})$ in W contenta, atque respondens (a, b, c) in W'. Ex his colligitur, multitudinem formarum in W aequalem esse multitudini omnium formarum reductarum ancipitum pr. prim. det. D; quoniam vero in singulis classibus ancipitibus *binae* formae reductae ancipites continentur (artt. 187, 194), multitudo omnium classium ancipitum pr. prim. det. D erit semissis multitudinis formarum in W, sive semissis multitudinis omnium characterum assignabilium.

259.

Multitudo classium ancipitum improprie primitivarum determinantis dati D multitudini proprie primitivarum eiusdem det. semper est aequalis. Sit K classis principalis, atque K', K'' etc. reliquae classes ancipites pr. primitivae huius determinantis; L aliqua classis anceps improprie primitiva eiusdem det., *e. g.* ea in qua est forma $(2, 1, \frac{1}{4} - \frac{1}{4}D)$. Prodibit itaque ex compositione classis L cum K classis L ipsa; ex compositione classis L cum K', K'' etc. provenire supponamus classes L', L'' etc. resp., quae manifesto omnes ad eundem determinantem D pertinebunt, atque improprie primitivae et ancipites erunt. Patet itaque, theorema demonstratum fore, simulac probatum fuerit, omnes classes L, L', L'' etc. esse diversas, aliasque ancipites impr. prim. det. D praeter illas non dari. Ad hunc finem sequentes casus distinguimus:

I. Quando multitudo classium impr. primitivarum multitudini pr. primitivarum aequalis est, quaevis illarum oritur ex compositione classis L cum classe determinata proprie primitiva, unde necessario omnes L, L', L'' etc. erunt diversae. Designante autem $\mathfrak{L}$ classem quamcunque ancipitem impr. prim. det. D, dabitur classis proprie primitiva $\mathfrak{K}$ talis ut sit $\mathfrak{K} + L = \mathfrak{L}$; si classi $\mathfrak{K}$ opposita est classis $\mathfrak{K}'$, erit etiam (quoniam classes L, $\mathfrak{L}$ sibi ipsae oppositae sunt) $\mathfrak{K}' + L = \mathfrak{L}$, unde necessario $\mathfrak{K}$ cum $\mathfrak{K}'$ identica erit, adeoque classis anceps: hinc $\mathfrak{K}$ reperietur inter classes K, K', K'' etc. atque $\mathfrak{L}$ inter has L, L', L'' etc.

II. Quando multitudo classium improprie primitivarum ter minor est quam multitudo classium pr. primitivarum, sit H classis in qua est forma $(4, 1, \frac{1-D}{4})$, H' ea in qua est forma $(4, 3, \frac{9-D}{4})$, eruntque H, H' proprie primitivae et tum

inter se tum a classe principali K diversae, atque $H+H'=K$; $2H=H'$, $2H'=H$; et si $\mathfrak{L}$ est classis quaecunque improprie primitiva det. D, quae oritur ex compositione classis L cum proprie primitiva $\mathfrak{K}$, erit etiam $\mathfrak{L}=L+\mathfrak{K}+H$ et $\mathfrak{L}=L+\mathfrak{K}+H'$; praeter tres classes (pr. prim. atque diversas) $\mathfrak{K}$, $\mathfrak{K}+H$, $\mathfrak{K}+H'$ aliae non dabuntur, quae cum L compositae ipsam $\mathfrak{L}$ producant. Quoniam igitur, si $\mathfrak{L}$ est anceps atque $\mathfrak{K}'$ ipsi $\mathfrak{K}$ opposita, etiam $L+\mathfrak{K}'=\mathfrak{L}$, necessario $\mathfrak{K}'$ cum aliqua illarum trium classium identica erit. Si $\mathfrak{K}'=\mathfrak{K}$, erit $\mathfrak{K}$ anceps; si $\mathfrak{K}'=\mathfrak{K}+H$, erit $K=\mathfrak{K}+\mathfrak{K}'=2\mathfrak{K}+H=2(\mathfrak{K}+H')$, adeoque $\mathfrak{K}+H'$ anceps; similiterque si $\mathfrak{K}'=\mathfrak{K}+H'$, erit $\mathfrak{K}+H$ anceps, unde concluditur, $\mathfrak{L}$ inter classes L, L', L'' etc. necessario reperiri. Facile autem perspicitur, inter tres classes $\mathfrak{K}$, $\mathfrak{K}+H$, $\mathfrak{K}+H'$ plures ancipites esse non posse; si enim tum $\mathfrak{K}$ tum $\mathfrak{K}+H$ ancipites essent sive cum oppositis suis $\mathfrak{K}'$, $\mathfrak{K}'+H'$ resp. identicae, foret $\mathfrak{K}+H=\mathfrak{K}+H'$; eadem conclusio resultat ex suppositione, $\mathfrak{K}$ et $\mathfrak{K}+H'$ esse ancipites; denique si $\mathfrak{K}+H$, $\mathfrak{K}+H'$ ancipites sive cum oppositis suis $\mathfrak{K}'+H'$, $\mathfrak{K}'+H$ identicae essent, fieret $\mathfrak{K}+H+\mathfrak{K}'+H=\mathfrak{K}'+H'+\mathfrak{K}+H'$, unda $2H=2H'$, sive $H'=H$. Quamobrem unica tantum classis anceps pr. prim. dabitur, quae cum L composita ipsam $\mathfrak{L}$ producit, adeoque omnes L, L', L'' etc. erunt diversae.

Multitudo classium ancipitum in ordine *derivato* manifesto aequalis est multitudini classium ancipitum in ordine primitivo, ex quo est derivatus, adeoque per praecedentia semper poterit assignari.

260.

Problema. *Classis proprie primitiva K determinantis D oritur ex duplicatione classis proprie primitivae k eiusdem determinantis: quaeruntur omnes similes classes, ex quarum duplicatione classis K oritur.*

Sol. Sit H classis principalis det. D atque H', H'', H''' etc. reliquae classes ancipites pr. primitivae eiusdem determinantis; classes quae ex harum compositione cum k oriuntur, $k+H'$, $k+H''$, $k+H'''$ designentur per k', k'', k''' etc. Tunc omnes classes k, k', k'' etc. erunt pr. primitivae det. D et inter se diversae; aeque facile perspicitur, ex singularum duplicatione oriri classem K. Denotante autem $\mathfrak{K}$ classem quamcunque pr. prim. det. D, quae duplicata producit classem K, necessario inter classes k, k', k'' etc. contenta erit. Ponatur enim $\mathfrak{K}=k+\mathfrak{H}$, ita ut $\mathfrak{H}$ sit classis pr. prim. det. D (art. 249), eritque

$2k+2\mathfrak{H}=2\mathfrak{K}=K=2k$, unde facile concluditur, $2\mathfrak{H}$ coincidere cum classe principali, $\mathfrak{H}$ esse ancipitem sive inter H, H', H'' etc. contentam, atque $\mathfrak{K}$ inter k, k', k'' etc.; quamobrem hae classes completam problematis solutionem exhibent.

Ceterum manifestum est, in eo casu, ubi D sit negativus, e classibus k, k', k'' etc. semissem fore classes positivas, semissem negativas.

Quum igitur quaevis classis pr. prim. det. D, quae ex ullius classis similis duplicatione oriri potest, omnino ex totidem classium similium duplicatione proveniat, quot classes ancipites pr. prim. det. D dantur: perspicuum est, si multitudo cunctarum classium pr. prim. det. D sit r, multitudo omnium classium ancipitum pr. prim. huius det. n, multitudinem omnium classium pr. prim. eiusdem det. quae ex duplicatione similis classis produci possint, fore $\frac{r}{n}$. Eadem formula resultat, si, pro det. negativo, characteres r, n multitudinem classium *positivarum* designant, ille *omnium* pr. prim., hic solarum ancipitum. Ita *e. g.* pro $D=-161$ multitudo omnium classium pr. prim. positivarum est 16, multitudo ancipitum 4, unde multitudo omnium classium, quae per duplicationem alicuius classis oriri possunt, debebit esse 4. Et revera invenitur, omnes classes in genere principali contentas hac proprietate esse praeditas; scilicet classis principalis $(1, 0, 161)$ oritur ex duplicatione quatuor classium ancipitum; $(2, 1, 81)$ ex duplicatione classium $(9, 1, 18)$, $(9, -1, 18)$, $(11, 2, 15)$, $(11, -2, 15)$; $(9, 1, 18)$ ex dupl. classium $(3, 1, 54)$, $(6, 1, 27)$, $(5, -2, 33)$, $(10, 3, 17)$; denique $(9, -1, 18)$ ex duplicatione classium $(3, -1, 54)$, $(6, -1, 27)$, $(5, 2, 33)$, $(10, -3, 17)$.

Certe semissi omnium characterum pro determinante dato assignabilium genera proprie primitiva (positiva pro det. neg.) respondere nequeunt.

261.

Theorema. *Semissi omnium characterum assignabilium pro determinante positivo non-quadrato nulla genera proprie primitiva respondere possunt; pro determinante negativo autem nulla genera proprie primitiva positiva.*

Dem. Sit m multitudo omnium generum proprie primitivorum (positivorum) determinantis D; k multitudo classium in singulis generibus contentarum, ita ut km sit multitudo omnium classium proprie primitivarum (positivarum); n multitudo omnium characterum diversorum pro hoc det. assignabilium. Tunc

per art. 258 multitudo omnium classium ancipitum (positivarum) pr. primitivarum erit $\frac{1}{2}n$; hinc per art. praec. multitudo omnium classium pr. prim., quae ex duplicatione similis classis oriri possunt, erit $\frac{2km}{n}$. Sed per art. 247 hae classes omnes pertinent ad genus principale, in quo continentur k classes; si itaque omnes classes generis principalis ex duplicatione alicuius classis provenire possunt (quod revera semper locum habere in sequentibus demonstrabitur), erit $\frac{2km}{n} = k$, sive $m = \frac{1}{2}n$; certo autem nequit esse $\frac{2km}{n} > k$ neque adeo $m > \frac{1}{2}n$. Quoniam itaque multitudo omnium generum pr. prim. (positivorum) certo non est maior quam semissis omnium characterum assignabilium: ad minimum horum semissi talia genera respondere nequeunt. *Q. E. D.* — Ceterum probe notandum est, hinc nondum sequi, semissi omnium characterum assignabilium revera respondere genera pr. prim. (positiva), sed huius propositionis gravissimae veritas infra demum e reconditissimis numerorum mysteriis enodari poterit.

Quum pro determinante negativo totidem genera negativa semper exstent quot positiva, manifesto ex omnibus characteribus assignabilibus non plures quam semissis generibus pr. prim. negativis competere possunt, de qua re ut et de generibus impr. prim. infra loquemur. Denique observamus, theorema ad determinantes positivos quadratos non extendi, pro quibus nullo negotio perspicitur singulis characteribus assignabilibus genera revera respondere.

Theorematis fundamentalis et reliquorum theorematum ad residua $-1, +2, -2$ pertinentium demonstratio secunda.

262.

In eo itaque casu, ubi pro determinante non-quadrato dato D duo tantummodo characteres diversi assignari possunt, unico tantum genus pr. primitivum (positivum) respondebit, (quod non poterit esse aliud quam genus principale), alter nulli formae pr. prim. (pos.) illius determinantis competet. Hoc evenit pro determinantibus -1, 2, -2, -4, numeris primis formae $4n+1$ positive, iisque formae $4n+3$ negative acceptis, denique pro omnibus numerorum primorum formae $4n+1$ potestatibus exponentis imparis positive sumtis, et pro potestatibus numerorum primorum formae $4n+3$ positive vel negative sumtis prout exponentes sunt pares vel impares. Ex hoc principio methodum novam haurire possumus, non modo theorema fundamentale, sed etiam reliqua theoremata Sect. praec. ad residua $-1, +2, -2$ pertinentia demonstrandi, quae a methodis in

Sect. praec. adhibitis omnino est diversa, elegantiaque his nentiquam inferior aestimanda videtur. Determinantem -4 autem, et qui sunt numerorum primorum potestates, quum nihil novi doceant, praeteribimus.

Pro determinante -1 itaque nulla forma positiva datur, cuius character sit $3, 4$; pro determinante $+2$ nulla omnino forma, cuius character sit $3 et 5, 8$; pro determinante -2 nulli formae positivae competet character $5 et 7, 8$; pro determinante $+p$, si p est numerus primus formae $4n+1$, vel pro determinante $-p$, si p est numerus primus formae $4n+3$, nulli formae pr. pr. (positivae in casu post.) competet character Np. Hinc theoremata Sect. praec. sequenti modo demonstramus:

I. Est -1 non-residuum cuiusvis numeri (positivi) formae $4n+3$. Si enim -1 residuum talis numeri A esset, faciendo $-1 = BB - AC$, foret (A, B, C) forma positiva det. -1, cuius character $3, 4$.

II. Est -1 residuum cuiusvis numeri primi p formae $4n+1$. Nam character formae $(-1, 0, p)$, sicuti omnium proprie primitivarum det. p, erit Rp, adeoque $-1\,Rp$.

III. Tum $+2$ tum -2 est residuum cuiusvis numeri primi p formae $8n+1$. Nam vel formae $(8, 1, \frac{1-p}{8})$, $(-8, 1, \frac{p-1}{8})$, vel hae $(8, 3, \frac{9-p}{8})$, $(-8, 3, \frac{p-9}{8})$ erunt proprie primitivae (prout n impar vel par), adeoque ipsarum character Rp: hinc $+8\,Rp$ et $-8\,Rp$, unde etiam $2Rp$, $-2Rp$.

IV. Est $+2$ non-residuum cuiusvis numeri formae $8n+3$ aut $8n+5$. Si enim esset residuum talis numeri A, daretur forma (A, B, C) determinantis $+2$, cuius character $3 et 5, 8$.

V. Simili modo -2 est non-residuum cuiusvis numeri formae $8n+5$ aut $8n+7$, alioquin enim daretur forma (A, B, C) determinantis -2, cuius character $5 et 7, 8$.

VI. Est -2 residuum cuiusvis numeri primi p formae $8n+3$. Hanc propositionem per methodum duplicem demonstrare licet. *Primo*, quum per IV sit $+2\,Np$, atque per I. $-1\,Np$, necessario erit $-2\,Rp$. Demonstratio *secunda* petitur ex consideratione determinantis $+2p$, pro quo quatuor characteres sunt assignabiles, puta Rp, $1 et 3, 8$; Rp, $5 et 7, 8$; Np, $1 et 3, 8$; Np, $5 et 7, 8$, ex quibus igitur saltem duobus nulla genera respondebunt. Iam formae

$(1, 0, -2p)$ competit character primus; formae $(-1, 0, 2p)$ quartus; quare qui reiici debent sunt secundus atque tertius. Quum itaque character formae $(p, 0, -2)$ relative ad numerum 8 sit 1 *et* $3, 8$, ipsius character relative ad p non poterit esse alius quam Rp, unde $= 2Rp$.

VII. Est $+2$ residuum cuiusvis numeri primi p formae $8n+7$, quod per methodum duplicem demonstrare licet. *Primo*, quum ex I et V sit $-1Np$, $-2Np$, erit $+2Rp$. *Secundo* quum vel $(8, 1, \frac{1+p}{8})$ vel $(8, 3, \frac{3+p}{8})$ sit forma proprie primitiva determinantis $-p$ (prout n par vel impar), ipsius character erit Rp, adeoque $8Rp$ et $2Rp$.

VIII. Quilibet numerus primus p formae $4n+1$ est non-residuum cuiusvis numeri imparis q, qui ipsius p non-residuum est. Patet enim, si p esset residuum ipsius q, dari formam proprie primitivam determinantis p, cuius character Np.

IX. Simili modo si numerus quicunque impar q est non-residuum numeri primi p formae $4n+3$, erit $-p$ non-residuum ipsius q; alioquin enim daretur forma positiva pr. primitiva determinantis $-p$ cuius character Np.

X. Quivis numerus primus p formae $4n+1$ est residuum cuiusvis alius numeri primi q, qui ipsius p residuum est. Si etiam q est formae $4n+1$, hoc statim sequitur ex VIII; si vero q est formae $4n+3$, erit etiam $-q$ residuum ipsius p (propter II) adeoque pRq (ex IX).

XI. Si numerus quicunque primus q est residuum alius numeri primi p formae $4n+3$, erit $-p$ residuum ipsius q. Si enim q est formae $4n+1$; ex VIII sequitur pRq, adeoque (per II), $-pRq$; casus autem ubi etiam q est formae $4n+3$, huic methodo se subducit, attamen facile ex consideratione determinantis $+pq$ absolvi potest. Scilicet quum ex quatuor characteribus pro hoc determinante assignabilibus Rp, Rq; Rp, Nq; Np, Rq; Np, Nq duobus nulla genera respondere possint, atque formarum $(1, 0, -pq)$, $(-1, 0, pq)$ characteres respective sint primus et quartus, character secundus et tertius nulli formae pr. prim. det. pq competere possunt. Quum itaque character formae $(q, 0, -p)$ resp. numeri p per hyp. sit Rp, eiusdem formae character respectu numeri q debet esse Rq, adeoque $-pRq$. *Q. E. D.*

Si in proposs. VIII et IX, q supponitur designare numerum primum, hae cum X et XI iunctae theorema fundamentale Sect. praec. exhibent.

Ea characterum semissis, quibus genera respondere nequeunt, propius determinantur.

263.

Postquam theorema fundamentale demonstratione nova comprobavimus, eam characterum semissem, quibus nullae formae pr. primitivae (positivae) respondere possunt, pro determinante quocunque non-quadrato dato discernere ostendemus, quod negotium eo brevius absolvere licebit, quum ipsius fundamentum iam in disquisitione artt. 147—150 sit contentum. Sit ee quadratum maximum, determinantem propositum D metiens, atque $D = D'ee$, ita ut D' nullum factorem quadratum implicet; porro sint a, b, c etc. omnes divisores primi impares ipsius D', adeoque D' sine respectu signi sui vel productum ex his numeris vel duplum huius producti. Designetur per Ω complexus characterum particularium Na, Nb, Nc etc., solus, quando $D' \equiv 1 \pmod 4$; adiuncto charactere $3, 4$, quando $D' \equiv 3$ atque e impar aut impariter par; adiunctis his $3, 8$ atque $7, 8$, quando $D' \equiv 3$ atque e pariter par; adiuncto vel charactere 3 *et* $5, 8$, vel duobus $3, 8$ atque $5, 8$, quando $D' \equiv 2 \pmod 8$ atque e vel impar vel par; denique adiuncto vel charactere 5 *et* $7, 8$, vel duobus $5, 8$ atque $7, 8$, quando $D' \equiv 6 \pmod 8$ atque e vel impar vel par. His ita factis, omnibus characteribus integris, in quibus multitudo impar characterum particularium Ω continetur, nulla genera proprie primitiva (positiva) determinantis D respondere poterunt. In omnibus casibus characteres particulares, qui exprimunt relationem ad tales divisores primos ipsius D, qui ipsum D' non metiuntur, ad generum possibilitatem vel impossibilitatem nihil conferunt. — Ex theoria combinationum autem facillime perspicitur, hoc modo revera semissem omnium characterum integrorum assignabilium excludi.

Demonstratio horum praeceptorum adornatur sequenti modo. E principiis Sect. praec., sive theorematibus in art. praec. denuo demonstratis nullo negotio deducitur, si p sit numerus primus (impar positivus) ipsum D non metiens, cui aliquis e characteribus reiectis competat, D' implicare multitudinem imparem factorum, qui sint non-residua ipsius p, atque adeo D', et hinc etiam D, esse non-residuum ipsius p; porro facile perspicitur, productum e numeris quotcunque imparibus ad D primis, quorum nulli aliquis characterum reiectorum competat, etiam cum tali charactere consentire non posse; hinc vice versa perspicuum est, quemvis numerum imparem positivum ad D primum, cui aliquis characte-

rum reiectorum conveniat, certe aliquem factorem primum eiusdem qualitatis implicare, adeoque D ipsius non-residuum esse. Si itaque forma proprie primitiva (positiva) determinantis D daretur, alicui characterum reiectorum respondens, D foret non-residuum cuiusvis numeri positivi imparis ad ipsum primi per talem formam repraesentabilis, quod manifesto cum theoremate art. 154 consistere nequit.

Tamquam exempla conferantur classificationes in artt. 231, 232 traditae, quarum numerum quisque pro lubitu augere poterit.

264.

Hoc itaque modo pro quovis determinante non-quadrato dato omnes characteres assignabiles in duas species P, Q aequaliter distribuuntur, ita ut nulli characterum Q forma proprie primitiva (positiva) respondere possit, reliquis autem P, quantum quidem hucusque novimus, nihil obstet, quominus ad tales formas pertineant. Circa has characterum species notetur imprimis propositio sequens, quae ex ipsarum criterio facile deducitur: Si character ex P cum charactere ex Q componitur (ad normam art. 246 perinde ac si etiam huic genus responderet) prodibit character ex Q; si vero duo characteres ex P, vel duo ex Q componuntur, character resultans ad P pertinebit. Adiumento huius theorematis etiam pro generibus negativis atque improprie primitivis semissis omnium characterum assignabilium excludi potest sequenti modo.

I. Pro determinante negativo D genera negativa positivis hoc respectu prorsus contraria erunt, scilicet nullus characterum P pertinebit ad genus proprie primitivum negativum, sed haec genera omnia habebunt characteres ex Q. Quando enim $D' \equiv 1 \pmod 4$, erit $-D'$ numerus positivus formae $4n+3$, adeoque inter a, b, c etc. multitudo impar numerorum formae $4n+3$, quorum singulorum non-residuum erit -1, unde patet, in characterem integrum formae $(-1, 0, D)$ in hoc casu ingredi multitudinem imparem characterum particularium ex Ω, sive illum pertinere ad Q; quando $D' \equiv 3 \pmod 4$, ex simili ratione inter a, b, c etc. vel nullus numerus formae $4n+3$ reperietur, vel duo, vel quatuor etc., sed quum vel 3, 4 vel 3, 8 vel 7, 8 in hoc casu occurrat inter characteres particulares formae $(-1, 0, D)$, patet, characterem integrum huius formae etiam hic pertinere ad Q. Eadem conclusio aeque facile in casibus reliquis

obtinetur, ita ut forma negativa $(-1, 0, D)$ semper habeat characterem ex Q. Sed quoniam haec forma cum quacunque alia pr. primitiva negativa eiusdem det. composita similem formam positivam producit, facile perspicitur, nullam formam pr. prim. negativam characterem ex P habere posse.

II. Pro generibus improprie primitivis (positivis) simili modo probatur, rem vel eodem modo se habere ut in proprie primitivis, vel contrario, prout $D \equiv 1$ vel $\equiv 5 \pmod 8$. Nam in casu priori erit etiam $D' \equiv 1 \pmod 8$, unde facile concluditur, inter numeros a, b, c etc. vel nullum numerum formae $8n+3$ et $8n+5$ reperiri vel duos vel quatuor etc. (scilicet productum ex quotcunque numeris imparibus, inter quos numeri formae $8n+3$ et $8n+5$ coniunctim multitudinem imparem efficiunt, semper evadit vel $\equiv 3$ vel $\equiv 5 \pmod 8$), productum autem ex omnibus a, b, c etc. aequale esse debet vel ipsi D' vel ipsi $-D'$); hinc patet, characterem integrum formae $(2, 1, \frac{1-D}{2})$ involvere vel nullum characterem particularem ex Ω, vel duos vel quatuor etc., adeoque pertinere ad P. Iam quum quaevis forma improprie primitiva (positiva) determinantis D spectari possit tamquam composita ex $(2, 1, \frac{1-D}{2})$ atque proprie primitiva (positiva) eiusdem determinantis, perspicuum est, nullam formam improprie primitivam (positivam) characterem ex Q in hoc casu habere posse. In casu altero, $D \equiv 5 \pmod 8$, omnia contraria sunt, scilicet D', qui etiam erit $\equiv 5$, certo multitudinem imparem factorum formae $8n+3$ atque $8n+5$ implicabit, unde concluditur, characterem formae $(2, 1, \frac{1-D}{2})$, atque hinc etiam characterem cuiusvis formae improprie primitivae (pos.) det. D pertinere ad Q, adeoque nulli characterum P genus impr. prim. pos. respondere posse.

III. Denique pro determinante negativo genera improprie primitiva negativa rursus contraria sunt generibus improprie primitivis positivis, scilicet illa non poterunt habere characterem ex P vel ex Q, prout $D \equiv 1$ vel $\equiv 5 \pmod 8$, sive prout $-D$ est formae $8n+7$ vel $8n+3$. Hoc nullo negotio deducitur inde, quod ex compositione formae $(-1, 0, D)$, cuius character est ex Q, cum formis improprie primitivis negativis eiusdem determinantis formae improprie primitivae positivae proveniunt, adeoque, quando ab his exclusi sunt characteres Q, necessario ab illis exclusi esse debent characteres P, et contra.

Methodus peculiaris, numeros primos in duo quadrata decomponendi.

265.

Ex disquisitionibus artt. 257, 258 supra multitudine classium ancipitum, quibus omnia praecedentia sunt superstructa, multae aliae conclusiones attentione perdignae deduci possunt, quas brevitatis caussa supprimere oportet; sequentem tamen, elegantia sua insignem, praeterire non possumus. Pro determinante positivo p, qui est numerus primus formae $4n+1$, unicam tantummodo classem ancipitem proprie primitivam dari ostendimus; quapropter omnes formae ancipites proprie primitivae talis determinantis proprie aequivalentes erunt. Si itaque b est numerus integer positivus proxime minor quam $\sqrt{p}$, atque $p-bb=a'$, formae $(1, b, -a')$, $(-1, b, a')$, proprie aequivalebunt, adeoque, quum utraque manifesto sit forma reducta, altera in alterius periodo erit contenta. Tribuendo formae priori in periodo sua indicem 0, index posterioris necessario erit impar (quoniam termini primi harum duarum formarum signa opposita habent); ponatur itaque $=2m+1$. Porro facile perspicitur, si formae indicum 1, 2, 3 etc. resp. sint

$$(-a', b', a''),\ (a'', b'', -a'''),\ (-a''', b''', a'''')\ \text{etc.}$$

indicibus $2m, 2m-1, 2m-2, 2m-3$ etc. responsuras esse formas

$$(a', b, -1),\ (-a'', b', a'),\ (a''', b'', -a''),\ (-a'''', b''', a''')\ \text{etc.}$$

Hinc colligitur, si forma indicis m sit (A, B, C), eandem fore $(-C, B, -A)$, adeoque $C=-A$ et $p=BB+AA$. Quare quivis numerus primus formae $4n+1$ in duo quadrata decomponi potest (quam propositionem supra, art. 182, e principiis prorsus diversis deduximus), et ad talem decompositionem pervenire possumus per methodum simplicissimam et omnino uniformem, scilicet per evolutionem periodi formae reductae, cuius determinans est ille numerus primus et cuius terminus primus 1, usque ad formam, cuius termini externi magnitudine sunt aequales, signis oppositi. Ita *e.g.* pro $p=233$ habetur $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$, atque $233=64+169$. Ceterum patet, A necessario fieri imparem (quoniam $(A, B, -A)$ debet esse forma proprie primitiva), et proin B parem. — Quum pro determinante positivo p, qui est numerus primus formae $4n+1$, etiam in ordine improprie primitivo unica tantum classis anceps contineatur, perspicuum est, si g sit numerus

impar proxime minor quam $\sqrt{p}$, atque $p-gg=4h$, formas reductas improprie primitivas $(2, g, -2h)$, $(-2, g, 2h)$ proprie aequivalere, adeoque alteram in alterius periodo contentam esse. Hinc per ratiocinia praecedentibus omnino similia concluditur, in periodo formae $(2, g, -2h)$ reperiri formam, cuius termini externi magnitudine aequales sint, signa habeant opposita, ita ut discerptio numeri p in duo quadrata etiam hinc peti possit. Patet autem, terminos externos huius formae fore pares, adeoque medium imparem; et quum constet, numerum primum unico tantum modo in duo quadrata decomponi posse, forma per hanc posteriorem methodum inventa erit vel $(B, \pm A, -B)$ vel $(-B, \pm A, B)$. Ita in exemplo nostro pro $p=233$ habetur $(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$, et $233=169+64$ ut supra.

DIGRESSIO CONTINENS TRACTATUM DE FORMIS TERNARIIS.

266.

Hactenus disquisitionem nostram ad tales functiones secundi gradus restrinximus, quae *duas* indeterminatas implicant, neque opus fuit, denominationem specialem ipsis tribuere. Sed manifesto hoc argumentum tamquam sectionem maxime particularem disquisitionis generalissimae *de functionibus algebraicis rationalibus integris homogeneis plurium indeterminatarum et plurium dimensionum* considerare, talesque functiones secundum multitudinem dimensionum in *formas secundi, tertii, quarti gradus etc.*, secundum multitudinem indeterminatarum autem in *formas binarias, ternarias, quaternarias* etc. commode distinguere possumus. Formae itaque, hactenus simpliciter sic dictae, vocabuntur *formae binariae secundi gradus;* tales autem functiones ut

$$Axx+2Bxy+Cyy+2Dxz+2Eyz+Fzz$$

(denotantibus A, B, C, D, E, F integros datos) dicentur *formae ternariae secundi gradus* et sic porro. Proxime quidem Sectio praesens solis formis binariis secundi gradus est dicata; sed quoniam complures veritates ad has spectantes, eaeque pulcherrimae, adhuc supersunt, quarum fons proprius in theoria formarum ternariarum secundi gradus est quaerendus, brevem ad hanc theoriam digressionem hic intercalamus, in qua ex primis eius elementis ea trademus, quae ad perfectionem theoriae formarum binariarum sunt necessaria, quod geometris acceptius fore spe-

ramus, quam si illas vel supprimeremus, vel per methodos minus genuinas eueremus. Exactiorem autem de hoc argumento gravissimo disquisitionem ad aliam occasionem nobis reservare debemus, tum quod ipsius ubertas limites huius operis iam nunc longe egrederetur, tum quod spes est, luculentis adhuc incrementis eam in posterum locupletatum iri. Formae vero tum quaternariae, quinariae etc. secundi gradus, tum omnes superiorum graduum hoc quidem loco ab instituto nostro penitus excluduntur *), sufficiatque hunc campum vastissimum geometrarum attentioni commendavisse, in quo materiem ingentem vires suas exercendi, Arithmeticamque sublimiorem egregiis incrementis augendi invenient.

267.

Ad perspicuitatem multum proderit, inter tres indeterminatas, in formam ternariam ingredientes, simili modo ut in formis binariis, ordinem fixum stabilire, ita ut *indeterminata prima*, *secunda* et *tertia* ab invicem distinguantur; in disponendis autem singulis formae partibus hunc ordinem semper observabimus, ut primum locum obtineat ea pars quae quadratum indeterminatae primae implicat, in sequentibus eae quae implicant quadratum indeterminatae secundae, quadratum tertiae, productum duplum secundae in tertiam, productum duplum primae in tertiam, productum duplum primae in secundam deinceps sequantur; denique numeros integros determinatos per quos haec quadrata et producta dupla multiplicata sunt, eodem ordine *coëfficientem primum*, *secundum*, *tertium*, *quartum*, *quintum*, *sextum* vocabimus. Ita

$$axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

erit forma ternaria rite ordinata, cuius indeterminata prima x, secunda x', tertia x'', coëfficiens primus a etc., quartus b etc. Sed quoniam ad brevitatem multum conferet, si non semper necesse est, indeterminatas formas ternariae per literas peculiares denotare, eandem formam, quatenus ad indeterminatas non respicimus, etiam hoc modo

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

designabimus.

*) Propter hanc rationem formae binariae vel ternariae *secundi gradus* in sequentibus semper sunt intelligendae, quoties de talibus formis simpliciter loquemur.

Ponendo

$$\begin{array}{lll} bb - a'a'' = A, & b'b' - aa'' = A', & b''b'' - aa' = A'' \\ ab - b'b'' = B, & ab' - bb'' = B', & ab'' - bb' = B'' \end{array}$$

oritur alia forma

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} \ldots F$$

quam *formae*

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \ldots f$$

adiunctam dicemus. Hinc rursus invenitur, denotando brevitatis caussa numerum

$$abb + a'b'b' + a''b''b'' - aa'a'' - 2bb'b'' \quad \text{per} \quad D$$

$$\begin{array}{lll} BB - A'A'' = aD, & B'B' - AA'' = a'D, & B''B'' - AA' = a''D \\ AB - B'B'' = bD, & AB' - BB'' = b'D, & AB'' - BB' = b''D \end{array}$$

unde patet, formae F adiunctam esse formam

$$\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}$$

Numerum D, a cuius indole proprietates formae ternariae f imprimis pendent, *determinantem* huius formae vocabimus; hoc modo determinans formae F fit $= DD$, sive aequalis quadrato determinantis formae f, cui adiuncta est.

Ita *e. g.* formae ternariae $\left(\begin{smallmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{smallmatrix}\right)$ adiuncta est $\left(\begin{smallmatrix} -68, & -260, & -181 \\ 217, & -111, & 133 \end{smallmatrix}\right)$, utriusque determinans $= 1$.

Formae ternariae determinantis 0 ab investigatione sequente omnino excludentur, quippe quae, ut in formarum ternariarum theoria, alia occasione uberius tradenda, ostendetur, *specie* tantum sunt ternariae, reveraque binariis aequipollentes.

268.

Si forma aliqua ternaria f determinantis D, cuius indeterminatae sunt x, x', x'' (puta prima $= x$ etc.) in formam ternariam g determinantis E, cuius indeterminatae sunt y, y', y'', transmutatur per substitutionem talem

$$x = \alpha y + \vec{\delta} y' + \gamma y''$$
$$x' = \alpha' y + \vec{\delta}' y' + \gamma' y''$$
$$x'' = \alpha'' y + \vec{\delta}'' y' + \gamma'' y''$$

ubi novem coëfficientes α, $\vec{\delta}$ etc. omnes supponuntur esse numeri integri, brevitatis caussa neglectis indeterminatis simpliciter dicemus, f transire in g per substitutionem (S)

$$\begin{matrix} \alpha, & \vec{\delta}, & \gamma \\ \alpha', & \vec{\delta}', & \gamma' \\ \alpha'', & \vec{\delta}'', & \gamma'' \end{matrix}$$

atque f *implicare* ipsam g, sive g *sub* f *contentam* esse. Ex tali itaque suppositione sponte sequuntur sex aequationes pro sex coëfficientibus in g, quas apponere non erit necessarium; hinc autem per calculum facilem sequentes conclusiones evolvuntur:

I. Designato brevitatis caussa numero

$$\alpha\vec{\delta}'\gamma'' + \vec{\delta}\gamma'\alpha'' + \gamma\alpha'\vec{\delta}'' - \gamma\vec{\delta}'\alpha'' - \alpha\gamma'\vec{\delta}'' - \vec{\delta}\alpha'\gamma'' \text{ per } k$$

invenitur post debitas reductiones $E = kkD$, unde patet, D metiri ipsum E et quotientem esse quadratum. Patet itaque, numerum k pro transformationibus formarum ternariarum simile quid esse, ac numerum $\alpha\delta - \vec{\delta}\gamma$ in art. 157 pro transformationibus formarum binariarum, puta radicem quadratam ex quotiente determinantium, unde coniectare possemus, diversitatem signi ipsius k etiam hic stabilire differentiam essentialem inter transformationes atque implicationes proprias et improprias. Sed rem propius contemplando perspicuum est, f transire in g etiam per hanc substitutionem

$$\begin{matrix} -\alpha, & -\vec{\delta}, & -\gamma \\ -\alpha', & -\vec{\delta}', & -\gamma' \\ -\alpha'', & -\vec{\delta}'', & -\gamma'' \end{matrix}$$

ponendo autem in valore ipsius k pro α, $-\alpha$, pro $\vec{\delta}$, $-\vec{\delta}$ etc. prodibit $-k$, quare haec substitutio substitutioni S dissimilis foret, et quaevis forma ternaria, aliam uno modo implicans, eandem etiam altero modo implicaret. Talis itaque

distinctio, quoniam in formis ternariis nullum usum habet, hic omnino proscribetur.

II. Denotando per F, G formas ipsis f, g resp. adiunctas, determinantur coëfficientes in F per coëfficientes in f, coëfficientesque in G per valores coëfficientium formae g ex aequationibus quas suppeditat substitutio S notos. Exprimendo coëfficientes formae f per literas, ex comparatione valorum coëfficientium formarum F, G nullo negotio confirmatur, F implicare formam G atque in eam transmutari per substitutionem (S')

$$\begin{matrix} \vec{\delta}'\gamma'' - \vec{\delta}''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\vec{\delta}'' - \alpha''\vec{\delta}' \\ \vec{\delta}''\gamma - \vec{\delta}\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\vec{\delta} - \alpha\vec{\delta}'' \\ \vec{\delta}\gamma' - \vec{\delta}'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\vec{\delta}' - \alpha'\vec{\delta} \end{matrix}$$

Calculum ipsum nullis difficultatibus obnoxium non adscribimus.

III. Forma g per substitutionem (S'')

$$\begin{matrix} \vec{\delta}'\gamma'' - \vec{\delta}''\gamma', & \vec{\delta}''\gamma - \vec{\delta}\gamma'', & \vec{\delta}\gamma' - \vec{\delta}'\gamma \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha \\ \alpha'\vec{\delta}'' - \alpha''\vec{\delta}', & \alpha''\vec{\delta} - \alpha\vec{\delta}'', & \alpha\vec{\delta}' - \alpha'\vec{\delta} \end{matrix}$$

manifesto in eandem formam transmutatur, in quam f transit per hanc

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k \end{matrix}$$

sive in eam, quae oritur multiplicando singulos coëfficientes formae f per kk. Hanc formam designabimus per f'.

IV. Prorsus simili modo probatur, formam G per substitutionem (S''')

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \vec{\delta}, & \vec{\delta}', & \vec{\delta}'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

transire in formam, quae oritur ex F, multiplicando singulos coëfficientes per kk. Hanc formam exprimemus per F'.

Substitutionem S''' oriri dicemus *per transpositionem* substitutionis S; tunc manifesto S rursus prodit ex transpositione substitutionis S'''; atque S', S'' altera ex alterius transpositione. — Substitutio S' commode appellari potest substitutioni S *adiuncta*, unde substitutioni S''' adiuncta erit S''.

269.

Si non modo forma f implicat ipsam g, sed etiam haec illam, formae f, g *aequivalentes* vocabuntur. In hoc itaque casu non modo D ipsum E metietur, sed etiam E ipsum D, unde facile concluditur, esse debere $D = E$. Vice versa autem, si forma f implicat formam g eiusdem determinantis, hae duae formae erunt aequivalentes. Erit enim (adhibendo eadem signa ut in art. praec. excipiendoque casum ubi $D = 0$) $k = \pm 1$, adeoque forma f', in quam transit g per substitutionem S'', cum f identica, sive f sub g contenta. Porro patet, in hoc casu etiam formas F, G, ipsius f, g adiunctas, inter se aequivalentes fore, posterioremque in priorem transire per substitutionem S'''. Denique vice versa, si formae F, G aequivalentes esse *supponuntur*, atque prior transit in posteriorem per substitutionem T, etiam formae f, g aequivalentes erunt, transibitque f in g per substitutionem ipsi T adiunctam, atque g in f per eam, quae oritur ex transpositione substitutionis T. Nam per has duas substitutiones resp. transit forma ipsi F adiuncta in formam ipsi G adiunctam atque haec in illam; hae duae formae autem oriuntur ex f, g multiplicando singulos coëfficientes per D; unde nullo negotio concluditur, per easdem substitutiones transire f in g, atque g in f resp.

270.

Si forma ternaria f formam ternariam f' implicat, atque haec formam f'': implicabit etiam f ipsam f'''. Facillime enim perspicietur, si transeat

f in f' per substitutionem	f' in f'' per substitutionem
α, $\vec{\upsilon}$, γ	$\hat{\upsilon}$, ε, ζ
α', $\vec{\upsilon}'$, γ'	δ', ε', ζ'
α'', $\vec{\upsilon}''$, γ''	δ'', ε'', ζ''

f transmutatum iri per substitutionem

$$\begin{array}{lll} \alpha\delta+\vec{\upsilon}\delta'+\gamma\delta'', & \alpha\varepsilon+\vec{\upsilon}\varepsilon'+\gamma\varepsilon'', & \alpha\zeta+\vec{\upsilon}\zeta'+\gamma\zeta'' \\ \alpha'\delta+\vec{\upsilon}'\delta'+\gamma'\delta'', & \alpha'\varepsilon+\vec{\upsilon}'\varepsilon'+\gamma'\varepsilon'', & \alpha'\zeta+\vec{\upsilon}'\zeta'+\gamma'\zeta'' \\ \alpha''\delta+\vec{\upsilon}''\delta'+\gamma''\delta'', & \alpha''\varepsilon+\vec{\upsilon}''\varepsilon'+\gamma''\varepsilon'', & \alpha''\zeta+\vec{\upsilon}''\zeta'+\gamma''\zeta'' \end{array}$$

In eo itaque casu, ubi f aequivalet ipsi f', atque f' ipsi f'', forma f etiam formae f'' aequivalebit. — Ceterum sponte manifestum est, quomodo haec theoremata ad plures formas sint applicanda.

271.

Hinc iam patet, omnes formas ternarias, perinde ac binarias, in *classes* distribui posse, referendo ad classem eandem formas aequivalentes, non-aequivalentes ad diversas. Formae itaque determinantium diversorum certo ad classes diversas pertinebunt, et proin classes infinite multae formarum ternariarum dabuntur; formae autem ternariae eiusdem determinantis modo minorem modo maiorem classium numerum efficiunt; quod vero tamquam proprietas palmaris harum formarum est considerandum, *omnes formae eiusdem determinantis dati semper constituunt classium multitudinem finitam*. Evolutioni uberiori huius gravissimi theorematis praemittenda est explicatio sequentis differentiae essentialis, quae inter formas ternarias obtinet.

Quaedam formae ternariae ita sunt comparatae, ut per ipsas sine discrimine repraesentari possint numeri positivi et negativi, *e. g.* forma $xx+yy-zz$, quamobrem *formae indefinitae* vocabuntur. Contra per alias numeri negativi repraesentari nequeunt, sed (praeter cifram quae prodit, ponendo singulas indeterminatas $= 0$) positivi tantum, ut $xx+yy+zz$, quare *formae positivae* dicentur; denique per alias numeri positivi repraesentari nequeunt, ut $-xx-yy-zz$, unde appellabuntur *formae negativae*; formae positivae et negativae nomine communi *formae definitae* dicentur. Ecce iam criteria generalia, per quae haec formarum indoles discerni poterit.

Multiplicando formam ternariam

$$f = axx+a'x'x'+a''x''x''+2bx'x''+2b'xx''+2b''xx'$$

determinantis D per a, denotandoque coëfficientes formae ipsi f adiunctae perinde ut in art. 267 per A, A', A'', B, B', B'', prodit

$$(ax+b''x'+b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = g$$

multiplicando denuo per A', provenit

$$A'(ax+b''x'+b'x'')^2 - (A'x''-Bx')^2 + aDx'x' = h$$

Hinc statim concluditur, si tum A' tum aD sint numeri negativi, omnes valores ipsius h esse negativos, unde manifesto per formam f tales tantummodo numeri repraesentari poterunt, quorum signum oppositum est signo ipsius aA', *i. e.* identicum cum signo ipsius a, sive oppositum signo ipsius D. In hoc itaque casu f erit forma definita, et quidem positiva vel negativa, prout a est positivus vel negativus, sive prout D est negativus vel positivus.

Si vero vel vterque aD, A' est positivus, vel alter positivus alter negativus (neuter $= 0$), facile perspicietur, h per debitam quantitatum x, x', x'' determinationem valores tum positivos tum negativos nancisci posse. Quare in hoc casu f valores tum eodem signo affectos ut aA' tum opposito obtinere poterit, eritque adeo forma indefinita.

Pro eo casu, ubi $A' = 0$, neque vero $a = 0$, fit

$$g = (ax+b''x'+b'x'')^2 - x'(A''x' - 2Bx'')$$

Tribuendo ipsi x' valorem arbitrarium (qui tamen non $= 0$), accipiendoque x'' ita ut $\frac{A''x'}{2B} - x''$ signum idem obtineat ut Bx' (quod fieri posse facile perspicitur, quum B nequeat esse $= 0$, hinc enim foret $BB - A'A'' = aD = 0$, adeoque etiam $D = 0$, quem casum excludimus), erit $x'(A''x' - 2Bx'')$ quantitas positiva, unde facile patet, x' ita determinari posse, ut g obtineat valorem negativum. Manifesto hi valores etiam ita accipi poterunt, ut, si desideretur, omnes sint integri. Denique patet, si ipsis x', x'' valores quicunque tribuantur, ipsum x tam magnum accipi posse, ut g fiat positivus. Hinc concluditur, in hoc casu formam f esse indefinitam.

Denique si $a = 0$, erit

$$f = a'x'x' + 2b'x'x'' + a''x''x'' + 2x(b''x' + b'x'')$$

Accipiendo itaque x', x'' ad lubitum, ita tamen ut $b''x' + b'x''$ non sit $= 0$ (quod manifesto fieri poterit, nisi simul b' et b'' sint $= 0$; tunc autem foret $D = 0$), nullo negotio perspicitur, x ita determinari posse, ut f obtineat valores tum positivos, tum negativos. Quare etiam in hocce casu f erit forma indefinita.

Eodem modo, ut hic ex numeris aD, A' indolem formae f diiudicavimus, etiam aD et A'' adhiberi possunt, ita ut f sit forma definita, si tum aD tum A'' sit negativus; indefinita in omnibus reliquis casibus. Nec non prorsus simili modo eidem fini inservire potest consideratio numerorum $a'D$ et A, vel horum $a'D$ et A'', vel horum $a''D$ et A, vel denique ipsorum $a''D$ et A'.

Ex his omnibus colligitur, in forma definita sex numeros $A, A', A'', aD, a'D, a''D$ esse negativos, et quidem in forma positiva a, a', a'' erunt positivi, D negativus; in negativa autem a, a', a'' erunt negativi, D positivus. Hinc patet, omnes formas ternarias determinantis dati positivi distribui in negativas et indefinitas; omnes autem determinantis negativi in positivas et indefinitas; denique formas positivas determinantis positivi, seu negativas determinantis negativi omnino non dari. — Indidem facile perspicitur, formae definitae semper adiunctam esse definitam et quidem *negativam*, indefinitae indefinitam.

Quum omnes numeri per formam ternariam datam repraesentabiles manifesto etiam per omnes formas huic aequivalentes repraesentari possint: formae ternariae in eadem classe contentae vel omnes erunt indefinitae, vel omnes positivae, vel omnes negativae. Quamobrem has formarum denominationes etiam ad classes integras transferre licebit.

272.

Theorema in art. praec. propositum, quod omnes formae ternariae determinantis dati in multitudinem *finitam* classium distribuuntur, per methodum ei qua in formis binariis usi sumus analogam tractabimus, scilicet ostendendo, primo, quo pacto quaevis forma ternaria ad formam simpliciorem reduci possit, dein, formarum simplicissimarum (ad quas per tales reductiones perveniatur) multitudinem pro quovis determinante dato esse finitam. Supponamus generali-

ter, propositam esse formam ternariam $f = \binom{a, a', a''}{b, b', b''}$ determinantis D (a cifra diversi), quae per substitutionem (S)

$$\begin{matrix} \alpha, & \vec{\beta}, & \gamma \\ \alpha', & \vec{\beta}', & \gamma' \\ \alpha'', & \vec{\beta}'', & \gamma'' \end{matrix}$$

transeat in aequivalentem $g = \binom{m, m', m''}{n, n', n''}$; versabiturque negotium nostrum in eo, ut α, $\vec{\beta}$, γ etc. ita definiantur, ut forma g simplicior evadat quam f. Sint formae ipsis f, g adiunctae resp. $\binom{A, A', A''}{B, B', B''}$, $\binom{M, M', M''}{N, N', N''}$, quae designentur per F, G. Tunc per art. 269 F transibit in G per substitutionem ipsi S adiunctam, G autem in F per substitutionem ex transpositione ipsius S oriundam. Numerum

$$\alpha\vec{\beta}''\gamma' + \alpha'\vec{\beta}''\gamma + \alpha''\vec{\beta}\gamma' - \alpha''\vec{\beta}'\gamma - \alpha\vec{\beta}''\gamma' - \alpha'\vec{\beta}\gamma''$$

qui esse debebit vel $= +1$ vel $= -1$, denotabimus per k. Quibus ita factis observamus

I. Si fiat $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\vec{\beta}'' = 0$, $\gamma'' = 1$, fore

$$m = a\alpha\alpha + 2b''\alpha\alpha' + a'\alpha'\alpha', \quad m' = a\vec{\beta}\vec{\beta} + 2b''\vec{\beta}\vec{\beta}' + a'\vec{\beta}'\vec{\beta}', \quad m'' = a''$$
$$n = b\vec{\beta}' + b'\vec{\beta}, \quad n' = b\alpha' + b'\alpha, \quad n'' = a\alpha\vec{\beta} + b''(\alpha\vec{\beta}' + \vec{\beta}\alpha') + a'\alpha'\vec{\beta}'$$

Praeterea esse debebit $\alpha\vec{\beta}' - \vec{\beta}\alpha'$ vel $= +1$ vel $= -1$. Hinc manifestum est, formam binariam (a, b'', a'), cuius determinans est A'', transmutari per substitutionem α, $\vec{\beta}$, α', $\vec{\beta}'$ in formam binariam (m, n'', m') determinantis M'', et proin ipsi aequivalere propter $\alpha\vec{\beta}' - \vec{\beta}\alpha' = \pm 1$, unde erit $M'' = A''$, quod etiam directe facile confirmatur. Nisi itaque (a, b'', a') iam est forma simplicissima in classe sua, ipsos α, $\vec{\beta}$, α', $\vec{\beta}'$ ita determinare licebit, ut (m, n'', m') sit forma simplicior; et quidem e theoria aequivalentiae formarum binariarum facile concluditur, hoc ita fieri posse, ut m non sit maior quam $\sqrt{-\frac{4}{3}A''}$, si A'' fuerit negativus, vel non maior quam $\sqrt{A''}$, si A'' fuerit positivus, vel $m = 0$, si $A'' = 0$, ita ut in omnibus casibus valor (absolutus) ipsius m certe vel infra vel saltem usque ad $\sqrt{\pm\frac{4}{3}A''}$ deprimi possit. Hoc itaque modo forma f ad aliam reducitur coëfficientem primum, si fieri potest, minorem habentem, et cuius forma adiuncta coëfficientem tertium eundem habet ut forma F ipsi f adiuncta. In hoc consistit *reductio prima*.

II. Si vero fit $\alpha = 1$, $\vec{\beta} = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, erit $k = \vec{\beta}''\gamma' - \vec{\beta}'\gamma' = \pm 1$; substitutio itaque ipsi S adiuncta erit

$$\begin{matrix} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\vec{\beta}'' \\ 0, & -\gamma', & \vec{\beta}' \end{matrix}$$

per quam F transibit in G. Habebitur itaque

$$\begin{aligned} m &= a, \quad n' = b'\gamma'' + b''\gamma', \quad n'' = b'\vec{\beta}'' + b''\vec{\beta}' \\ m' &= a'\vec{\beta}'\vec{\beta}' + 2b\vec{\beta}'\vec{\beta}'' + a''\vec{\beta}''\vec{\beta}'' \\ m'' &= a'\gamma'\gamma' + 2b'\gamma'\gamma'' + a''\gamma''\gamma'' \\ n &= a'\vec{\beta}'\gamma' + b(\vec{\beta}'\gamma'' + \gamma'\vec{\beta}'') + a''\vec{\beta}''\gamma'' \\ M' &= A'\gamma''\gamma'' - 2B'\gamma'\gamma'' + A''\gamma'\gamma' \\ N &= -A'\vec{\beta}''\gamma'' + B(\vec{\beta}'\gamma'' + \gamma'\vec{\beta}'') - A''\vec{\beta}'\gamma' \\ M'' &= A'\vec{\beta}''\vec{\beta}'' - 2B\vec{\beta}'\vec{\beta}'' + A''\vec{\beta}'\vec{\beta}' \end{aligned}$$

Hinc patet, formam binariam (A'', B, A'), cuius determinans est Da, transire per substitutionem $\vec{\beta}'$, $-\gamma'$, $-\vec{\beta}''$, γ'' in formam (M'', N, M') determinantis Dm, adeoque (propter $\vec{\beta}'\gamma'' - \gamma'\vec{\beta}'' = \pm 1$, vel propter $Da = Dm$) ipsi aequivalere. Nisi itaque (A'', B, A') iam est forma simplicissima classis suae, coëfficientes $\vec{\beta}'$, γ', $\vec{\beta}''$, γ'' ita determinari poterunt, ut (M'', N, M') sit simplicior, et quidem hoc semper poterit fieri ita, ut M'' sine respectu signi non sit maior quam $\sqrt{\pm\frac{4}{3}Da}$. Hoc itaque modo forma f reducitur ad aliam coëfficientem primum eundem habentem, sed cuius forma adiuncta coëfficientem tertium si fieri potest minorem habeat quam forma F ipsi f adiuncta. In hoc consistit *reductio secunda*.

III. Si itaque f est forma ternaria, ad quam neque reductio prima neque secunda est applicabilis, *i. e.* quae per neutram in formam simpliciorem transmutari potest: necessario erit tum $aa <$ vel $= \frac{4}{3}A''$, tum $A''A'' <$ vel $= \frac{4}{3}aD$ sine respectu signi. Hinc a^4 erit $<$ vel $= \frac{16}{9}A''A''$, adeoque $a^4 <$ vel $= \frac{64}{27}aD$, $a^3 <$ vel $= \frac{64}{27}D$, et $a <$ vel $= \frac{4}{3}\sqrt[3]{D}$; hinc rursus $A''A'' <$ vel $= \frac{16}{9}\sqrt[3]{D^4}$ atque $A'' <$ vel $= \frac{4}{3}\sqrt[3]{D^2}$. Quamobrem quamdiu a vel A'' hos limites adhuc superant, necessario una aut altera reductionum praecedentium ad formam f applicari poterit. — Ceterum haec conclusio non est convertenda, quum utique saepius

accidat, ut forma ternaria, cuius coëfficiens primus, atque coëfficiens tertius formae adiunctae iam sunt infra illos limites, nihilominus per unam alteramve reductionem adhuc simplicior reddi possit.

IV. Quodsi vero ad formam ternariam quamcunque datam determinantis D alternis vicibus reductio prima et secunda applicantur, *i. e.* ad ipsam prima vel secunda, ad eam quae hinc resultat secunda vel prima, ad eam quae hinc provenit iterum prima vel secunda etc., manifestum est, tandem necessario ad formam perventum iri, ad quam neutra amplius applicari possit. Quum enim magnitudo absoluta tum coëfficientium primorum formarum hoc modo prodeuntium, tum coëfficientium tertiorum formarum illis adiunctarum continuo alternis vicibus eadem maneat atque decrescat, hic progressus necessario tandem alicubi finietur, quia alioquin duae series infinitae numerorum continuo decrescentium haberentur. Hinc iam nacti sumus egregium theorema: *Quaevis forma ternaria determinantis D reduci potest ad aliam aequivalentem, cuius coëfficiens primus non sit maior quam* $\frac{4}{3}\sqrt[3]{D}$, *atque coëfficiens tertius formae ipsi adiunctae non maior quam* $\frac{4}{3}\sqrt[3]{D^2}$ *sine respectu signi; siquidem forma proposita his proprietatibus ipsa nondum est praedita.* — Ceterum loco coëfficientis primi formae f atque tertii formae ipsi f adiunctae prorsus simili modo tractare potuissemus vel coëfficientem primum formae ipsius et secundum adiunctae; vel secundum formae ipsius et primum vel tertium adiunctae; vel tertium formae ipsius et primum vel secundum adiunctae, quibus viis perinde ad finem nobis propositum perveniremus: sed e re est, methodo uni constanter adhaerere, quo facilius operationes huc pertinentes ad algorithmum fixum reduci possint. Denique observamus, duobus coëfficientibus, quos infra limites fixos deprimere docuimus, limites adhuc minores constitui posse, si formae definitae ab indefinitis separentur; hoc vero ad institutum praesens non est necessarium.

273.

Ecce iam quaedam exempla, per quae praecepta praecedentia magis illustrabuntur.

Ex. 1. Sit $f = \left(\begin{smallmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{smallmatrix}\right)$, erit $F = \left(\begin{smallmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{smallmatrix}\right)$, $D = -1$. Quum $(19, 1, 21)$ sit forma binaria reducta, cui alia, termini primi minoris quam 19, non aequivalet, reductio prima hic non est applicabilis; forma binaria

$(A'', B, A') = (-398, 257, -166)$ autem per theoriam aequivalentiae formarum binariarum in simpliciorem aequivalentem $(-2, 1, -10)$ transmutabilis invenitur, in quam transit per substitutionem $2, 7, 3, 11$. Faciendo itaque $\delta' = 2$, $\gamma' = -7$, $\delta'' = -3$, $\gamma'' = 11$, applicanda erit ad formam f substitutio $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 2, & -7 \\ 0, & -3, & 11 \end{smallmatrix}\right\}$ per quam invenitur transire in hanc $\left(\begin{smallmatrix} 19, & 354, & 4769 \\ -1299, & 301, & -82 \end{smallmatrix}\right) \ldots f'$. Coëfficiens tertius formae, huic adiunctae, est -2, quo respectu f'' simplicior est censenda quam f.

Ad formam f' applicari potest reductio prima. Scilicet quum forma binaria $(19, -82, 354)$ transmutetur in $(1, 0, 2)$ per substitutionem $13, 4, 3, 1$: applicanda erit ad formam f' substitutio $\left\{\begin{smallmatrix} 13, & 4, & 0 \\ 3, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$ per quam transit in hanc $\left(\begin{smallmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{smallmatrix}\right) \ldots f''$.

Ad formam f'', cui adiuncta est $\left(\begin{smallmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{smallmatrix}\right)$, denuo applicari potest reductio secunda. Scilicet $(-2, -95, -4513)$ transit per substitutionem $47, 1, -1, 0$ in $(-1, 1, -2)$: quamobrem ad f'' applicanda erit substitutio $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 47, & -1 \\ 0, & 1, & 0 \end{smallmatrix}\right\}$ per quam transit in $\left(\begin{smallmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{smallmatrix}\right) \ldots f'''$. Huius coëfficiens primus per reductionem primam amplius diminui non potest, neque formae, ipsi adiunctae, tertius per secundam.

Ex. 2. Proposita sit forma $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right) \ldots f$, cui adiuncta est $\left(\begin{smallmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{smallmatrix}\right)$ et cuius determinans $= 2$. Hic successive reperiuntur, applicando alternatim reductionem secundam et primam,

substitutiones	per quas transit	in
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 4, & -1 \end{smallmatrix}\right\}$	f	$\left(\begin{smallmatrix} 10, & 2, & 2 \\ -1, & 0, & -4 \end{smallmatrix}\right) = f'$
$\left\{\begin{smallmatrix} 0, & -1, & 0 \\ 1, & -2, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$	f'	$\left(\begin{smallmatrix} 2, & 2, & 2 \\ 2, & -1, & 0 \end{smallmatrix}\right) = f''$
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 2, & -1 \end{smallmatrix}\right\}$	f''	$\left(\begin{smallmatrix} 2, & 2, & 2 \\ -2, & 1, & -2 \end{smallmatrix}\right) = f'''$
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$	f'''	$\left(\begin{smallmatrix} 0, & 2, & 2 \\ -2, & -1, & 0 \end{smallmatrix}\right) = f''''$

Forma f'''' per reductionem primam vel secundam ulterius deprimi nequit.

274.

Quando forma ternaria habetur, cuius coëfficiens primus, atque formae adiunctae tertius, quantum fieri potest per methodos praecedentes sunt depressi: methodus sequens reductionem ulteriorem suppeditat.

Adhibendo signa eadem ut in art. 272, et ponendo $\alpha = 1$, $\alpha' = 0$, $\delta' = 1$, $\alpha'' = 0$, $\delta'' = 0$, $\gamma'' = 1$, *i. e.* adhibendo substitutionem

$$\begin{matrix} 1, & \delta, & \gamma \\ 0, & 1, & \gamma' \\ 0, & 0, & 1 \end{matrix}$$

erit

$$m = a,\quad m' = a' + 2b'\delta + a\delta\delta,\quad m'' = a'' + 2b\gamma + 2b'\gamma + a\gamma\gamma + 2b''\gamma\gamma + a'\gamma'\gamma'$$
$$n = b + a'\gamma' + b'\delta + b''(\gamma + \delta\gamma) + a\delta\gamma,\quad n' = b' + a\gamma + b''\gamma',\quad n'' = b'' + a\delta$$

praeterea

$$M'' = A'',\quad N = B - A''\gamma',\quad N' = B' - N\delta - A''\gamma$$

Per talem itaque substitutionem coëfficientes a, A'', qui per reductiones praecedentes diminuti sunt, non mutantur; quamobrem negotium in eo versatur, ut per idoneam determinationem ipsorum δ, γ, γ' depressiones in coëfficientibus reliquis obtineantur. Ad hunc finem observamus primo, si fuerit $A'' = 0$, supponi posse, esse etiam $a = 0$; si enim a non $= 0$, reductio prima adhuc semel applicabilis foret, quum cuivis formae binariae determinantis 0 aequivaleat forma talis $(0, 0, h)$, sive cuius terminus primus $= 0$ (V. art. 215). Prorsus simili ratione supponere licet, esse etiam $A'' = 0$, si fuerit $a = 0$, ita ut vel neuter numerorum a, A'' sit 0 vel uterque.

In casu priori manifestum est, ipsos δ, γ, γ' ita determinari posse, ut sine respectu signi n'', N, N' resp. non sint maiores quam $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$. Ita in exemplo primo art. praec. transibit forma postrema $\left(\begin{smallmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{smallmatrix}\right)$, cui adiuncta est $\left(\begin{smallmatrix} -513, & -2, & -1 \\ 1, & -16, & 32 \end{smallmatrix}\right)$, per substitutionem $\left(\begin{smallmatrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1 \end{smallmatrix}\right)$ in hanc $\left(\begin{smallmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right) \ldots f''''$, cui adiuncta est $\left(\begin{smallmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$.

In casu posteriori, ubi $a = A'' = 0$, adeoque etiam $b'' = 0$ erit

$$m = 0,\quad m' = a',\quad m'' = a'' + 2b\gamma' + 2b'\gamma + a'\gamma'\gamma'$$
$$n = b + a'\gamma' + b'\delta,\quad n' = b',\quad n'' = 0$$

Erit itaque

$$D = a'b'b' = m'n'n'$$

perspicieturque facile, δ et γ' ita determinari posse, ut n fiat aequalis residuo absolute minimo ipsius b secundum modulum, qui est divisor communis maximus

ipsorum a', b', i. e. ut n fiat non maior quam semissis huius divisoris sine respectu signi, adeoque $n = 0$, quoties a', b' inter se sunt primi. Ipsis δ, γ' in hunc modum determinatis, valor ipsius γ ita accipi poterit, ut m'' non sit maior quam b' sine respectu signi; hoc quidem impossibile esset, quando $b' = 0$; tunc vero foret $D = 0$, quem casum exclusimus. Ita fit pro forma postrema in *ex.* 2 art. praec. $n = -2 - \delta + 2\gamma'$, unde statuendo $\delta = -2$, $\gamma' = 0$, fit $n = 0$, porro $m'' = 2 - 2\gamma$, et ponendo $\gamma = 1$, $m'' = 0$. Habemus itaque substitutionem $\left(\begin{smallmatrix} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right)$ per quam forma illa transit in $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right) \ldots f''''$.

275.

Si habetur series formarum ternariarum aequivalentium f, f', f'', f''' etc., atque transformationes cuiusvis harum formarum in sequentem: ex transformationibus formae f in f', formaeque f' in f'' per art. 270 deducitur transformatio formae f in f''; ex hac atque transf. formae f'' in f''' sequitur transf. formae f in f''' etc., manifestoque hoc pacto transformatio formae f in quamcunque aliam seriei inveniri poterit. Et quum ex transformatione formae f in quamcunque aliam aequivalentem g deduci possit transformatio formae g in f (S'' ex S artt. 268, 269), hoc modo erui poterit transformatio cuiuslibet formae seriei f', f'' etc. in primam f. — Ita pro formis exempli primi art. praec. inveniuntur substitutiones

$$\left(\begin{smallmatrix} 13, & 4, & 0 \\ 6, & 2, & -7 \\ -9, & -3, & 11 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 13, & 188, & -4 \\ 6, & 87, & -2 \\ -9, & -130, & 3 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 13, & -20, & 16 \\ 6, & -9, & 7 \\ -9, & 14, & -11 \end{smallmatrix}\right)$$

per quas f transit in f''', f'''', f''''' resp., et ex subst. ultima haec $\left(\begin{smallmatrix} 1, & 4, & 4 \\ 2, & 4, & 5 \\ 3, & -2, & 3 \end{smallmatrix}\right)$ per quam f''''' transit in f. Simili modo pro *ex.* 2 art. praec. prodeunt substitutiones

$$\left(\begin{smallmatrix} 1, & -1, & 1 \\ -3, & 4, & -3 \\ 10, & -14, & 11 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 2, & -3, & -1 \\ 3, & 1, & 0 \\ 2, & 4, & 1 \end{smallmatrix}\right)$$

per quas resp. transit forma $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right)$ in $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right)$, atque haec in illam.

276.

THEOREMA. *Classium, in quas omnes formae ternariae determinantis dati distribuuntur, multitudo semper est finita.*

Dem. I. Multitudo omnium formarum $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ determinantis dati D, in quibus $a = 0$, $b'' = 0$, b non maior quam semissis divisoris comm. max. numerorum a', b'; a'' non maior quam b', manifesto est finita. Quoniam enim esse debet $a'b'b' = D$, pro b' alii valores accipi nequeunt, quam $+1$, -1 atque radices quadratorum ipsum D metientium (si quae alia praeter 1 dantur) signo positivo et negativo affectae, quorum valorum multitudo finita est. Pro singulis autem valoribus ipsius b' valor ipsius a' est determinatus, ipsorumque b, a'' valores manifesto limitantur ad multitudinem finitam.

II. Simili modo finita est multitudo omnium formarum $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ determinantis D, in quibus a non $= 0$, neque maior quam $\frac{1}{2}\sqrt[3]{\pm D}$; $b''b'' - aa' = A''$ non $= 0$ neque maior quam $\frac{1}{2}\sqrt[3]{D^2}$; b'' non maior quam $\frac{1}{2}a$; $ab - b'b'' = B$ et $a'b' - bb'' = B'$ non maiores quam $\frac{1}{2}A''$. Nam multitudo omnium combinationum valorem ipsorum a, b'', A'', B, B' finita erit; his vero singulis determinatis, etiam formae coëfficientes reliqui a', b, b', a'', coëfficientesque formae adiunctae

$$bb - a'a'' = A, \quad b'b' - aa'' = A', \quad a''b'' - bb' = B''$$

determinati erunt per aequationes hasce:

$$a' = \frac{b''b'' - A''}{a}, \quad A' = \frac{BB - aD}{A''}, \quad A = \frac{B'B' - a'D}{A''}, \quad B'' = \frac{BB' + b''D}{A''}$$

$$b = \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}, \quad b' = \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''}$$

$$a'' = \frac{b'b' - A'}{a} = \frac{bb - A}{a'} = \frac{bb' + B''}{b''}$$

Iam quum omnes illae formae obtineantur, eligendo e cunctis combinationibus valorum ipsorum a, b'', A'', B, B' eas, e quibus etiam a', a'', b, b' valores integros nanciscuntur, illarum multitudo manifesto erit finita.

III. Cunctae itaque formae in I et II multitudinem finitam classium constituunt, quae etiam formarum ipsarum multitudine minor esse poterit, si quae ex ipsis inter se sunt aequivalentes. Iam quum per disquisitiones praecedentes quaevis forma ternaria determinantis D alicui ex illis formis necessario acquivaleat, *i. e.* ad aliquam e classibus, quas hae formae constituunt, pertineat: hae classes omnes formas det. D complectentur, *i. e.* omnes formae ternariae det. D in multitudinem finitam classium distribuentur. *Q. E. D.*

277.

Regulae, per quas omnes formae in I et II art. praec. erui possunt, ex ipsarum explicatione sponte defluunt; quare sufficiet quaedam exempla apposuisse. Pro $D = 1$, formae I hae sex (per ambiguitatem signorum) prodeunt

$$\left(\begin{smallmatrix} 0, & 1, & 0 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & 1, & \pm 1 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right)$$

in formis II a et A'' alios valores quam $+1$ et -1 habere nequeunt, pro singulis quatuor combinationum hinc oriundarum b'', B et B' poni debent $= 0$, unde emergunt quatuor formae

$$\left(\begin{smallmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

Simili modo pro $D = -1$ sex formae I quatuorque II habentur,

$$\left(\begin{smallmatrix} 0, & -1, & 0 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & -1, & \pm 1 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right); \quad \left(\begin{smallmatrix} 1, & -1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

Pro $D = 2$ sex formae I proveniunt

$$\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & 2, & \pm 1 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right)$$

octoque formae II

$$\left(\begin{smallmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & 1, & 2 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

$$\left(\begin{smallmatrix} 1, & -2, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & 2, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & 2, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & -2, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

Ceterum multitudo classium ex his formis in his tribus casibus prodeuntium formarum multitudine multo minor est. Scilicet facile confirmatur

I. Formam $\left(\begin{smallmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{smallmatrix}\right)$ transire in

$$\left(\begin{smallmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

resp. per substitutiones

$$\left(\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & -1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 0, & 0, & 1 \\ 0, & 1, & -1 \\ \pm 1, & 1, & 0 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 0, & 0, & 1 \\ 0, & 1, & 1 \\ \pm 1, & -1, & -1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 1, & 0, & -1 \\ 1, & 1, & -1 \\ 0, & -1, & 1 \end{smallmatrix}\right)$$

formam $\left(\begin{smallmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$ autem in $\left(\begin{smallmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$ per solam indeterminatarum permutationem. Quare illae decem formae ternariae det. 1 ad has duas reducuntur.

$\left(\begin{smallmatrix}0,&1,&0\\0,&1,&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}-1,&-1,&-1\\0,&0,&0\end{smallmatrix}\right)$; pro priori, si magis arridet, etiam haec $\left(\begin{smallmatrix}1,&0,&0\\1,&0,&0\end{smallmatrix}\right)$ accipi potest. Quum forma prior indefinita sit, posterior definita, manifestum est, quamvis formam ternariam indefinitam det. 1 aequivalere formae $xx+2yz$, quamvis definitam huic $-xx-yy-zz$.

II. Prorsus simili modo invenitur, quamlibet formam ternariam indefinitam determinantis -1 aequivalere formae $-xx+2yz$, quamlibet definitam huic $xx+yy+zz$.

III. Pro determinante 2 ex octo formis (II) statim reiici possunt secunda, sexta et septima, quippe quae ex prima per solam indeterminatarum permutationem oriuntur, similique ratione etiam quinta quae e tertia, et octava quae e quarta perinde proveniunt; tres reliquae cum sex formis I, tres classes constituunt; scilicet $\left(\begin{smallmatrix}0,&2,&0\\0,&1,&0\end{smallmatrix}\right)$ transit in $\left(\begin{smallmatrix}0,&2,&0\\0,&-1,&0\end{smallmatrix}\right)$ per substitutionem $\left\{\begin{smallmatrix}1,&0,&0\\0,&1,&0\\0,&0,&-1\end{smallmatrix}\right\}$ formaque $\left(\begin{smallmatrix}1,&1,&-2\\0,&0,&0\end{smallmatrix}\right)$ in

$$\left(\begin{smallmatrix}0,&2,&1\\0,&1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}0,&2,&1\\0,&-1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}0,&2,&-1\\0,&1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}0,&2,&-1\\0,&-1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}1,&-1,&2\\0,&0,&0\end{smallmatrix}\right)$$

resp. per substitutiones

$$\left(\begin{smallmatrix}1,&0,&1\\1,&2,&0\\1,&1,&0\end{smallmatrix}\right)\quad \left(\begin{smallmatrix}1,&0,&-1\\1,&2,&0\\1,&1,&0\end{smallmatrix}\right)\quad \left(\begin{smallmatrix}1,&0,&0\\1,&2,&-1\\1,&1,&-1\end{smallmatrix}\right)\quad \left(\begin{smallmatrix}1,&0,&0\\1,&2,&1\\1,&1,&1\end{smallmatrix}\right)\quad \left(\begin{smallmatrix}1,&0,&0\\0,&1,&2\\0,&1,&1\end{smallmatrix}\right)$$

Quaevis itaque forma ternaria determinantis 2 ad aliquam ex his tribus est reducibilis

$$\left(\begin{smallmatrix}0,&2,&0\\0,&1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}1,&1,&-2\\0,&0,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}-1,&-1,&-2\\0,&0,&0\end{smallmatrix}\right)$$

loco primae, si magis placet, etiam $\left(\begin{smallmatrix}7,&0,&0\\1,&0,&0\end{smallmatrix}\right)$ accipi potest. Manifesto autem quaevis forma ternaria definita necessario aequivalebit tertiae $-xx-yy-2zz$, quum duae priores sint indefinitae; quaevis indefinita primae vel secundae, et quidem primae $2xx+2yz$, si ipsius coëfficiens primus, secundus et tertius simul sunt pares (quoniam facile perspicitur, talem formam per substitutionem quamcunque in similem formam transire, adeoque formae secundae aequivalere non posse), secundae $xx+yy-2zz$ autem, si ipsius coëfficiens primus, secundus et tertius non simul pares sunt, sed unus, duo omnesve impares (in talem enim formam ex simili ratione forma prima $2xx+2yz$ per nullam substitutionem transformabilis esse poterit).

Quod igitur in exemplis artt. 273, 274 evenit, ut forma definita $\left(\begin{smallmatrix}19,&24,&50\\15,&28,&1\end{smallmatrix}\right)$ determinantis -1 ad hanc $xx+yy+zz$, atque forma indefinita $\left(\begin{smallmatrix}10,&26,&2\\7,&0,&4\end{smallmatrix}\right)$ determinantis 2 ad $2xx-2yz$ sive (quod eodem redit) ad $2xx+2yz$ reduceretur, per disquisitiones praecedentes a priori praevideri potuisset.

278.

Per formam ternariam, cuius indeterminatae sunt x, x', x'', *repraesentantur* tum numeri, tribuendo ipsis x, x', x'' valores determinatos, tum formae binariae per huiusmodi substitutiones

$$x = mt+nu, \quad x' = m't+n'u, \quad x'' = m''t+n''u$$

designantibus m, n, m' etc. numeros determinatos; t, u indeterminatas formae repraesentatae. Ad theoriam itaque completam formarum ternariarum requireretur solutio sequentium problematum: I. Invenire omnes repraesentationes numeri dati per formam ternariam datam. II. Invenire omnes repraesentationes formae binariae datae per ternariam datam. III. Diiudicare, utrum duae formae ternariae datae eiusdem determinantis aequivalentes sint, necne, et in casu priori omnes transformationes alterius in alteram invenire. IV. Diiudicare, utrum forma ternaria data aliam datam determinantis maioris implicet, necne, et in casu priori omnes transformationes illius in hanc assignare. De quibus problematibus longe difficilioribus quam analoga in formis binariis alio loco pluribus agemus: hic disquisitionem nostram restringimus ad ostendendum, quomodo problema primum ad secundum secundumque ad tertium reduci possit; tertium vero pro casibus quibusdam simplicissimis formarumque binariarum theoriam imprimis illustrantibus solvere docebimus; quartum hic omnino excludemus.

279.

Lemma. *Propositis tribus numeris integris quibuscunque* a, a', a'' *(qui tamen non omnes simul* $=0$*): invenire sex alios* B, B', B'', C, C', C'' *ita comparatos ut fiat*

$$B'C''-B''C' = a, \quad B''C-BC'' = a', \quad BC'-B'C = a''$$

Sol. Sit α div. comm. max. ipsorum a, a', a'', accipianturque integri A, A', A'' ita ut fiat

$$Aa+A'a'+A''a'' = \alpha$$

Porro accipiantur tres integri $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ ad lubitum ea sola conditione, ut tres numeri $\mathfrak{C}'A''-\mathfrak{C}''A'$, $\mathfrak{C}''A-\mathfrak{C}A''$, $\mathfrak{C}A'-\mathfrak{C}'A$, quos resp. per b, b', b'' ipsorumque divisorem communem maximum per $\vec{0}$ designabimus, non fiant simul $=0$. Tunc ponatur

$$a'b''-a''b' = a\vec{0}C, \quad a''b-ab'' = a\vec{0}C', \quad ab'-a'b = a\vec{0}C''$$

patetque, ipsos C, C', C'' fore integros. Denique accipiendo integros $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ ita ut fiat

$$\mathfrak{B}b+\mathfrak{B}'b'+\mathfrak{B}''b'' = \vec{0}$$

ponendo

$$\mathfrak{B}a+\mathfrak{B}'a'+\mathfrak{B}''a'' = h$$

et statuendo

$$B = \alpha\mathfrak{B}-hA, \quad B' = \alpha\mathfrak{B}'-hA', \quad B'' = \alpha\mathfrak{B}''-hA''$$

hi valores ipsorum B, B', B'', C, C', C'' aequationibus praescriptis satisfacient.

Invenitur enim

$$aB+a'B'+a''B'' = 0$$
$$bA+b'A'+b''A'' = 0 \quad \text{unde} \quad bB+b'B'+b''B'' = \alpha\vec{0}$$

Iam ex valoribus ipsorum C', C'' fit

$$\begin{aligned}\alpha\vec{0}(B'C''-B''C') &= ab'B'-a'bB'-a''bB''+ab''B'' \\ &= a(bB+b'B'+b''B'')-b(aB+a'B'+a''B'') = \alpha\vec{0}a\end{aligned}$$

adeoque $B'C''-B''C' = a$; similique modo invenitur $B''C-BC'' = a'$, $BC'-B'C = a''$. *Q. E. F.* — Ceterum analysis per quam haec solutio inventa est, nec non methodus ex una solutione omnes inveniendi, hic sunt supprimendae.

280.

Supponamus, formam binariam

$$att+2btu+cuu \ldots \varphi$$

cuius determinans $=D$, repraesentari per formam ternariam f, cuius indeterminatae x, x', x'', ponendo

$$x = mt+nu, \quad x' = m't+n'u, \quad x'' = m''t+n''u$$

ipsique f adiunctam esse formam F, cuius indeterminatae X, X', X''. Tunc per calculum facile confirmatur (designando coëfficientes formarum f, F per literas peculiares) sive etiam ex art. 268. II. protinus deducitur, numerum D repraesentari per F ponendo

$$X = m'n''-m''n', \quad X' = m''n-mn'', \quad X'' = mn'-m'n$$

quae repraesentatio numeri D repraesentationi formae φ per f *adiuncta* commode dici potest. Si valores ipsarum X, X', X'' divisorem communem non habent, brevitatis caussa hanc repraesentationem ipsius D *propriam* vocabimus, sin secus, *impropriam*, easdem denominationes etiam repraesentationi formae φ per f, cui illa repraes. ipsius D adiuncta est, tribuemus. Iam inventio omnium repraesentationum propriarum numeri D per formam F sequentibus momentis innititur:

I. Nulla repraesentatio ipsius D per F datur, quae non ex aliqua repraesentatione alicuius formae determinantis D per formam f deduci possit, *i. e.* tali repraesentationi adiuncta sit.

Sit enim repraesentatio quaecunque ipsius D per F haec: $X = L$, $X' = L'$, $X'' = L''$; accipiantur per lemma art. praec. m, m', m'', n, n', n'' ita ut fiat

$$m'n''-m''n' = L, \quad m''n-mn'' = L', \quad mn'-m'n = L''$$

transeatque f per substitutionem

$$x = mt+nu, \quad x' = m't+n'u, \quad x'' = m''t+n''u$$

in formam binariam $\varphi = att+2btu+cuu$. Tunc facile perspicietur, D fore determinantem formae φ ipsiusque repraesentationi per f repraesentationem propositam ipsius D per F adiunctam.

Ex. Sit $f = xx+x'x'+x''x''$, adeoque $F = -XX-X'X'-X''X''$; $D = -209$; ipsiusque repraesentatio per F haec $X = 1$, $X' = 8$, $X'' = 12$;

hinc inveniuntur valores ipsorum m, m', m'', n, n', n'' hi $-20, 1, 1, -12, 0, 1$ resp., atque $\varphi = 402tt + 482tu + 145uu$.

II. Si φ, χ sunt formae binariae proprie aequivalentes, quaevis repraesentatio ipsius D per F alicui repraesentationi formae φ per f adiuncta, etiam alicui repraesentationi formae χ per f adiuncta erit.

Sint p, q indeterminatae formae χ; transeat φ in χ per substitutionem propriam $t = \alpha p + \beta q$, $u = \gamma p + \delta q$, sitque aliqua repraesentatio formae φ per f haec

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u \ldots (R)$$

Tunc nullo negotio perspicitur, si ponatur

$$\begin{array}{llll} \alpha m + \gamma n = g, & \alpha m' + \gamma n' = g', & \alpha m'' + \gamma n'' = g'' \\ \beta m + \delta n = h, & \beta m' + \delta n' = h', & \beta m'' + \delta n'' = h'' \end{array}$$

formam χ repraesentatum iri per f statuendo

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q \ldots (R')$$

calculoque facto invenitur (propter $\alpha\delta - \beta\gamma = 1$) esse

$$g'h'' - g''h' = m'n'' - m''n', \quad g''h - gh'' = m''n - mn'', \quad gh' - g'h = mn' - m'n$$

i. e. repraesentationibus R, R' eadem repraesentatio ipsius D per F adiuncta est.

Ita in ex. praec. formae φ aequivalere invenitur $\chi = 13pp - 10pq + 18qq$, in quam illa transit per substitutionem propriam $t = -3p + q$, $u = 5p - 2q$; hinc invenitur repraesentatio formae χ per f haec $x = 4q$, $x' = -3p + q$, $x'' = 2p - q$, ex qua eadem numeri -209 repraesentatio deducitur, a qua profecti eramus.

III. Denique si duae formae binariae φ, χ determinantis D, quarum indeterminatae sunt t, u; p, q, per f repraesentari possunt, alicuique repraesentationi unius eadem repraesentatio propria ipsius D per F adiuncta est, atque alicui repraesentationi alterius, illae formae necessario erunt proprie aequivalentes. Supponamus φ repraesentari per f ponendo

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$$

χ vero statuendo

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q$$

atque esse

$$\begin{array}{l} m'n'' - m''n' = g'h'' - g''h' = L \\ m''n - mn'' = g''h - gh'' = L' \\ mn' - m'n = gh' - g'h = L'' \end{array}$$

Accipiantur integri l, l', l'' ita ut fiat $Ll + L'l' + L''l'' = 1$, ponaturque

$$\begin{array}{l} n'l'' - n''l' = M, \quad n''l - nl'' = M', \quad nl' - n'l = M'' \\ l'm'' - l''m' = N, \quad l''m - lm'' = N', \quad lm' - l'm = N'' \end{array}$$

denique statuatur

$$\begin{array}{l} gM + g'M' + g''M'' = \alpha, \quad hM + h'M' + h''M'' = \beta \\ gN + g'N' + g''N'' = \gamma, \quad hN + h'N' + h''N'' = \delta \end{array}$$

Hinc facile deducitur

$$\begin{array}{l} \alpha m + \gamma n = g - l(gL + g'L' + g''L'') = g \\ \beta m + \delta n = h - l(hL + h'L' + h''L'') = h \end{array}$$

similique modo

$$\alpha m' + \gamma n' = g', \quad \beta m' + \delta n' = h', \quad \alpha m'' + \gamma n'' = g'', \quad \beta m'' + \delta n'' = h''$$

Hinc patet, $mt + nu$, $m't + n'u$, $m''t + n''u$ transire per substitutionem

$$t = \alpha p + \beta q, \quad u = \gamma p + \delta q \ldots (S)$$

in $gp + hq$, $g'p + h'q$, $g''p + h''q$ resp., unde manifestum est, φ transire per substitutionem S in eandem formam, in quam f transeat ponendo

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q$$

adeoque in formam χ, cui itaque aequivalet. Denique per substitutiones debitas facile invenitur

$$\alpha\delta - \beta\gamma = (Ll + L'l' + L''l'')^2 = 1$$

quocirca substitutio S est propria, formaeque φ, χ proprie aequivalentes.

Ex his observationibus derivantur regulae sequentes ad inveniendum omnes repraesentationes proprias ipsius D per F: Evolvantur omnes classes formarum binariarum determinantis D, et ex singulis una forma ad libitum eligatur; quaerantur omnes repraesentationes propriae singularum harum formarum per f (reiectis iis, quae forte per f repraesentari nequeunt), et ex singulis hisce repraesentationibus deducantur repraesentationes numeri D per F. Ex I et II manifestum est, hoc modo omnes repraesentationes proprias possibiles obtineri, adeoque solutionem esse completam; ex III, transformationes formarum e classibus diversis certo producere repraesentationes diversas.

281.

Investigatio repraesentationum *impropriarum* numeri dati D per formam F ad casum praecedentem facile reducitur. Scilicet manifestum est, si D per nullum quadratum (praeter 1) divisibilis sit, tales repraesentationes omnino non dari; sin secus, metientibus ipsum D quadratis $\lambda\lambda$, $\mu\mu$, $\nu\nu$ etc., omnes repraesentationes improprias ipsius D per F inveniri, si omnes repraesentationes propriae numerorum $\frac{D}{\lambda\lambda}, \frac{D}{\mu\mu}, \frac{D}{\nu\nu}$ etc. per eandem formam evolvantur, indeterminatarumque valores per λ, μ, ν etc. resp. multiplicentur.

Hoc itaque modo inventio omnium repraesentationum numeri dati per formam ternariam datam, *quae alicui formae ternariae adiuncta est*, a problemate secundo pendet; ad hunc vero casum, qui primo aspectu minus late patere videri posset, reliqui ita reducuntur. Sit D numerus repraesentandus per formam $\left(\begin{smallmatrix} g, & g', & g'' \\ h, & h', & h'' \end{smallmatrix}\right)$, cuius determinans Δ; et cui adiuncta est forma $\left(\begin{smallmatrix} G, & G', & G'' \\ H, & H', & H'' \end{smallmatrix}\right) = f$. Tunc huic rursus adiuncta erit $\left(\begin{smallmatrix} \Delta g, & \Delta g', & \Delta g'' \\ \Delta h, & \Delta h', & \Delta h'' \end{smallmatrix}\right) = F$; patetque, repraesentationes numeri ΔD per F (quarum investigatio a praecc. pendet) omnino identicas esse cum repraesentationibus numeri D per formam propositam. — Ceterum quando omnes coëfficientes formae f divisorem communem μ habent, perspicuum est, omnes coëfficientes formae F divisibiles esse per $\mu\mu$, quocirca etiam ΔD per $\mu\mu$ divisibilis esse debebit (alioquin nullae repraesentationes darentur); repraesentationesque numeri D per formam propositam coincident cum repraesentationibus numeri $\frac{\Delta D}{\mu\mu}$ per formam, quae oritur ex F, dividendo singulos coëfficientes per $\mu\mu$, quae forma adiuncta erit ei, quae oritur ex f, dividendo singulos coëfficientes per μ.

Denique observamus, hanc problematis primi solutionem in unico casu, ubi

$D = 0$, non esse applicabilem; hic enim omnes formae binariae determinantis D in multitudinem finitam classium non distribuuntur; infra autem hunc casum ex aliis principiis solvemus.

282.

Investigatio repraesentationum formae binariae datae, cuius determinans non $= 0$ *), per ternariam datam pendet ab observationibus sequentibus:

I. Ex quavis repraesentatione propria formae binariae $(p, q, r) = \varphi$ determinantis D per ternariam f determinantis Δ deduci possunt integri B, B' tales ut sit

$$BB \equiv \Delta p, \quad BB' \equiv -\Delta q, \quad B'B' \equiv \Delta r \pmod{D}$$

i. e. valor expressionis $\sqrt{\Delta}(p, -q, r) \pmod{D}$. Habeatur repraesentatio propria formae φ per f haec

$$x = \alpha t + \vec{\alpha} u, \quad x' = \alpha' t + \vec{\alpha}' u, \quad x'' = \alpha'' t + \vec{\alpha}'' u$$

(designantibus x, x', x''; t, u indeterminatas formarum f, φ); accipiantur integri $\gamma, \gamma', \gamma''$ ita ut

$$(\alpha'\vec{\alpha}'' - \alpha''\vec{\alpha}')\gamma + (\alpha''\vec{\alpha} - \alpha\vec{\alpha}'')\gamma' + (\alpha\vec{\alpha}' - \alpha'\vec{\alpha})\gamma''$$

$= k$ fiat vel $= +1$ vel $= -1$, transeatque f per substitutionem

$$\begin{matrix} \alpha, & \vec{\alpha}, & \gamma \\ \alpha', & \vec{\alpha}', & \gamma' \\ \alpha'', & \vec{\alpha}'', & \gamma'' \end{matrix}$$

in formam $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right) = g$, cui adiuncta sit $\left(\begin{smallmatrix} A, & A', & A'' \\ B, & B', & B'' \end{smallmatrix}\right) = G$. Tunc manifestum est, fore $a = p$, $b'' = q$, $a' = r$, $A'' = D$, atque Δ determinantem formae g; unde

$$BB = \Delta p + A'D, \quad BB' = -\Delta q + B''D, \quad B'B' = \Delta r + AD$$

Ita *e. g.* forma $19tt + 6tu + 41uu$ repraesentatur per $xx + x'x' + x''x''$ ponendo $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$; unde statuendo $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$.

*) Hunc casum per methodum aliquantum diversam tractandum hoc loco brevitatis caussa praeterimus.

eruitur $B \equiv -171$, $B' \equiv 27$, sive valor $(-171, 27)$ expr. $\sqrt{-1}\,(19, -3, 41)$ (mod. 770).

Hinc iam sequitur, si $\Delta(p, -q, r)$ non sit residuum quadratum ipsius D, φ per nullam formam ternariam determinantis Δ proprie repraesentabilem esse posse; in eo itaque casu, ubi Δ, D inter se primi sunt, Δ numerus characteristicus formae φ esse debebit.

II. Quum $\gamma, \gamma', \gamma''$ infinite multis modis diversis determinari possint, etiam alii atque alii valores ipsorum B, B' inde prodibunt, qui quem nexum inter se habeant videamus. Ponamus, etiam $\delta, \delta', \delta''$ ita comparatos esse, ut $(\alpha'\vec{\sigma}''-\alpha''\vec{\sigma}')\delta+(\alpha''\vec{\sigma}-\alpha\vec{\sigma}'')\delta'+(\alpha\vec{\sigma}'-\alpha'\vec{\sigma})\delta'' = \mathfrak{k}$ fiat vel $=+1$ vel $=-1$, formamque f transire per substitutionem

$$\begin{matrix} \alpha, & \vec{\sigma}, & \delta \\ \alpha', & \vec{\sigma}', & \delta' \\ \alpha'', & \vec{\sigma}'', & \delta'' \end{matrix}$$

in $\left(\begin{smallmatrix} \mathfrak{a}, & \mathfrak{a}', & \mathfrak{a}'' \\ \mathfrak{b}, & \mathfrak{b}', & \mathfrak{b}'' \end{smallmatrix}\right) = \mathfrak{g}$, cui adiuncta $\left(\begin{smallmatrix} \mathfrak{A}, & \mathfrak{A}', & \mathfrak{A}'' \\ \mathfrak{B}, & \mathfrak{B}', & \mathfrak{B}'' \end{smallmatrix}\right) = \mathfrak{G}$. Tunc g, $\mathfrak{g}$ erunt aequivalentes, adeoque etiam G et $\mathfrak{G}$, et per applicationem praeceptorum in artt. 269, 270 traditorum *) invenitur, si statuatur

$$\begin{aligned} (\vec{\sigma}'\gamma''-\vec{\sigma}''\gamma')\delta+(\vec{\sigma}''\gamma-\vec{\sigma}\gamma'')\delta'+(\vec{\sigma}\gamma'-\vec{\sigma}'\gamma)\delta'' &= \zeta \\ (\gamma'\alpha''-\gamma''\alpha')\delta+(\gamma''\alpha-\gamma\alpha'')\delta'+(\gamma\alpha'-\gamma'\alpha)\delta'' &= \eta \end{aligned}$$

formam $\mathfrak{G}$ transire in G per substitutionem

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k} \end{matrix}$$

Hinc erit

$$B = \eta\mathfrak{k}D+\mathfrak{k}k\mathfrak{B}, \quad B' = \zeta\mathfrak{k}D+\mathfrak{k}k\mathfrak{B}'$$

adeoque, propter $\mathfrak{k}k = \pm 1$, vel $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$, vel $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mod. D). In casu priori valores (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ aequivalentes vocamus, in posteriori oppositos; repraesentationem formae φ autem ad quemlibet valorem

*) Eruendo ex transf. formae f in g, transformationem formae g in f; ex hac atque transf. formae f in $\mathfrak{g}$, transf. formae g in $\mathfrak{g}$; denique ex hac, per transpositionem, transf. formae $\mathfrak{G}$ in G.

expr. $\sqrt{\Delta}(p, -q, r)\,(\mathrm{mod}.\, D)$, qui ex ipsa per methodum in I deduci potest, *pertinere* dicemus. Hinc omnes valores, ad quos eadem repraesentatio pertinet, vel aequivalentes erunt vel oppositi.

III. Vice versa autem, si ut ante in I repraesentatio formae φ per f haec $x = \alpha t+\vec{\sigma}u$ etc. ad valorem (B, B') pertinet, qui inde deducitur adiumento transformationis

$$\begin{matrix} \alpha, & \vec{\sigma}, & \gamma \\ \alpha', & \vec{\sigma}', & \gamma' \\ \alpha'', & \vec{\sigma}'', & \gamma'' \end{matrix}$$

eadem quoque ad quemvis alium valorem $(\mathfrak{B}, \mathfrak{B}')$ pertinebit, qui illi vel aequivalens est vel oppositus; *i. e.* loco ipsorum $\gamma, \gamma', \gamma''$ alios integros $\delta, \delta', \delta''$ accipere licebit, pro quibus aequatio (2) haec

$$(\alpha'\vec{\sigma}''-\alpha''\vec{\sigma}')\delta+(\alpha''\vec{\sigma}-\alpha\vec{\sigma}'')\delta'+(\alpha\vec{\sigma}'-\alpha'\vec{\sigma})\delta'' = \pm 1$$

locum habeat, et qui ita comparati sint, ut coëfficiens 4 et 5 in forma ei adiuncta, in quam f per substitutionem (S)

$$\begin{matrix} \alpha, & \vec{\sigma}, & \delta \\ \alpha', & \vec{\sigma}', & \delta' \\ \alpha'', & \vec{\sigma}'', & \delta'' \end{matrix}$$

transit, resp. fiant $= \mathfrak{B}, \mathfrak{B}'$. Statuatur enim

$$\pm B = \mathfrak{B}+\eta D, \quad \pm B' = \mathfrak{B}'+\zeta D$$

(accipiendo hic et postea signa superiora vel inferiora, prout valores (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ aequivalentes sunt vel oppositi), unde ζ, η erunt integri, transeatque g per substitutionem

$$\begin{matrix} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{matrix}$$

in formam $\mathfrak{g}$, cuius determinantem esse Δ, in forma adiuncta vero coëfficientes 4 et 5 resp. $= \mathfrak{B}, \mathfrak{B}'$ fieri facile perspicietur. Faciendo autem

$$\alpha\zeta+\vec{\sigma}\eta\pm\gamma = \delta, \quad \alpha'\zeta+\vec{\sigma}'\eta\pm\gamma' = \delta', \quad \alpha''\zeta+\vec{\sigma}''\eta\pm\gamma'' = \delta''$$

nullo negotio patebit, f per substitutionem (S) transire in $\mathfrak{g}$, atque aequationi (Ω) satisfactum esse. *Q. E. D.*

283.

Ex his principiis deducitur methodus sequens, omnes repraesentationes proprias formae binariae

$$\varphi = ptt+2qtu+ruu$$

determinantis D per ternariam f determinantis Δ inveniendi.

I. Eruantur omnes valores diversi (*i. e.* non-aequivalentes) expressionis $\sqrt{\Delta}(p, -q, r) \pmod{D}$. Hoc problema pro eo casu, ubi φ est forma primitiva atque Δ ad D primus, supra (art. 233) solutum est, casusque reliqui ad hunc facillime reducuntur, quam tamen rem fusius hic explicare brevitas non permittit. Observamus tantummodo, quoties Δ ad D primus sit, expressionem $\Delta(p, -q, r)$ residuum quadraticum ipsius D esse non posse, nisi φ fuerit forma primitiva. Supponendo enim

$$\Delta p = BB-DA', \quad -\Delta q = BB'-DB'', \quad \Delta r = B'B'-DA''$$

fit

$$(DB''-\Delta q)^2 = (DA'+\Delta p)(DA''+\Delta r)$$

hinc, per evolutionem et substituendo $qq-pr$ pro D, fit

$$(qq-pr)(B'B''-A'A'')-\Delta(Ap+2B''q+A''r)+\Delta\Delta = 0$$

unde facile concluditur, si p, q, r divisorem communem haberent, hunc etiam ipsum $\Delta\Delta$ metiri; tunc vero Δ ad D primus esse non posset. Quare p, q, r divisorem communem habere nequeunt, sive φ erit forma primitiva.

II. Designemus multitudinem horum valorum per m, supponamusque, inter eos reperiri n valores, qui sibi ipsis oppositi sint (statuendo $n = 0$, quando tales non adsunt). Tunc manifestum est, ex $m-n$ reliquis valoribus binos semper oppositos fore (quoniam cuncti valores complete haberi supponuntur); reiiciatur e binis quibusque valoribus oppositis unus ad libitum, remanebuntque omnino valores $\frac{1}{2}(m+n)$. Ita *e. g.* ex octo valoribus expr. $\sqrt{-1}\,(19, -3, 41)$

(mod. 770) his (39, 237), (171, −27), (269, −83), (291, −127), (−39, −237), (−171, 27), (−269, 83), (−291, 127), quatuor posteriores sunt reiiciendi, tamquam quatuor prioribus oppositi. Ceterum perspicuum est, si (B, B') sit valor sibi ipsi oppositus, $2B$, $2B'$ et proin etiam $2\Delta p$, $2\Delta q$, $2\Delta r$ per D divisibiles fore; quodsi itaque Δ, D inter se primi sunt, etiam $2p$, $2q$, $2r$ per D divisibiles erunt, et quum, per I, in hoc casu etiam p, q, r divisorem communem habere nequeant, etiam 2 per D divisibilis esse debebit, quod fieri nequit nisi D vel $= \pm 1$, vel $= \pm 2$. Quamobrem pro omnibus valoribus ipsius D maioribus quam 2 semper erit $n = 0$, si Δ ad D est primus.

III. His ita factis manifestum est, quamvis repraesentationem propriam formae φ per f necessario ad aliquem e valoribus remanentibus pertinere debere, et quidem ad unicum tantum. Quare hi valores successive sunt percurrendi, repraesentationesque ad singulos pertinentes investigandae. Ut inveniantur repraesentationes ad valorem *datum* (B, B') pertinentes, primo determinanda est forma ternaria $g = \left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$, cuius determinans $= \Delta$ et in qua $a = p$, $b'' = q$, $a' = r$, $ab-b'b'' = B$, $a'b'-bb'' = B'$; valores ipsorum a'', b, b' hinc inveniuntur adiumento aequationum in II art. 276, ex quibus facile perspicitur, in eo casu, ubi Δ, D inter se primi sint, b, b' a'' necessario fieri integros (nempe quoniam hi tres numeri, multiplicati tum per D tum per Δ integros producunt). Iam si vel aliquis coëfficientium b, b', b'' fractus est, vel formae f, g non sunt aequivalentes: nullae repraesentationes formae φ per f ad (B, B') pertinentes dari possunt; si vero b, b', a'' sunt integri, formaeque f, g aequivalentes, quaevis transformatio illius in hanc, ut

$$\begin{matrix} \alpha, & \vec{6}, & \gamma \\ \alpha', & \vec{6}', & \gamma' \\ \alpha'', & \vec{6}'', & \gamma'' \end{matrix}$$

talem repraesentationem suppeditat, puta

$$x = \alpha t+\vec{6}u, \quad x' = \alpha' t+\vec{6}'u, \quad x'' = \alpha'' t+\vec{6}''u$$

manifestoque nulla huiusmodi repraesentatio exstare poterit, quae non ex aliqua transformatione deduci posset. Hoc itaque modo ea problematis secundi pars, quae investigat repraesentationes *proprias*, ad problema tertium iam est reducta.

IV. Ceterum transformationes diversae formae f in g semper producunt repraesentationes diversas, eo solo casu excepto, ubi valor (B, B') sibi ipsi oppositus est, in quo binae transformationes unicam semper repraesentationem suppeditant. Supponendo enim, f transire in g etiam per substitutionem

$$\begin{matrix} \alpha, & \vec{o}, & \delta \\ \alpha', & \vec{o}', & \delta' \\ \alpha'', & \vec{o}'', & \delta'' \end{matrix}$$

(quae eandem repr. praebet ut transf. praec.), denotandoque per k, $\mathfrak{k}$, ζ, η numeros eosdem ut in II art. praec., erit

$$B = k\mathfrak{k}B + \eta\mathfrak{k}D, \quad B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D$$

si itaque vel uterque k, $\mathfrak{k}$ supponitur $= +1$, vel uterque $= -1$, erit (quia casum $D = 0$ exclusimus) $\zeta = 0$, $\eta = 0$, unde facile sequitur $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$; quare illae duae transformationes in eo solo casu diversae esse possunt, ubi alter numerorum $k, \mathfrak{k}$ est $+1$, alter -1; tunc erit $B \equiv -B$, $B' \equiv -B'$, (mod. D), sive valor (B, B') sibi ipsi oppositus.

V. Ex iis, quae supra (art. 271) de criteriis formarum definitarum et indefinitarum tradidimus, facile sequitur, si Δ sit positivus, D negativus, atque φ forma negativa, g fieri formam definitam negativam; si vero Δ sit positivus, atque vel D positivus, vel D negativus et φ forma positiva, g evadere formam indefinitam. Iam quum f, g certo aequivalentes esse nequeant, nisi respectu huius qualitatis similes sint, manifestum est, formas binarias determinantis positivi nec non positivas, per ternariam negativam proprie repraesentari non posse, neque formas binarias negativas per ternariam indefinitam determinantis positivi; sed per formam ternariam prioris posteriorisve speciei unice binarias posterioris priorisve resp. Simili modo concluditur, per formam ternariam determinantis negativi definitam (*i. e.* positivam) unice repraesentari binarias positivas, per indefinitam unice negativas et formas det. positivi.

284.

Quum repraesentationes *impropriae* formae binariae φ determinantis D per ternariam f, cui adiuncta est F, eae sint, ex quibus repraesentationes

impropriae numeri D per formam F sequuntur, φ per f manifesto nequit improprie repraesentari, nisi D factores quadratos implicet. Ponamus, omnia quadrata ipsum D metientia (praeter 1) esse ee, $e'e'$, $e''e''$ etc. (quorum multitudo finita erit, quia supponimus, non esse $D = 0$), praebebitque quaelibet repr. impr. formae φ per f repraesentationem numeri D per F, in qua valores indeterminatarum aliquem e numeris e, e', e'' etc. pro divisore communi maximo habebunt; hoc respectu brevitatis caussa quamvis repr. impr. formae φ ad divisorem quadratum ee vel $e'e'$ vel $e''e''$ etc. *pertinere* dicemus. Iam omnes repr. formae φ ad eundem divisorem quadratum *datum* ee (cuius radicem e positive acceptam supponimus) pertinentes per regulas sequentes inveniuntur, ex quarum demonstratione synthetica, propter brevitatem hic praeferenda, analysis per quam evolutae sunt, facile restitui poterit.

Primo eruantur omnes formae binariae determinantis $\frac{D}{ee}$, quae in formam φ transeunt per substitutionem propriam talem $T = \varkappa t + \lambda u$, $U = \mu u$, designantibus T, U indeterminatas talis formae; t, u indet. formae φ; $\varkappa$, μ integros positivos (quorum productum itaque $= e$); λ integrum positivum minorem quam μ (sive etiam cifram). Hae formae, cum transformationibus respondentibus, ita inveniuntur:

Aequetur $\varkappa$ successive singulis divisoribus ipsius e positive acceptis (inclusis etiam 1 et e), fiatque $\mu = \frac{e}{\varkappa}$; pro singulis valoribus determinatis ipsorum $\varkappa$, μ tribuantur ipsi λ omnes valores integri a 0 usque ad $\mu - 1$, quo pacto omnes transformationes certo habebuntur. Iam forma, quae per quamvis substitutionem $T = \varkappa t + \lambda u$, $U = \mu u$ in φ transit, invenitur investigando formam, in quam φ transit per hanc $t = \frac{1}{\varkappa} T - \frac{\lambda}{e} U$, $u = \frac{1}{\mu} U$; sic formae singulis transformationibus respondentes obtinebuntur; sed ex omnibus his formis eae tantum retinendae sunt, in quibus omnes tres coëfficientes evadunt integri *).

Secundo ponamus Φ esse aliquam ex hisce formis, quae in φ transeat per subst. $T = \varkappa t + \lambda u$, $U = \mu u$; investigentur omnes repraesentationes *propriae*

*) Si de hoc problemate fusius agere hic liceret, solutionem admodum contrahere possemus. Id statim obvium est, pro $\varkappa$ alios divisores ipsius e accipere non esse necessarium, nisi quorum quadratum metiatur coëfficientem primum formae φ. Ceterum hoc problema, ex quo etiam solutiones simpliciores probl. artt. 213, 214 deduci possunt, alia occasione idonea resumere nobis reservamus.

formae Φ per f (si quae dantur), exhibeanturque indefinite per

$$x = \mathfrak{A}T + \mathfrak{B}U, \quad x' = \mathfrak{A}'T + \mathfrak{B}'U, \quad x'' = \mathfrak{A}''T + \mathfrak{B}''U \ldots (\mathfrak{R})$$

denique ex singulis $(\mathfrak{R})$ deducatur repraesentatio

$$x = \alpha t + \vec{\alpha} u, \quad x' = \alpha' t + \vec{\alpha}' u, \quad x'' = \alpha'' t + \vec{\alpha}'' u. \ldots . (\rho)$$

per aequationes

$$\begin{aligned} &\alpha = \varkappa\mathfrak{A}, && \alpha' = \varkappa\mathfrak{A}', && \alpha'' = \varkappa\mathfrak{A}'' \ldots\ldots\ldots (R)\\ &\vec{\alpha} = \lambda\mathfrak{A} + \mu\mathfrak{B}, && \vec{\alpha}' = \lambda\mathfrak{A}' + \mu\mathfrak{B}', && \vec{\alpha}'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}'' \end{aligned}$$

Eodem prorsus modo, ut forma Φ, tractentur formae reliquae per regulam primam inventae (si plures adsunt), ita ut ex singulis cuiusque repraesentationibus propriis aliae repraesentationes deriventur, dicoque, hoc modo prodire cunctas repraesentationes formae φ ad divisorem ee pertinentes, et quidem quamlibet semel tantum.

Dem. I. Formam ternariam f per quamvis substitutionem (ρ) revera transire in φ, tam obvium est, ut explicatione ampliori non opus sit; quamlibet autem repr. (ρ) esse impropriam et ad divisorem ee pertinere, inde patet, quod numeri $\alpha'\vec{\alpha}'' - \alpha''\vec{\alpha}'$, $\alpha''\vec{\alpha} - \alpha\vec{\alpha}''$, $\alpha\vec{\alpha}' - \alpha'\vec{\alpha}$ resp. fiunt $= e(\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B})$, unde illorum divisor comm. max. manifesto erit e (quoniam $(\mathfrak{R})$ est repraesentatio propria).

II. Ostendemus, ex quavis repraesentatione data (ρ) formae φ, inveniri posse repraesentationem propriam formae determinantis $\frac{D}{ee}$, inter formas per regulam primam inventas contentae, sive ex valoribus datis ipsorum $\alpha, \alpha', \alpha''$, $\vec{\alpha}, \vec{\alpha}', \vec{\alpha}''$ deduci posse valores integros ipsorum $\varkappa, \lambda, \mu$, conditionibus praescriptis, atque valores ipsorum $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$, $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$, aequationibus (R) satisfacientes, et quidem unico tantum modo. Primo statim patet ex tribus aequ. primis in (R), pro $\varkappa$ accipi debere divisorem communem maximum ipsorum $\alpha, \alpha', \alpha''$ signo positivo (quum enim $\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}''$, $\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B}$ divisorem communem non habere debeant, etiam $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ div. comm. habere nequeunt); hinc etiam $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ determinati erunt, nec non $\mu = \frac{e}{\varkappa}$ (quem necessario integrum fieri facile perspicitur). Ponamus, tres integros a, a', a'' ita acceptos esse, ut fiat $a\mathfrak{A} + a'\mathfrak{A}' + a''\mathfrak{A}'' = 1$, scribamusque brevitatis caussa k pro $a\mathfrak{B} + a'\mathfrak{B}' + a''\mathfrak{B}''$.

Tunc ex tribus ultimis aeq. (R) sequitur, esse debere $a\vec{\alpha} + a'\vec{\alpha}' + a''\vec{\alpha}'' = \lambda + \mu k$, unde statim patet, pro λ unicum tantummodo valorem inter limites 0 et $\mu - 1$ situm dari. Quo facto quum etiam $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ valores determinatos nanciscantur, nihil superest, nisi ut demonstremus, hos semper hinc integros evadere. Fiet autem

$$\begin{aligned} \mathfrak{B} = \tfrac{1}{\mu}(\vec{\alpha} - \lambda\mathfrak{A}) &= \tfrac{1}{\mu}(\vec{\alpha}(1 - a\mathfrak{A}) - \mathfrak{A}(a'\vec{\alpha}' + a''\vec{\alpha}'')) + \mathfrak{A}k\\ &= \tfrac{1}{\mu}(a''(\mathfrak{A}''\vec{\alpha} - \mathfrak{A}\vec{\alpha}'') - a'(\mathfrak{A}\vec{\alpha}' - \mathfrak{A}'\vec{\alpha})) + \mathfrak{A}k\\ &= \tfrac{1}{e}(a''(\alpha''\vec{\alpha} - \alpha\vec{\alpha}'') - a'(\alpha\vec{\alpha}' - \alpha'\vec{\alpha})) + \mathfrak{A}k \end{aligned}$$

eritque adeo manifesto integer, similiterque facile confirmatur, etiam ipsos $\mathfrak{B}', \mathfrak{B}''$ valores integros nancisci. — Ex his ratiociniis colligitur, nullam repraesentationem impropriam formae φ per f, ad divisorem ee pertinentem, exstare posse, quae per methodum traditam vel non vel pluries obtineatur.

Quodsi iam eodem modo reliqui divisores quadrati ipsius D tractantur, repraesentationesque ad singulos pertinentes eruuntur, cunctae repraesentationes impropriae formae φ per f habebuntur.

Ceterum ex hac solutione facile deducitur, theorema ad finem art. praec. pro repraess. propriis traditum etiam ad improprias patere, scilicet generaliter nullam formam binariam positivam det. negativi per ternariam negativam repraesentari posse etc.; patet enim, si φ sit forma talis binaria, quae propter illud theorema per f proprie repraesentari nequeat, etiam omnes formas determinantium $\frac{D}{ee}$, $\frac{D}{e'e'}$ etc., ipsam φ implicantes per f proprie repraesentari non posse, quum hae formae omnes determinantem eodem signo affectum habeant ut φ, et quoties hi determinantes negativi sunt, vel omnes evadant formae positivae vel negativae, prout φ ad illas vel ad has pertinet.

285.

De quaestionibus problema tertium nobis propositum constituentibus (ad quod duo priora in praecc. sunt reducta), scilicet propositis duabus formis ternariis eiusdem determinantis, diiudicare, utrum aequivalentes sint necne, et in casu priori omnes transformationes alterius in alteram invenire, pauca tantum hoc loco inserere possumus, quum solutio completa, qualem pro problematibus analogis in formis binariis tradidimus, hic adhuc maioribus difficultatibus sit obnoxia.

Quamobrem ad quosdam casus particulares, propter quos praecipue haecce digressio instituta est, disquisitionem nostram limitabimus.

I. Pro determinante $+1$ supra ostensum est, omnes formas ternarias in duas classes distribui, quarum altera omnes formas indefinitas, altera omnes definitas (negativas) contineat. Hinc statim concluditur, duas formas ternarias quascunque det. 1 aequivalentes esse, si vel utraque sit definita vel utraque indefinita; si vero altera sit definita, altera indefinita, aequivalentiam locum non habere (propositionis pars posterior manifesto valet generaliter pro formis determinantis cuiuscunque). — Simili modo duae formae quaecunque determinantis -1 certo aequivalebunt, si vel utraque definita est, vel utraque indefinita. — Duae formae definitae determinantis 2 semper aequivalebunt; duae indefinitae non aequivalebunt, si in altera tres coëfficientes primi omnes pares sunt, in altera vero non omnes sunt pares; in casibus reliquis (si vel utraque tres coëfficientes primos simul pares habet, vel neutra) aequivalebunt. — Hoc modo adhuc multo plures propositiones speciales exhibere possemus, si supra (art. 277) plura exempla evoluta fuissent.

II. Pro omnibus hisce casibus poterit etiam, designantibus f, f' formas ternarias aequivalentes, transformatio una alterius in alteram inveniri. Nam pro omnibus casibus in quavis classe formarum ternariarum multitudo satis parva formarum supra assignata est, ad quarum aliquam per methodos uniformes quaevis forma eiusdem classis reduci possit; has omnes ad unicam reducere ibidem docuimus. Sit F haec forma in ea classe, in qua sunt f, f', poteruntque per praecepta supra tradita inveniri transformationes formarum f, f' in F, nec non formae F in f, f'. Hinc per art. 270 deduci poterunt transformationes formae f in f' formaeque f' in f.

III. Superesset itaque tantummodo, ostendere, quo pacto ex una transformatione formae ternariae f in aliam f' omnes transformationes possibiles derivari possint. Hoc problema pendet ab alio simpliciori, scilicet invenire omnes transformationes formae ternariae f in se ipsam. Nimirum si f per plures substitutiones (τ), (τ'), (τ'') etc. in se ipsam et per substitutionem (t) in f' transit, patet si ad normam art. 270 combinetur transformatio (t) cum (τ), (τ'), (τ'') etc., prodire transformationes, per quas omnes f in f' transeat; praeterea per calculum facile probatur, quamvis transformationem formae f in f' hoc modo deduci posse e combinatione transformationis datae (t) formae f in f' cum aliqua (et quidem

unica) transformatione formae f in se ipsam, adeoque ex combinatione transformationis datae formae f in f' cum *omnibus* transformationibus formae f in se ipsam oriri *omnes* transformationes formae f in f', et quidem singulas semel tantum.

Investigationem omnium transformationum formae f in se ipsam ad eum casum hic restringimus, ubi f est forma definita, cuius coëfficientes 4, 5, 6 omnes $= 0$ *). Sit itaque $f = (\begin{smallmatrix} a, & a', & a'' \\ 0, & 0, & 0 \end{smallmatrix})$, exhibeanturque omnes substitutiones, per quas f in se ipsam transit, indefinite per

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

ita ut satisfieri debeat aequationibus

$$\begin{aligned}
a\alpha\alpha + a'\alpha'\alpha' + a''\alpha''\alpha'' &= a \quad \ldots \quad (\Omega) \\
a\beta\beta + a'\beta'\beta' + a''\beta''\beta'' &= a' \\
a\gamma\gamma + a'\gamma'\gamma' + a''\gamma''\gamma'' &= a'' \\
a\alpha\beta + a'\alpha'\beta' + a''\alpha''\beta'' &= 0 \\
a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' &= 0 \\
a\beta\gamma + a'\beta'\gamma' + a''\beta''\gamma'' &= 0
\end{aligned}$$

Iam tres casus sunt distinguendi:

I. Quando a, a', a'' (qui idem signum habebunt) omnes sunt inaequales, supponamus $a < a'$, $a' < a''$ (si alius magnitudinis ordo adest, eaedem conclusiones prorsus simili modo eruentur). Tunc aequ. prima in (Ω) manifesto requirit, ut sit $\alpha' = \alpha'' = 0$, adeoque $\alpha = \pm 1$; hinc per aequ. 4, 5 erit $\beta = 0$, $\gamma = 0$; similiter ex aequ. 2 erit $\beta'' = 0$, et proin $\beta' = \pm 1$; hinc fit, per aequ. 6, $\gamma' = 0$, et per 3, $\gamma'' = \pm 1$, ita ut (ob signorum ambiguitatem independentem) omnino habeantur 8 transformationes diversae.

II. Quando e numeris a, a', a'' duo sunt aequales, *e. g.* $a' = a''$, tertius inaequalis, supponamus

primo $a < a'$. Tunc eodem modo ut in casu praec. erit $\alpha' = 0$, $\alpha'' = 0$, $\alpha = \pm 1$, $\beta = 0$, $\gamma = 0$; ex aequ. 2, 3, 6 autem facile deducitur, esse debere

*) Casus reliqui ubi f est forma definita, ad hunc reduci possunt; si vero f est forma indefinita, methodus omnino diversa adhibenda, transformationumque multitudo infinita erit.

vel $\vec{\sigma}' = \pm 1$, $\gamma' = 0$, $\vec{\sigma}'' = 0$, $\gamma'' = \pm 1$, vel $\vec{\sigma}' = 0$, $\gamma' = \pm 1$, $\vec{\sigma}'' = \pm 1$, $\gamma'' = 0$.

Si vero, *secundo*, $a > a'$, eaedem conclusiones sic obtinentur: ex aequ. 2, 3 necessario erit $\vec{\sigma} = 0$, $\gamma = 0$, et vel $\vec{\sigma}' = \pm 1$, $\gamma' = 0$, $\vec{\sigma}'' = 0$, $\gamma'' = \pm 1$, vel $\vec{\sigma}' = 0$, $\gamma' = \pm 1$, $\vec{\sigma}'' = \pm 1$, $\gamma'' = 0$; pro suppositione utraque ex aequ. 4, 5 erit $\alpha' = 0$, $\alpha'' = 0$, atque ex 1, $\alpha = \pm 1$. Habentur itaque, pro utroque casu, 16 transformationes diversae. — Duo casus reliqui, ubi vel $a = a''$, vel $a = a'$, prorsus simili modo absolvuntur, si modo characteres $\alpha, \alpha', \alpha''$ in priori cum $\vec{\sigma}, \vec{\sigma}', \vec{\sigma}''$, in posteriori cum $\gamma, \gamma', \gamma''$ resp. commutantur.

III. Quando omnes a, a', a'' aequales sunt, aequationes 1, 2, 3 requirunt, ut e tribus numeris $\alpha, \alpha', \alpha''$, nec non ex $\vec{\sigma}, \vec{\sigma}', \vec{\sigma}''$, ut et ex $\gamma, \gamma', \gamma''$ bini sint $= 0$, tertius $= \pm 1$. Per aequ. 4, 5, 6 autem facile intelligitur, e tribus numeris $\alpha, \vec{\sigma}, \gamma$ unum tantummodo $= \pm 1$ esse posse, similiterque ex $\alpha', \vec{\sigma}', \gamma'$, nec non ex $\alpha'', \vec{\sigma}'', \gamma''$. Quamobrem sex tantummodo combinationes dantur

$$\left.\begin{array}{|c|c|c|c|c|c|l} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \vec{\sigma}' & \vec{\sigma}'' & \vec{\sigma} & \vec{\sigma}'' & \vec{\sigma} & \vec{\sigma}' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1 \end{array}\right| \text{ Coëfficientes seni reliqui } = 0$$

ita ut ob signorum ambiguitatem omnino 48 transformationes habeantur. — Idem typus etiam casus praecedentes complectitur: sed e sex columnis primis prima sola accipi debet, quando a, a', a'' omnes sunt inaequales; columna prima et secunda, quando $a' = a''$; prima et tertia, quando $a = a'$; prima et sexta, quando $a = a''$.

Hinc colligitur, si forma $f = axx + a'x'x' + a''x''x''$ in aliam aequivalentem f' transeat per substitutionem

$$x = \hat{\sigma}y + \varepsilon y' + \zeta y'', \quad x' = \hat{\sigma}'y + \varepsilon' y' + \zeta' y'', \quad x'' = \hat{\sigma}''y + \varepsilon' y' + \zeta'' y''$$

omnes transf. formae f in f' contineri sub schemate sequente:

$$\left.\begin{array}{|c|c|c|c|c|c|l} x & x & x' & x' & x'' & x'' & = \pm(\hat{\sigma}y + \varepsilon y' + \zeta y'') \\ x' & x'' & x & x'' & x & x' & = \pm(\hat{\sigma}'y + \varepsilon' y' + \zeta' y'') \\ x'' & x' & x'' & x & x' & x & = \pm(\hat{\sigma}''y + \varepsilon'' y' + \zeta'' y'') \end{array}\right|$$

eo discrimine, ut sex columnae primae omnes adhibendae sint, quando $a = a' = a''$;

columna 1 et 2, quando a', a'' aequales, a inaequalis; 1 et 3, quando $a = a'$; 1 et 6, quando $a = a''$; denique columna prima sola, quando a, a', a'' omnes inaequales. In casu primo transformationum multitudo erit 48, in secundo, tertio et quarto 16, in quinto 8.

QUAEDAM APPLICATIONES AD THEORIAM FORMARUM BINARIARUM.

De invenienda forma, e cuius duplicatione forma binaria data generis principalis oriatur.

Ab hac succincta primorum elementorum theoriae formarum ternariarum expositione ad quasdem applicationes speciales progredimur, inter quas primum locum meretur sequens

286.

Problema. *Proposita forma binaria $F = (A, B, C)$ determinantis D ad genus principale pertinente: invenire formam binariam f, e cuius duplicatione illa oriatur.*

Sol. I. Quaeratur repraesentatio propria formae ipsi F oppositae $F' = ATT - 2BTU + CUU$ per formam ternariam $xx - 2yz$, quae sit

$$x = \alpha T + \vec{\sigma} U, \quad y = \alpha' T + \vec{\sigma}' U, \quad z = \alpha'' T + \vec{\sigma}'' U$$

quod fieri posse e theoria praec. formarum ternariarum facile colligitur. Quum enim F per hyp. sit e genere principali, dabitur valor expr. $\sqrt{(A, B, C)} \pmod D$, unde inveniri poterit forma ternaria φ determinantis 1, in quam $(A, -B, C)$ tamquam pars ingrediatur, cuius formae coëfficientes omnes fore integros nullo negotio perspicietur. Aeque facile intelligitur, φ fore formam indefinitam (quoniam per hyp. F certo non est forma negativa); unde necessario formae $xx - 2yz$ aequivalens erit. Assignari poterit itaque transformatio huius in illam, quae repraesentationem propriam formae F' per $xx - 2yz$ suppeditabit. — Tunc igitur erit

$$A = \alpha\alpha - 2\alpha'\alpha'', \quad -B = \alpha\vec{\sigma} - \alpha'\vec{\sigma}'' - \alpha''\vec{\sigma}', \quad C = \vec{\sigma}\vec{\sigma} - 2\vec{\sigma}'\vec{\sigma}''$$

porro designatis numeris $\alpha\mathfrak{G}' - \alpha'\mathfrak{G}$, $\alpha'\mathfrak{G}'' - \alpha''\mathfrak{G}'$, $\alpha''\mathfrak{G} - \alpha\mathfrak{G}''$ per a, b, c resp., hi divisorem communem non habebunt, eritque $D = bb - 2ac$.

II. Hinc adiumento observationis ultimae art. 235 facile concluditur, F transire per substitutionem $2\mathfrak{G}', \mathfrak{G}, \mathfrak{G}, \mathfrak{G}''$; $2\alpha', \alpha, \alpha, \alpha''$ in productum formae $(2a, -b, c)$ in se ipsam, nec non per substitutionem $\mathfrak{G}', \mathfrak{G}, \mathfrak{G}, 2\mathfrak{G}''$; $\alpha', \alpha, \alpha, 2\alpha''$ in productum formae $(a, -b, 2c)$ in se ipsam. Iam divisor communis maximus numerorum $2a, 2b, 2c$ est 2; si itaque c est impar, $2a, 2b, c$ divisorem communem non habebunt, sive $(2a, -b, c)$ erit forma proprie primitiva; similiter, si a est impar, $(a, -b, 2c)$ forma proprie primitiva erit; in casu priori F oritur ex duplicatione formae $(2a, -b, c)$, in posteriori ex duplicatione formae $(a, -b, 2c)$, (V. concl. 4. art. 235); unus vero horum casuum certo semper locum habebit. Si enim uterque a, c esset par, b necessario foret impar; iam facile confirmatur, esse $\mathfrak{G}''a + \mathfrak{G}b + \mathfrak{G}'c = 0$, $\alpha''a + \alpha b + \alpha' c = 0$, unde sequeretur, $\mathfrak{G}b$, αb, adeoque etiam α et $\mathfrak{G}$ esse pares. Hinc autem A et C forent pares, quod esset contra hypothesin, secundum quam F est forma e genere principali adeoque ex ordine proprie primitivo. — Ceterum fieri etiam potest, ut tum a tum c impares sint, in quo itaque casu duae statim formae habebuntur, e quarum duplicatione F oritur.

Ex. Proposita sit forma $F = (5, 2, 31)$, det. -151. Valor expressionis $\sqrt{(5, 2, 31)}$ hic invenitur $(55, 22)$; hinc forma ternaria $\varphi = \left(\begin{smallmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{smallmatrix}\right)$; huic per praeceptа art. 272 aequivalens invenitur forma $\left(\begin{smallmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$, quae in φ transit per substitutionem $\left(\begin{smallmatrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{smallmatrix}\right)$. Hinc adiumento transformationum in art. 277 traditarum invenitur, $\left(\begin{smallmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{smallmatrix}\right)$ transire in φ per substitutionem $\left(\begin{smallmatrix} 3, & -7, & -2 \\ 2, & -4, & 0 \\ 1, & -9, & -3 \end{smallmatrix}\right)$. Fit itaque $a = 11$, $b = -17$, $c = 20$; quare quum a sit impar, F oritur ex duplicatione formae $(11, 17, 40)$ transitque in productum huius formae in se ipsam per substitutionem $-1, -7, -7, -18$; $2, 3, 3, 2$.

Omnibus characteribus, praeter eos, qui in artt. 263, 264 impossibiles inventi sunt, genera revera respondent.

287.

Circa problema in art. praec. solutum sequentes adhuc annotationes adiicimus.

I. Si forma F per substitutionem p, p', p'', p'''; q, q', q'', q''' in productum e duabus formis (h, i, k), (h', i', k') transformatur, utraque uti semper suppo-

nimus proprie accepta), habebuntur aequationes, ex concl. 3 art. 235 facile deducendae:

$$\begin{gathered} p''hn' - p'kn - p(in' - i'n) = 0 \\ (p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) = 0 \\ p'kn' - p''kn - p'''(in' - i'n) = 0 \end{gathered}$$

tresque aliae ex his per commutationem numerorum p, p', p'', p''' cum q, q', q'', q''' oriundae; n, n' sunt radices quadratae positivae e quotientibus prodeuntibus, si determinantes formarum (h, i, k), (h', i', k') per det. formae F dividuntur. Si itaque hae formae sunt identicae, sive $n = n'$, $h = h'$, $i = i'$, $k = k'$, illae aequationes transeunt in has:

$$(p'' - p')hn = 0, \quad (p'' - p')in = 0, \quad (p'' - p')kn = 0$$

unde erit *necessario* $p' = p''$, prorsusque simili modo $q' = q''$. — Tribuendo itaque formis (h, i, k), (h', i', k') *easdem* indeterminatas t, u, designandoque indeterminatas formae F per T, U, transibit F per substitutionem

$$T = ptt + 2p'tu + p'''uu, \quad U = qtt + 2q'tu + q'''uu \text{ in } (htt + 2itu + kuu)^2$$

II. Si forma F oritur e duplicatione formae f, orietur etiam e duplicatione cuiusvis alius formae cum f in eadem classe contentae sive classis formae F e duplicatione classis formae f (V. art. 238). Ita in ex. art. praec. $(5, 2, 31)$ oritur etiam e duplicatione formae $(11, -5, 16)$, ipsi $(11, 17, 40)$ proprie aequivalentis. Ex una classe, per cuius dupl. classis formae F oritur, *omnes* (si plures dantur) inveniuntur adiumento probl. 260; in exemplo nostro alia huiusmodi classis positiva non dabitur, quia una tantummodo classis anceps proprie primitiva positiva det. -151 exstat (puta principalis); quum e compositione classis unicae ancipitis negativae $(-1, 0, -151)$, cum classe $(11, -5, 16)$ oriatur classis $(-11, -5, -16)$, haec erit unica negativa, e cuius duplicatione classis $(5, 2, 31)$ oritur.

III. Quum per solutionem ipsam probl. art. praec. evictum sit, quamvis classem formarum binariarum proprie primitivam (positivam) ad genus principale pertinentem ex alicuius classis pr. prim. eiusdem det. duplicatione oriri posse; theorema art. 261, per quod certi eramus, *ad minimum* semissi omnium characterum

pro determinante non-quadrato dato D assignabilium genera proprie primitiva (positiva) respondere non posse, eo iam ampliatur, ut *praecise* semissi omnium horum characterum talia genera revera respondeant, alterique ideo semissi nulla respondere possint (V. demonstr. illius theor.). Quare quum in art. 264 omnes illi characteres assignabiles in duas species P, Q aequaliter distributi sint, e quibus posteriores Q formis pr. prim. (positivis) respondere non posse probatum erat, de reliquis autem P incertum maneret, an singulis genera semper revera responderent: nunc hoc dubium penitus est sublatum, certique sumus, in toto characterum complexu P nullum adesse, cui genus non respondeat. — Hinc facile quoque deducitur, pro determinante negativo in ordine pr. prim. *negativo*, in quo omnes P impossibiles *solosque* Q possibiles esse in art. 264, I ostensum est, *omnes* Q revera possibiles esse. Designante enim K characterem quemcunque ex Q, f formam arbitrariam ex ordine pr. prim. neg. formarum det. D, atque K' ipsius characterem, hic erit ex Q; unde facile perspicitur, characterem ex K, K' compositum (ad normam art. 246) ad P pertinere, adeoque formas pr. primitivas positivas det. D exstare, quae ei respondeant; ex compositione talis formae cum f manifesto orietur forma pr. prim. neg. det. D, cuius character erit K. — Prorsus simili ratione probatur, in ordine improprie primitivo eos characteres, qui per praecepta art. 264 II, III *soli* possibiles inveniuntur, *omnes* possibiles esse, sive sint P sive Q. — Haecce theoremata, ni vehementer fallimur, ad pulcherrima in theoria formarum binariarum sunt referenda, eo magis quod licet summa simplicitate gaudeant, tamen tam recondita sint ut ipsarum demonstrationem rigorosam absque tot aliarum disquisitionum subsidio condere non liceat.

Theoria decompositionis tum numerorum tum formarum binariarum in tria quadrata:

Transimus iam ad aliam applicationem digressionis praecedentis, ad discerptionem tum numerorum tum formarum binariarum in terna quadrata, cui praemittimus sequens

288.

Problema. *Designante M numerum positivum, invenire conditiones sub quibus formae binariae primitivae negativae determinantis $-M$ dari possint, quae sint residua quadratica ipsius M sive pro quibus 1 sit numerus characteristicus.*

Sol. Designemus per Ω complexum omnium characterum particularium, quos praebent relationes numeri 1 tum ad singulos divisores primos (impares) ipsius M tum ad numerum 8 vel 4, quando ipsum M metitur; manifesto hi characteres erunt Rp, Rp', Rp'' etc., denotantibus p, p', p'' etc. illos divisores primos, atque $1,4$ quando 4; $1,8$ quando 8 ipsum M metitur. Praeterea utamur literis P, Q in eadem significatione ut in art. praec. sive ut in 264. Iam distinguamus casus sequentes.

I. Quando M per 4 divisibilis est, Ω erit character integer, patetque ex art. 233 V, 1 talium tantummodo formarum numerum characteristicum esse posse, quarum character sit Ω. Sed manifestum est, Ω fore characterem formae principalis $(1, 0, M)$, adeoque ad P pertinere et proin formae proprie primitivae negativae competere non posse; quare quum formae improprie primitivae pro tali det. non dentur, nullae omnino formae prim. neg. in hoc casu dantur, quae sint residua ipsius M.

II. Quando $M \equiv 3 \pmod 4$, prorsus eadem ratiocinia valent ea sola exceptione ut in hoc casu ordo *improprie* primitivus negativus exstet, in quo characteres P vel possibiles erunt, vel impossibiles, prout $M \equiv 3$ vel $\equiv 7 \pmod 8$, V. art. 264, III. In casu igitur priori in hoc ordine genus dabitur, cuius character sit Ω, unde 1 erit numerus characteristicus omnium formarum in ipso contentarum; in casu posteriori nullae omnino formae negativae hac proprietate praeditae dari poterunt.

III. Quando $M \equiv 1 \pmod 4$, Ω nondum est character completus, sed insuper accedere debet relatio ad numerum 4; patet autem, Ω necessario in characterem formae, cuius num. char. sit 1, ingredi debere, et vice versa, formam quamvis, cuius character sit vel $\Omega; 1,4$, vel $\Omega; 3,4$, habere numerum char. 1. Iam $\Omega; 1,4$ manifesto est character generis principalis, qui ad P pertinet adeoque in ordine pr. prim. negativo impossibilis est; ex eadem ratione $\Omega; 3,4$ ad Q pertinebit (art. 263), unde ipsi in ordine pr. prim. negativo genus respondebit, cuius formae omnes habebunt num. char. 1. Ordo improprie primitivus in hoc casu, ut in sequente, non datur.

IV. Quando $M \equiv 2 \pmod 4$, ad Ω accedere debet relatio ad 8, quo fiat character completus, puta vel 1 *et* 3, 8, vel 5 *et* 7, 8, quando $M \equiv 2 \pmod 8$; et vel 1 *et* 7, 8, vel 3 *et* 5, 8, quando $M \equiv 6 \pmod 8$. Pro casu priori character $\Omega; 1$ *et* 3, 8 manifesto pertinet ad P, adeoque $\Omega; 5$ *et* 7, 8 ad Q, unde ipsi respon-

debit genus pr. prim. neg.; similique ratione pro posteriori unum genus in ordine pr. prim. negativo dabitur, cuius formae proprietate praescripta praeditae sint. puta cuius character Ω; 3 *et* 5, 8.

Ex his colligitur, formas primitivas negativas det. $-M$, quarum numerus characteristicus sit 1, dari, quando M alicui numerorum 1, 2, 3, 5, 6 secundum modulum 8 congruus sit et quidem in unico semper genere, quod improprium erit quando $M \equiv 3$; tales formas omnino non dari, quando $M \equiv 0$, 4 vel 7 (mod. 8). Ceterum manifestum est, si $(-a, -b, -c)$ sit forma primitiva negativa, cuius num. char. $+1$, (a, b, c) esse formam primitivam positivam, cuius num. char. -1; hinc perspicuum est, in quinque casibus prioribus (quando $M \equiv 1, 2, 3, 5, 6$) dari genus unum primitivum positivum, cuius formae habeant num. char. -1, et quidem pro $M \equiv 3$ *improprium*, in tribus reliquis vero (quando $M \equiv 0, 4, 7$) tales formas positivas omnino dari non posse.

289.

Circa repraesentationes proprias formarum binariarum per ternariam $xx+yy+zz=f$, e theoria generali in art. 282 tradita colliguntur haec:

I. Forma binaria φ per f proprie repraesentari nequit, nisi fuerit forma positiva primitiva, atque -1 (*i. e.* det. formae f) ipsius numerus characteristicus. Quare pro determinante positivo, nec non pro negativo $-M$, quando M est vel per 4 divisibilis vel formae $8n+7$, nullae formae binariae per f proprie repraesentabiles dantur.

II. Si vero $\varphi = (p, q, r)$ est forma positiva primitiva determinantis $-M$, atque -1 numerus characteristicus formae φ, adeoque etiam oppositae $(p, -q, r)$: dabuntur repraesentationes propriae formae φ per f ad quemlibet valorem datum expr. $\sqrt{-}(p, -q, r)$ pertinentes. Scilicet omnes coëfficientes formae ternariae g det. -1 (art. 283) necessario fient integri, g vero forma definita, adeoque ipsi f certo aequivalens (art. 285, I).

III. Multitudo omnium repraesentationum ad eundem valorem expr. $\sqrt{-}(p, -q, r)$ pertinentium in omnibus casibus, praeter $M=1$ et $M=2$, per art. 283, III aeque magna est ac multitudo transformationum formae f in g, adeoque, per art. 285, $=48$; ibinde patet, si una repraesentatio ad valorem datum pertinens habeatur, 47 reliquas inde derivari, valores ipsorum x, y, z

omnibus quibus fieri potest modis tum inter se permutando tum signis oppositis afficiendo; quare omnes 48 repraesentationes *unicam* decompositionem formae φ in tria quadrata producunt, si ad quadrata ipsa tantum, neque ad ipsorum ordinem radicumve signa respicitur.

IV. Posita multitudine omnium numerorum primorum imparium diversorum ipsum M metientium $=\mu$, haud difficile ex art. 233 concluditur, multitudinem omnium valorum diversorum expressionis $\sqrt{-}(p, -q, r) \pmod{M}$ fore $=2^\mu$, e quibus per art. 283 semissem tantum considerare oportet (quando $M>2$). Quare multitudo omnium repraesentationum propriarum formae φ per f erit $= 48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+3}$; multitudo autem discerptionum diversarum in terna quadrata $= 2^{\mu-1}$.

Ex. Sit $\varphi = 19tt+6tu+41uu$, adeoque $M=770$; hic quatuor valores sequentes expr. $\sqrt{-}(19, -3, 41) \pmod{770}$ considerare oportet (art. 283): (39, 237), (171, −27), (269, −83), (291, −127). Ut inveniantur repraesentationes ad valorem (39, 237) pertinentes, primo eruitur forma ternaria $\left(\begin{smallmatrix} 19, & 11, & 2 \\ 3, & 6, & 3 \end{smallmatrix}\right) = g$, in quam per praecepta artt. 272, 275 f transire invenitur per substitutionem $\left\{\begin{smallmatrix} 1, & -6, & -9 \\ -3, & 2, & 1 \\ -3, & -1, & -1 \end{smallmatrix}\right\}$ unde habetur repraesentatio formae φ per f haec:

$$x = t-6u, \quad y = -3t-2u, \quad z = -3t-u$$

repraesentationes 47 reliquas ad eundem valorem pertinentes, quae ex horum valorum permutatione signorumque conversione oriuntur, brevitatis caussa non adscribimus. Omnes vero 48 repraesentationes eandem discerptionem formae φ in tria quadrata

$$tt-12tu+36uu, \quad 9tt+12tu+4uu, \quad 9tt+6tu+uu$$

producunt.

Prorsus simili modo valor (171, −27) suppeditat discerptionem in quadrata $(3t+5u)^2$, $(3t-4u)^2$, tt; valor (269, −83) hanc $(t+6u)^2+(3t+u)^2+(3t-2u)^2$; denique valor (291, −127) hanc $(t+3u)^2+(3t+4u)^2+(3t-4u)^2$; singulae hae decompositiones 48 repraesentationibus aequipollent. — Praeter has 192 repraesentationes autem, sive quatuor discerptiones, aliae non dabuntur, quum 770 per nullum quadratum divisibilis sit, adeoque repraesentationes impropriae exstare non possint.

290.

De formis determinantis -1 et -2, quae quibusdam exceptionibus obnoxiae erant, paucis seorsim agemus. Praemittimus observationem generalem, si φ, φ' sint formae binariae aequivalentes quaecunque, (θ) transformatio data illius in hanc, ex combinatione repraesentationis cuiusvis formae φ per aliquam ternariam f cum substitutione (θ) prodire repraesentationem formae φ' per f; porro ex repraesentationibus propriis ipsius φ hoc modo oriri repraesentationes proprias formae φ', e diversis diversas, denique e cunctis cunctas. Haec omnia per calculum facillime comprobantur. Quare una formarum φ, φ' totidem modis per f repraesentari poterit ac altera.

I. Sit primo $\varphi = tt+uu$, atque φ' forma quaecunque alia binaria positiva det. -1, cui itaque φ aequivalebit; transeat φ in φ' per substitutionem $t = \alpha t'+\delta u'$, $u = \gamma t'+\delta u'$. Forma φ repraesentatur per ternariam $f = zz+yy+zz$ ponendo $x = t$, $y = u$, $z = 0$; permutando x, y, z hinc emergunt *sex* repraesentationes, et e singulis rursus quatuor mutando signa ipsorum t, u, ita ut omnino 24 repraesentationes diversae habeantur, quibus unica discerptio in tria quadrata aequipollet et praeter quas alias dari non posse facile perspicitur. Hinc concluditur, etiam formam φ' unico tantum modo in tria quadrata decomponi posse, puta in $(\alpha t'+\delta u')^2$, $(\gamma t'+\delta u')^2$ et 0, quae discerptio 24 repraesentationibus aequivalet.

II. Sit $\varphi = tt+2uu$, φ' quaecunque alia forma binaria positiva det. -2, in quam φ transeat per substitutionem $t = \alpha t'+\delta u'$, $u = \gamma t'+\delta u'$. Tunc simili modo ut in casu praec. concluditur, φ, et proin etiam φ', unico tantum modo in tria quadrata discerpi posse, puta φ in $tt+uu+uu$, atque φ' in $(\alpha t'+\delta u')^2+(\gamma t'+\delta u')^2+(\gamma t'+\delta u')^2$; talem decompositionem 24 repraesentationibus aequipollere facile perspici potest.

Hinc colligitur, formas binarias determinantium -1 et -2 respectu multitudinis repraesentationum per ternariam $xx+yy+zz$ cum aliis formis binariis omnino convenire; quum enim in utroque casu fiat $\mu = 0$, formula in art. praec. IV. tradita utique producit 24 repraesentationes. Ratio huius rei est, quod duae exceptiones, quibus tales formae obnoxiae erant, se mutuo compensant.

Theoriam generalem repraesentationum impropriarum in art. 284 explicatam ad formam $xx+yy+zz$ applicare, brevitatis gratia supersedemus.

291.

Quaestio de inveniendis omnibus repraesentationibus propriis *numeri* positivi dati M per formam $xx+yy+zz$ primo per art. 281 reducitur ad investigationem repraesentationum propriarum numeri $-M$ per formam $-xx-yy-zz = f$; hae vero per praecepta art. 280 ita eruuntur:

I. Evolvantur omnes classes formarum binariarum determinantis $-M$, quarum formae per $XX+YY+ZZ = F$ (cui formae ternariae adiuncta est f) proprie repraesentari possunt. Quando $M \equiv 0$, 4 vel 7 (mod. 8), tales classes per art. 288 non dantur, adeoque M in tria quadrata, quae divisorem communem non habeant, discerpi nequit *). Quando vero $M \equiv 1, 2, 5$ vel 6, dabitur genus positivum proprie primitivum, et quando $M \equiv 3$, improprie primitivum, quod omnes illas classes complectetur: designemus multitudinem harum classium per k.

II. Eligantur iam ex hisce classibus k formae ad lubitum, e singulis una, quae sint φ, φ', φ'' etc.; investigentur omnes omnium repraesentationes propriae per F. quarum itaque multitudo erit $3.2^{\mu+3}k = K$, designante μ multitudinem factorum primorum (imparium) ipsius M; denique e quavis huiusmodi repraesentatione ut

$$X = mt+nu, \quad Y = m't+n'u, \quad Z = m''t+n''u$$

derivetur repraesentatio ipsius M per $xx+yy+zz$ haec

$$x = m'n''-m''n', \quad y = m''n-mn'', \quad z = mn'-m'n$$

In complexu harum K repraesentationum, quem per Ω designemus, omnes repraesentationes ipsius M necessario contentae erunt.

III. Superest itaque tantummodo, ut inquiramus, num in Ω repraesentationes *identicae* occurrere possint; et quum ex art. 280, III iam constet, eas repraesentationes in Ω, quae e formis diversis *e.g.* ex φ et φ' derivatae sint, ne-

*) Haec impossibilitas etiam inde manifesta, quod summa trium quadratorum imparium necessario fit $\equiv 3$ (mod. 8); summa duorum imparium cum uno pari vel $\equiv 2$ vel $\equiv 6$; summa unius imparis cum duobus paribus vel $\equiv 1$ vel $\equiv 5$; denique summa trium parium vel $\equiv 0$ vel $\equiv 4$; sed in casu postremo repraesentatio manifesto est impropria.

cessario diversas esse, sola disquisitio restat, an repraesentationes diversae eiusdem formae, *e. g.* ipsius φ, per F, repraesentationes identicas numeri M per $xx+yy+zz$ producere possint. Iam statim manifestum est, si inter repraesentationes ipsius φ reperiatur haec

$$X = mt+nu, \quad Y = m't+n'u, \quad Z = m''t+n''u \ldots (r)$$

inter easdem fore hanc

$$X = -mt-nu, \quad Y = -m't-n'u, \quad Z = -m''t-n''u \ldots (r')$$

atque ex utraque derivari eandem repraesentationem ipsius M, quae designetur per (R); examinemus itaque, num eadem (R) ex aliis adhuc repraesentationibus formae φ sequi possit. Ex art. 280, III facile deducitur, statuendo ibi $\chi = \varphi$, si omnes transformationes propriae formae φ in se ipsam exhibeantur per

$$t = \alpha t+\vartheta u, \quad u = \gamma t+\delta u$$

omnes eas repraesentationes formae φ, e quibus R sequatur, expressum iri per

$$\begin{aligned} x &= (\alpha m+\gamma n)t+(\vartheta m+\delta n)u \\ y &= (\alpha m'+\gamma n')t+(\vartheta m'+\delta n')u \\ z &= (\alpha m''+\gamma n'')t+(\vartheta m''+\delta n'')u \end{aligned}$$

At e theoria transformationum formarum binariarum det. negativi in art. 179 explicata sequitur, in omnibus casibus praeter $M = 1$ et $M = 3$, duas tantummodo transformationes proprias formae φ in se ipsam dari, puta $\alpha, \vartheta, \gamma, \delta = 1, 0, 0, 1$ et $= -1, 0, 0, -1$ resp. (quum enim φ sit forma primitiva, id quod in art. 179 designabatur per m, erit vel 1 vel 2, et proin, praeter casus exceptos, certo (1) locum ibi habebit). Quare (R) e solis r, r' provenire poterit, adeoque quaevis repraesentatio propria numeri M bis et non pluries in Ω reperietur, et multitudo omnium repraess. propriarum diversarum ipsius M erit $\frac{1}{2}K = 3 \cdot 2^{\mu+2}k$.

Quod attinet ad casus exceptos, multitudo transformationum propriarum formae φ in se ipsam per art. 179 erit 4 pro $M = 1$, et 6 pro $M = 3$; reveraque facile confirmatur, multitudinem repraesentationum propriarum numerorum 1, 3 esse $\frac{1}{4}K$, $\frac{1}{6}K$ resp.; scilicet uterque numerus unico tantum modo in tria quadrata discerpi potest, 1 in $1+0+0$, 3 in $1+1+1$, discerptio ipsius 1 suppeditat sex, discerptio ipsius 3 octo repraesentationes diversas; K vero fit $= 24$ pro $M = 1$ (ubi $\mu = 0$, $k = 1$) et $= 48$ pro $M = 3$ (ubi $\mu = 1$, $k = 1$).

Ceterum observamus, si h designet multitudinem classium in genere principali, cui multitudo classium in quovis alio genere proprie primitivo per art. 252 aequalis est, fore $k = h$ pro $M \equiv 1, 2, 5$ vel $6 \pmod 8$, sed $k = \frac{1}{3}h$ pro $M \equiv 3 \pmod 8$, unico casu $M = 3$ excepto, ubi $k = h = 1$. Pro numeris itaque formae $8n+3$ multitudo repraesentationum *generaliter* est $= 2^{\mu+2}h$, quum in numero 3 duae exceptiones sese compensent.

292.

Discerptiones numerorum (ut formarum binariarum supra) in tria quadrata a repraesentationibus per formam $xx+yy+zz$ ita distinguimus, ut in illis ad solam quadratorum magnitudinem, in his vero insuper ad ipsorum ordinem radicumque signa respiciamus, adeoque repraesentationes $x = a$, $y = b$, $z = c$, et $x = a'$, $y = b'$, $z = c'$ pro diversis habeamus, nisi simul $a = a'$, $b = b'$, $c = c'$; discerptiones autem in $aa+bb+cc$ et in $a'a'+b'b'+c'c'$ pro una, si nullo ordinis respectu habito haec quadrata illis aequalia sunt. Hinc patet,

I. Discerptionem numeri M in quadrata $aa+bb+cc$ aequipollere 48 repraesentationibus, si nullum sit $= 0$ omniaque inaequalia; 24 autem, si *vel* unum $= 0$ reliqua inaequalia, *vel* nullum $= 0$ atque duo inter se aequalia. Si vero in discerptione numeri dati in tria quadrata duo ex his sunt $= 0$, *aut* unum $= 0$ reliqua aequalia, *aut* omnia aequalia, repraesentationibus 6, *aut* 12, *aut* 8 aequivalens erit; sed haec evenire nequeunt nisi in casibus singularibus, ubi $M = 1$ aut 2 aut 3 resp., siquidem repraesentationes esse debent propriae. His exclusis supponamus, multitudinem omnium discerptionum numeri M in terna quadrata (divisoris communis expertia) esse E, atque inter has reperiri e in quibus unum quadratum 0, et e' in quibus duo quadrata aequalia; illae etiam tamquam discerptiones in bina quadrata, hae tamquam discerptiones in quadratum et quadratum duplum spectari possunt. Tunc multitudo omnium repraesentationum propriarum numeri M per $xx+yy+zz$ erit

$$= 24(e+e')+48(E-e-e') = 48E-24(e+e')$$

At e theoria formarum binariarum facile deducitur, e fore vel $= 0$ vel $= 2^{\mu-1}$, prout -1 sit non-residuum vel residuum quadraticum ipsius M, nec non $e' = 0$ vel $= 2^{\mu-1}$, prout -2 non-residuum vel residuum ipsius M, denotante μ multitudinem factorum primorum (imparium) ipsius M (v. art. 182; expositionem uberiorem hic supprimimus). Hinc facile colligitur, fore

$$E = 2^{\mu-2}k, \text{ si tum } -1 \text{ tum } -2 \text{ sit } N.R. \text{ ipsius } M;$$
$$E = 2^{\mu-2}(k+2), \text{ si uterque numerus sit residuum; denique}$$
$$E = 2^{\mu-2}(k+1), \text{ si alter residuum sit alter non-residuum.}$$

In casibus exclusis $M = 1$ et $M = 2$, haec formula praeberet $E = \frac{3}{4}$, quum esse debeat $E = 1$; pro $M = 3$ autem recte provenit $E = 1$, exceptionibus se mutuo compensantibus.

Si itaque M est numerus primus, fit $\mu = 1$, adeoque $E = \frac{1}{2}(k+2)$ quando $M \equiv 1 \pmod 8$; $E = \frac{1}{2}(k+1)$ quando $M \equiv 3$ aut $\equiv 5$. Haecce theoremata specialia ab ill. Le Gendre per inductionem detecta et in commentatione egregia iam saepius laudata *Hist. de l'Ac. de Paris* 1785 *p.* 530 *sqq.* prolata fuerunt, etsi sub forma aliquantum diversa, cuius rei ratio imprimis in eo est sita, quod acquivalentiam propriam ab impropria non distinxit, et proin classes oppositas commiscuit.

II. Ad inventionem omnium discerptionum numeri M in terna quadrata (sine div. comm.) non opus est, omnes repraesentationes proprias omnium formarum $\varphi, \varphi', \varphi''$ eruere. Primo enim facile confirmatur, omnes (48) repraesentationes formae φ ad eundem valorem expr. $\sqrt{-(p, -q, r)}$ pertinentes (statuendo $\varphi = (p, q, r)$) discerptionem eandem numeri M praebere, adeoque sufficere, si una ex illis habeatur, sive quod eodem redit, si tantummodo omnes diversae discerptiones *) formae φ in terna quadrata conscriptae sint, et perinde de reliquis φ', φ'' etc. Dein si φ est e classe non ancipite, eam formam, quae e classe opposita electa est, omnino praeterire licebit, sive e binis classibus oppositis unicam considerare sufficit. Quum enim prorsus arbitrarium sit, quaenam forma e singulis classibus eligatur, supponamus e classe opposita ei in qua est φ eligi formam ipsi φ oppositam, quae sit $= \varphi'$. Tunc nullo negotio perspicitur, si

*) Semper subintelligendum *propriae*, si hanc expressionem a repraesentationibus ad discerptiones transferre lubet.

discerptiones propriae formae φ indefinite exhibeantur per

$$(gt+hu)^2+(g't+h'u)^2+(g''t+h''u)^2$$

omnes discerptiones formae φ' expressum iri per

$$(gt-hu)^2+(g't-h'u)^2+(g''t-h''u)^2$$

nec non ex his easdem discerptiones numeri M derivari ut ex illis. Denique pro eo casu ubi φ est forma e classe ancipite, attamen neque e classe principali neque formae $(2, 0, \frac{1}{2}M)$ aut $(2, 1, \frac{1}{2}(M+1))$ aequivalens (prout M par aut impar), e valoribus expr. $\sqrt{-(p, -q, r)}$ semissem omittere licet; sed brevitatis caussa hocce compendium fusius hic non explicamus. — Ceterum iisdem compendiis etiam uti possumus, quando omnes repraesentationes propriae ipsius M per $xx + yy + zz$ desiderantur, quum hae e discerptionibus facillime evolvantur.

Exempli caussa investigabimus omnes discerptiones numeri 770 in terna quadrata, ubi $\mu = 3$, $e = e' = 0$, adeoque $E = 2k$. Per classificationem formarum binariarum positivarum determinantis -770, quam quoniam a quovis ad normam art. 231 facile condi potest brevitatis gratia non adscribimus, invenitur classium positivarum multitudo $= 32$, quae omnes sunt proprie primitivae et inter 8 genera distribuuntur, ita ut sit $k = 4$, et proin $E = 8$. Genus, cuius numerus characteristicus -1, respectu numerorum 5, 7, 11 manifesto characteres particulares $R5$; $N7$; $N11$ habere debet, unde per art. 263 facile concluditur, ipsius characterem respectu numeri 8 esse debere 1 *et* 3, 8. Iam in eo genere, cuius character 1 *et* 3, 8; $R5$; $N7$; $N11$, quatuor classes reperiuntur, pro quarum repraesentantibus eligimus formas $(6, 2, 129)$, $(6, -2, 129)$, $(19, 3, 41)$, $(19, -3, 41)$; classem secundam vero et quartam reiicimus, utpote primae et tertiae oppositas. Quatuor discerptiones formae $(19, 3, 41)$ iam in art. 289 tradidimus, e quibus sequuntur discerptiones numeri 770 in $9+361+400$, $16+25+729$, $81+400+289$, $576+169+25$. Simili ratione inveniuntur quatuor discerptiones formae $6tt+4tu+129uu$ in

$$(t-8u)^2+(2t+u)^2+(t+8u)^2, \quad (t-10u)^2+(2t+5u)^2+(t+2u)^2$$
$$(2t-5u)^2+(t+10u)^2+(t+2u)^2, \quad (2t+7u)^2+(t-8u)^2+(t-4u)^2$$

resp. e valoribus expressionis $\sqrt{-(6, -2, 129)}$ hisce oriundae $(48, 369)$, $(62, -149)$, $(92, -159)$, $(202, 61)$; unde prodeunt discerptiones numeri 770 in $225+256+289$, $1+144+625$, $64+81+625$, $16+225+529$. Praeter has octo discerptiones aliae non dantur.

Quae ad discerptiones numerorum in terna quadrata divisores communes habentia attinent, tam facile e theoria generali art. 281 sequuntur, ut non opus sit huic rei immorari.

Demonstratio theorematum Fermatianorum, quemvis integrum in tres numeros trigonales vel quatuor quadrata discerpi posse.

293.

Disquisitiones praecedentes etiam suppeditant demonstrationem theorematis famosi, *omnem numerum integrum positivum in tres numeros trigonales discerpi posse*, quod a Fermatio olim inventum est, sed cuius demonstratio rigorosa hactenus desiderabatur. Manifestum est, quamvis discerptionem numeri M in trigonales

$$\tfrac{1}{2}x(x+1)+\tfrac{1}{2}y(y+1)+\tfrac{1}{2}z(z+1)$$

producere discerptionem numeri $8M+3$ in terna quadrata imparia

$$(2x+1)^2+(2y+1)^2+(2z+1)^2$$

et vice versa. Quivis autem numerus integer positivus $8M+3$ per theoriam praecedentem in tria quadrata resolubilis est, quae necessaria erunt imparia (V. annot. art. 291); resolutionumque multitudo pendet tum a multitudine factorum primorum ipsius $8M+3$, tum a multitudine classium, in quas formae binariae determinantis $-(8M+3)$ distribuuntur. Totidem discerptiones numeri M in ternos trigonales dabuntur. Supponimus autem, $\frac{1}{2}x(x+1)$ pro valore quocunque integro ipsius x tamquam trigonalem spectari; quodsi magis placeret cifram excludere, theorema ita immutare oporteret: Quivis integer positivus vel ipse trigonalis est, vel in duos vel in tres trigonales resolubilis. Similis mutatio in theoremate sequente facienda esset, si cifram a quadratis excludere placeret.

Ex iisdem principiis demonstratur aliud Fermatii theorema, *quemvis numerum integrum positivum in quatuor quadrata decomponi posse*. Subtrahendo a numero formae $4n+2$ quadratum arbitrarium (illo numero minus), a numero formae $4n+1$ quadratum par, a numero formae $4n+3$ quadratum impar, residuum in omnibus his casibus in tria quadrata resolubile erit, adeoque numerus propositus in quatuor. Denique numerus formae $4n$ exhiberi potest per $4^k N$ ita ut N ad aliquam trium formarum praecedentium pertineat: resoluto autem ipso N in quatuor quadrata, etiam $4^k N$ resolutus erit. A numero formae $8n+3$ etiam subduci potest quadratum radicis pariter paris, a numero formae $8n+7$ quadratum radicis impariter paris, a numero formae $8n+4$ quadratum impar, residuumque in tria quadrata resolubile erit. Ceterum hocce theorema iam ab ill. La Grange demonstratum erat, *Nouv. Mém. de l'Ac. de Berlin* 1770 *p.* 123, quam demonstrationem (a nostra prorsus diversam) fusius explicavit ill. Euler in *Actis Ac. Petr. Vol.* II. *p.* 48. — Alia Fermatii theoremata quae praecedentium quasi continuationem constituunt, quemvis numerum integrum in quinque numeros pentagonales, sex hexagonales, septem heptagonales etc. resolubilem esse, demonstratione hactenus carent, aliaque principia requirere videntur.

Solutio aequationis $axx+byy+czz=0$.

294.

THEOREMA. *Designantibus* a, b, c *numeros inter se primos, quorum nullus neque* $=0$ *neque per quadratum divisibilis, aequatio*

$$axx+byy+czz=0 \quad \ldots \quad (\Omega)$$

resolutionem in integris non admittet (praeter hanc $x=y=z=0$ *ad quam non respicimus) nisi* $-bc, -ac, -ab$ *resp. sint residua quadratica ipsorum* a, b, c, *atque hi numeri signis inaequalibus affecti; his vero quatuor conditionibus locum habentibus,* (Ω) *in integris resolubilis erit.*

Dem. Si (Ω) per integros omnino est resolubilis, etiam per tales valores ipsorum x, y, z resolvi poterit, qui divisorem communem non habent; nam valores quicunque, aequ. Ω satisfacientes, etiamnum satisfacient, si per divisorem communem maximum dividuntur. Iam supponendo $app+bqq+crr=0$, atque p, q, r a divisore communi liberos, etiam inter se primi erunt; si enim q, r divisorem communem μ haberent, hic ad p primus esset, $\mu\mu$ autem metiretur ipsum app adeoque etiam ipsum a, contra hyp.; et perinde p, r; p, q inter se primi erunt. Repraesentatur itaque $-app$ per formam binariam $byy+czz$,

tribuendo ipsis y, z valores inter se primos q, r; unde illius determinans $-bc$ residuum quadraticum ipsius app adeoque etiam ipsius a erit (art. 154); eodem modo erit $-acRb$, $-abRc$. Quod vero (Ω) resolutionem admittere non possit, si a, b, c idem signum habeant, tam obvium est, ut explicatione non egeat.

Demonstrationem propositionis inversae, quae theorematis partem secundam constituit, ita adornabimus, ut *primo* formam ternariam ipsi $\left(\begin{smallmatrix} a, & b, & c \\ \alpha, & \beta, & \gamma \end{smallmatrix}\right) \ldots f$ aequivalentem invenire doceamus, cuius coëfficientes 2, 3, 4 per abc divisibiles sint, unde *secundo* solutionem aequationis (Ω) deducemus.

I. Investigentur tres integri A, B, C a divisore communi liberi, atque ita comparati, ut A primus sit ad b et c; B ad a et c; C ad a et b; $aAA+bBB+cCC$ autem per abc divisibilis, quod efficietur sequenti modo. Sint $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ resp. valores expressionum $\sqrt{-bc}\,(\mathrm{mod.}\,a)$, $\sqrt{-ac}\,(\mathrm{mod.}\,b)$, $\sqrt{-ab}$ $(\mathrm{mod.}\,c)$, qui necessario ad a, b, c resp. primi erunt. Accipiantur tres integri $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ omnino ad lubitum, modo ita ut ad a, b, c resp. primi sint (*e. g.* omnes $= 1$), determinenturque A, B, C ita ut sit

$$\begin{aligned} A &\equiv \mathfrak{b}c\,(\mathrm{mod.}\,b) \text{ et } \equiv \mathfrak{c}\mathfrak{C}\,(\mathrm{mod.}\,c) \\ B &\equiv \mathfrak{c}a\,(\mathrm{mod.}\,c) \text{ et } \equiv \mathfrak{a}\mathfrak{A}\,(\mathrm{mod.}\,a) \\ C &\equiv \mathfrak{a}b\,(\mathrm{mod.}\,a) \text{ et } \equiv \mathfrak{b}\mathfrak{B}\,(\mathrm{mod.}\,b) \end{aligned}$$

Tunc fiet

$$aAA+bBB+cCC \equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A}+c\mathfrak{b}\mathfrak{b}) \equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A}-\mathfrak{A}\mathfrak{A}b) \equiv 0\ (\mathrm{mod.}\,a)$$

sive per a divisibilis, et perinde per b, c, adeoque etiam per abc divisibilis erit. Praeterea patet, A necessario fieri primum ad b et c; B ad a et c; C ad a et b. Si vero hi valores ipsorum A, B, C divisorem communem (maximum) μ implicant, hic manifesto ad a, b, c adeoque ad abc primus erit; quare illos valores per μ dividendo novos obtinebimus, qui divisorem communem non habebunt, valorem ipsius $aAA+bBB+cCC$ etiamnum per abc divisibilem producent, adeoque omnibus conditionibus satisfacient.

II. Numeris A, B, C, hoc modo determinatis, etiam Aa, Bb, Cc divisorem communem non habebunt. Si enim haberent div. comm. μ, hic necessario primus esset ad a (quippe qui tum ad Bb tum ad Cc primus est) et similiter ad

b et c; quare μ etiam ipsos A, B, C metiri deberet, contra hyp. Inveniri poterunt itaque integri α, $\mathfrak{b}$, γ tales, ut sit $\alpha Aa+\mathfrak{b}Bb+\gamma Cc = 1$; quaerantur insuper sex integri α', $\mathfrak{b}'$, γ', α'', $\mathfrak{b}''$, γ'' tales, ut sit

$$\mathfrak{b}'\gamma''-\gamma'\mathfrak{b}'' = Aa, \quad \gamma'\alpha''-\alpha'\gamma'' = Bb, \quad \alpha'\mathfrak{b}''-\mathfrak{b}'\alpha'' = Cc$$

Iam transeat f per substitutionem

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \mathfrak{b}, & \mathfrak{b}', & \mathfrak{b}'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

in $\left(\begin{smallmatrix} m, & m', & m'' \\ n, & n', & n'' \end{smallmatrix}\right) = g$ (quae ipsi f aequivalens erit), dicoque m', m'', n per abc divisibiles fore. Ponatur enim

$$\begin{aligned} \mathfrak{b}''\gamma-\gamma''\mathfrak{b} &= A', \quad \gamma''\alpha-\alpha''\gamma = B', \quad \alpha''\mathfrak{b}-\mathfrak{b}''\alpha = C' \\ \mathfrak{b}\gamma'-\gamma\mathfrak{b}' &= A'', \quad \gamma\alpha'-\alpha\gamma' = B'', \quad \alpha\mathfrak{b}'-\mathfrak{b}\alpha' = C'' \end{aligned}$$

eritque

$$\begin{aligned} \alpha' &= B''Cc-C''Bb, \quad \mathfrak{b}' = C''Aa-A''Cc, \quad \gamma' = A''Bb-B''Aa \\ \alpha'' &= C'Bb-B'Cc, \quad \mathfrak{b}'' = A'Cc-C'Aa, \quad \gamma'' = B'Aa-A'Bb \end{aligned}$$

Quibus valoribus in aequationibus

$$\begin{aligned} m' &= a\alpha'\alpha'+b\mathfrak{b}'\mathfrak{b}'+c\gamma'\gamma' \\ m'' &= a\alpha''\alpha''+b\mathfrak{b}''\mathfrak{b}''+c\gamma''\gamma'' \\ n &= a\alpha'\alpha''+b\mathfrak{b}'\mathfrak{b}''+c\gamma'\gamma'' \end{aligned}$$

substitutis, fit, secundum modulum a,

$$\begin{aligned} m' &\equiv bcA''A''(BBb+CCc) \equiv 0 \\ m'' &\equiv bcA'A'(BBb+CCc) \equiv 0 \\ n &\equiv bcA'A''(BBb+CCc) \equiv 0 \end{aligned}$$

i. e. m', m'', n per a divisibiles erunt; similique modo iidem numeri per b, c adeoque etiam per abc divisibiles inveniuntur. *Q. E. P.*

III. Ponamus, concinnitatis caussa, determinantem formarum f, g, i. e. numerum $-abc = d$,

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N''$$

patetque, f transire per substitutionem (S)

$$\begin{matrix} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{matrix}$$

in formam ternariam $\left(\begin{smallmatrix} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{smallmatrix}\right) = g'$ determinantis d^3, quae itaque sub f contenta erit. Iam dico, huic formae g' necessario aequivalere hanc $\left(\begin{smallmatrix} d, & 0, & 0 \\ d, & 0, & 0 \end{smallmatrix}\right) = g''$. Patet enim, $\left(\begin{smallmatrix} M, & M', & M'' \\ N, & N', & N'' \end{smallmatrix}\right) = g'''$ fore formam ternariam determinantis 1; porro quum per hyp. a, b, c eadem signa non habeant, f erit forma indefinita, unde facile concluditur, etiam g' et g''' indefinitas esse debere; quare g''' aequivalebit formae $\left(\begin{smallmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{smallmatrix}\right)$ (art. 277), poteritque transformatio (S') illius in hanc inveniri; manifesto autem per (S') forma g' transibit in g''. Hinc etiam g'' sub f contenta erit, et ex combinatione substitutionum (S), (S') deducetur transformatio formae f in g''. Quae si fuerit

$$\begin{matrix} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'' \end{matrix}$$

manifestum est, duplicem solutionem aequationis (Ω) haberi, puta $x = \delta'$, $y = \varepsilon'$, $z = \zeta'$, et $x = \delta''$, $y = \varepsilon''$, $z = \zeta''$; simul patet, neutros valores simul $= 0$ evadere posse, quum necessario fiat

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d. \qquad Q.\ E.\ S.$$

Exemplum. Sit aequatio proposita $7xx - 15yy + 23zz = 0$, quae resolubilis est, quia $345 R 7$, $-161 R 15$, $105 R 23$. Habentur hic valores ipsorum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ hi 3, 7, 6; faciendoque $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$ invenitur $A = 98$, $B = -39$, $C = -8$. Hinc eruitur substitutio $\left\{\begin{smallmatrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{smallmatrix}\right\}$ per quam f transit in $\left(\begin{smallmatrix} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{smallmatrix}\right) = g$. Hinc fit

$$(S) = \left\{\begin{matrix} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{matrix}\right\}, \qquad g''' = \left(\begin{matrix} 3670800, & 6, & -3 \\ & -1, & -1246, & 4735 \end{matrix}\right)$$

Forma g''' transire invenitur in $\left(\begin{smallmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{smallmatrix}\right)$ per substitutionem

$$\left\{\begin{matrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{matrix}\right\} \quad \ldots \quad (S')$$

qua cum (S) combinata prodit haec: $\left\{\begin{smallmatrix} 7, & 1, & 2 \\ -1, & 1, & -3 \\ -9, & 4, & 2 \end{smallmatrix}\right\}$ per quam f transit in g''. Habemus itaque duplicem aequationis propositae solutionem $x = 11$, $y = 9$, $z = 4$, et $x = 12$, $y = -9$, $z = 3$; posterior simplicior redditur dividendo valores per divisorem communem 3, unde $x = 4$, $y = -3$, $z = 1$.

295.

Pars posterior theorematis art. praec. etiam sequenti modo absolvi potest. Quaeratur integer h talis, ut sit $ah \equiv \mathfrak{C} \pmod{c}$, (characteres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ eadem significatione accipimus ut in art. praec.), fiatque $ahh + b = ci$. Tunc facile perspicitur, i fieri integrum, numerumque $-ab$ esse determinantem formae binariae $(ac, ah, i) \ldots \varphi$. Haec forma certo non erit positiva (quum enim per hyp. a, b, c eadem signa non habeant, ab et ac simul positivi esse nequeunt); porro habebit numerum characteristicum -1, quod synthetice ita demonstramus: Determinentur integri e, e' ita ut sit

$$e \equiv 0 \pmod{a} \text{ et } \equiv \mathfrak{B} \pmod{b}; \quad ce' \equiv \mathfrak{A} \pmod{a} \text{ et } \equiv h\mathfrak{B} \pmod{b}$$

eritque (e, e') valor expr. $\sqrt{-(ac, ah, i)} \pmod{-ab}$. Nam secundum modulum a erit

$$ee \equiv 0 \equiv -ac, \quad ee' \equiv 0 \equiv -ah$$
$$cee'e' \equiv \mathfrak{A}\mathfrak{A} \equiv -bc \equiv -cci \quad \text{adeoque} \quad e'e' \equiv -i$$

secundum modulum b autem erit

$$ee \equiv \mathfrak{B}\mathfrak{B} \equiv -ac, \quad cee' \equiv h\mathfrak{B}\mathfrak{B} \equiv -ach \quad \text{adeoque} \quad ee' \equiv -ah$$
$$coe'e' \equiv hh\mathfrak{B}\mathfrak{B} \equiv -achh \equiv -cci \quad \text{adeoque} \quad e'e' \equiv -i$$

eaedem vero tres congruentiae, quae secundum utrumque modulum a, b locum habent, etiam secundum modulum ab valebunt. Hinc per theoriam formarum ternariarum facile concluditur, φ repraesentabilem esse per formam $\left(\begin{smallmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{smallmatrix}\right)$; sit itaque

$$actt + 2ahtu + iuu = -(\alpha t + \delta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

eritque, multiplicando per c,

$$a(ct+hu)^2+buu = -c(at+\vec{b}u)^2+2c(\gamma t+\vec{\delta}u)(\varepsilon t+\zeta u)$$

Hinc patet, si ipsis t, u tales valores determinati tribuantur, ut vel $\gamma t+\vec{\delta}u$, vel $\varepsilon t+\zeta u$ fiat $=0$, haberi solutionem aequationis Ω, cui igitur satisfiet tum per

$$x = \vec{\delta}c-\gamma h, \quad y = \gamma, \quad z = a\vec{\delta}-\vec{b}\gamma$$

tum per

$$x = \zeta c-\varepsilon h, \quad y = \varepsilon, \quad z = a\zeta-\vec{b}\varepsilon$$

simul manifestum est, neque illos valores neque hos simul $=0$ fieri posse; si enim $\vec{\delta}c-\gamma h = 0$, $\gamma = 0$, fieret etiam $\vec{\delta} = 0$ atque $\varphi = -(at+\vec{b}u)^2$, unde $ab = 0$ contra hyp., et perinde de alteris. — In exemplo nostro invenimus formam φ hanc $(161, -63, 24)$, valorem expr. $\sqrt{-\varphi}(\text{mod. } 105) = (7, -51)$, atque repraesentationem formae φ per $\left(\begin{smallmatrix}-1, & 0, & 0\\ 1, & 0, & 0\end{smallmatrix}\right)$ hanc,

$$\varphi = -(13t-4u)^2+2(11t-4u)(15t-5u)$$

hinc prodeunt solutiones $x=7$, $y=11$, $z=-8$; $x=20$, $y=15$, $z=-5$, sive dividendo per 5 et negligendo signum ipsius z, $x=4$, $y=3$, $z=1$.

Ex his duabus methodis aequationem Ω solvendi posterior eo praestat, quod plerumque per numeros minores absolvitur; prior vero, quae etiam per varia artificia hic silentio praetereunda contrahi potest, elegantior videtur ea imprimis ratione, quod numeri a, b, c prorsus eodem modo tractantur, calculusque per horum permutationem quamcunque nihil mutatur. Hoc secus se habet in methodo secunda, ubi calculus maxime commodus plerumque provenit, si pro a accipitur minimus, pro c maximus trium numerorum datorum, uti in exemplo nostro fecimus.

De methodo per quam ill. Le Gendre theorema fundamentale tractavit.

296.

Elegans theorema in artt. praecc. explicatum primo inventum est ab ill. Le Gendre, *Hist. de l'Ac. de Paris* 1784 *p.* 507, atque demonstratione pulcra (a duabus nostris omnino diversa) munitum. Simul vero hic egregius geometra hoc loco operam dedit, demonstrationem propositionum, quae cum theoremate fundamentali

Sect. praecc. conveniunt, inde derivare, quam ad hunc scopum non idoneam nobis videri iam supra declaravimus, art. 151. Hic itaque locus erit, hanc demonstrationem (per se valde elegantem) breviter exponendi iudiciique nostri rationes adiungendi. Praemittitur sequens observatio: *Si numeri a, b, c omnes sunt* $\equiv 1$ *(mod. 4), aequatio* $axx+byy+czz = 0$ ... (Ω) *solubilis esse nequit.* Facillime enim perspicitur, valorem ipsius $axx+byy+czz$ necessario in hoc casu fieri vel $\equiv 1$, vel $\equiv 2$, vel $\equiv 3$ (mod. 4), nisi omnes x, y, z simul pares accipiantur; si itaque Ω solubilis esset, hoc aliter fieri non posset quam per valores pares ipsorum x, y, z, *Q. E. A.*, quoniam valores quicunque aequationi Ω satisfacientes etiamnum satisfaciunt, si per divisorem communem maximum dividuntur, unde necessario ad minimum unus impar prodire debet. Iam casus diversi theorematis demonstrandi ad sequentia momenta referuntur:

I. Designantibus p, q numeros primos formae $4n+3$ (positivos inaequales), nequit simul esse pRq, qRp. Si enim possibile esset, manifestum est statuendo $1 = a$, $-p = b$, $-q = c$, omnes conditiones ad resolubilitatem aequationis $axx+byy+czz = 0$ adimpletas esse (art. 294); eadem vero per observationem praec. resolutionem non admittit, quare suppositio consistere nequit. Hinc protinus sequitur propositio 7 art. 131.

II. Si p est numerus primus formae $4n+1$, q numerus primus formae $4n+3$, nequit simul esse qRp, pNq. Alioquin enim foret $-pRq$, atque aequatio $xx+pyy-qzz = 0$ resolubilis, quae per obs. praec. resolutionem respuit. Hinc derivantur casus 4 et 5 art. 131.

III. Si p, q sunt numeri primi formae $4n+1$, nequit simul esse pRq, qNp. Accipiatur alius numerus primus r formae $4n+3$, qui sit residuum ipsius q et cuius non-residuum sit p. Tunc erit per casus modo (II) demonstratos qRr, rNp. Si itaque esset pRq, qNp, foret $qrRp$, $prRq$, $pqNr$ et proin $-pqRr$. Hinc aequatio $pxx+qyy-rzz = 0$ resolubilis esset contra obs. praec.; quare suppositio consistere nequit. Hinc sequuntur casus 1 et 2 art. 131.

Concinnius hic casus sequenti modo tractatur. Designet r numerum primum formae $4n+3$, cuius non-residuum sit p. Tunc erit etiam rNp, adeoque (supponendo pRq, qNp) $qrRp$, porro $-pRq$, $-pRr$ et proin etiam $-pRqr$; quare aequatio $xx+pyy-qrzz = 0$ resolubilis esset contra obs. praec. Hinc etc.

IV. Si p est numerus primus formae $4n+1$, q primus formae $4n+3$,

nequit simul esse pRq, qNp. Accipiatur numerus primus auxiliaris r formae $4n+1$ qui sit non-residuum utriusque p, q. Tunc erit (per II) qNr et (per III) pNr; hinc $pqRr$; si itaque esset pRq, qNp, haberetur etiam $prNq$, $-prRq$, $qrRp$; quare aequatio $pxx-qyy+rzz=0$ resolubilis esset. Q. E. A. — Hinc derivantur casus 3 et 6 art. 131.

V. Designantibus p, q numeros primos formae $4n+3$, nequit simul esse pNq, qNp. Supponendo enim fieri posse, et accipiendo numerum primum auxiliarem r formae $4n+1$, qui sit non-residuum utriusque p, q erit $qrRp$, $prRq$; porro (per II) pNr, qNr, unde $pqRr$ et $-pqRr$; hinc aequatio $-pxx-qyy+rzz=0$ possibilis, contra obs. praec. Hinc deducitur casus 8 art. 131.

297.

Demonstrationem praec. proprius contemplando quisque facile intelliget, casus I et II ita absolutos esse ut nihil obiici possit. At demonstrationes casuum reliquorum innituntur existentiae numerorum auxiliarium, qua nondum demonstrata methodus manifesto omnem vim perdit. Quae suppositiones, etsi tam speciosae sint, ut minus attendenti demonstratione ne opus quidem esse videri possit, atque certe theorema demonstrandum ad maximum *probabilitatis* gradum evehant, tamen si rigor geometricus desideretur, neutiquam gratuito sunt admittendae. Quod quidem attinet ad suppositionem in IV et V, exstare numerum primum r formae $4n+1$, qui duorum aliorum primorum datorum p, q non-residuum sit, e Sect. IV facile concluditur, omnes numeros ipso $4pq$ minores ad ipsumque primos (quorum multitudo est $2(p-1)(q-1)$) in quatuor classes aequaliter distribui, quarum una contineat non-residua utriusque p, q, tres reliquae residua ipsius p non-residua ipsius q, non-residua ipsius p residua ipsius q, residua utriusque p, q; et in singulis classibus semissem fore numeros formae $4n+1$, semissem formae $4n+3$. Habebuntur itaque inter illos $\frac{1}{4}(p-1)(q-1)$ non-residua utriusque p, q formae $4n+1$, qui sint g, g', g'' etc.; numeri $\frac{1}{4}(p-1)(q-1)$ reliqui sint h, h', h'' etc. Manifesto omnes numeri in formis $4pqt+g$, $4pqt+g'$, $4pqt+g''$ etc. (G) contenti quoque erunt non-residua ipsorum p, q formae $4n+1$. Iam patet, ad suppositionem stabiliendam demonstrari tantummodo debere, sub formis (G) certo contineri *numeros primos*, quod sane iam per se valde plausibile videtur, quum hae formae una cum his $4pqt+h$, $4pqt+h'$ etc.

(H) omnes numeros ad $4pq$ primos adeoque etiam omnes numeros absolute primos (praeter 2, p, q) comprehendant, nullaque ratio adsit, quin numerorum primorum series inter illas formas aequaliter distributi sint, ita ut pars octava referantur ad (G), reliqui ad (H). Attamen perspicuum est, tale ratiocinium a rigore geometrico longe abesse. Ill. Le Gendre ipse fatetur, demonstrationem theorematis, sub tali forma $kt+l$, designantibus k, l numeros inter se primos datos, t indefinitum, certo contineri numeros primos, satis difficilem videri, methodumque obiter addigitat, quae forsan illuc conducere possit; multae vero disquisitiones praeliminares necessariae nobis videntur, antequam haece quidem via ad demonstrationem rigorosam pervenire liceat. — — Circa aliam vero suppositionem (III, meth. secunda) dari numerum primum r formae $3n+3$, cuius non-residuum sit alius numerus primus datus p formae $4n+1$, ill. Le Gendre nihil omnino adiecit. Supra demonstravimus (art. 129), numeros primos quorum $N.R.$ sit p certo dari, sed methodus nostra haud idonea videtur ad existentiam talium numerorum primorum *qui simul sint formae* $4n+3$ ostendendam (ut hic requiritur neque vero in dem. nostra prima). Ceterum veritatem quidem huius suppositionis ita facile probare possumus. Per art. 287 dabitur genus positivum formarum binariarum det. $-p$, cuius character $3, 4$; Np; sit (a, b, c) talis forma atque a impar (quod supponere licet). Tum a erit formae $4n+3$ atque vel ipse primus vel saltem factorem primum r formae $4n+3$ implicabit. Erit autem $-pRa$, adeoque etiam $-pRr$, unde pNr. At probe notandum est, propp. artt. 263, 287 theoremati fundamentali inniti, adeoque circulum vitiosum fore, si qua huius pars illis superstruatur. — — Denique suppositio in methodo prima III adhuc multo magis gratuita est, ita ut non opus sit plura de illa hic adiicere.

Liceat observationem addere circa casum V, qui per methodum praec. quidem non satis probatur, attamen per sequentem commode absolvitur. Si illic simul esset pNq, qNp, foret $-pRq$, $-qRp$, unde facile derivatur, -1 esse numerum characteristicum formae $(p, 0, q)$, quae proin, (secundum theoriam formarum ternariarum) per formam $xx+yy+zz$ repraesentari poterit. Sit

$$ptt+quu=(\alpha t+\beta u)^2+(\alpha' t+\beta' u)^2+(\alpha'' t+\beta'' u)^2$$

sive

$$\alpha\alpha+\alpha'\alpha'+\alpha''\alpha''=p,\quad \beta\beta+\beta'\beta'+\beta''\beta''=q,\quad \alpha\beta+\alpha'\beta'+\alpha''\beta''=0$$

eruntque ex aequatt. 1 et 2, omnes $\alpha, \alpha', \alpha'', \mathfrak{b}, \mathfrak{b}', \mathfrak{b}''$ impares; tum vero manifesto aequatio tertia consistere nequit. — Haud absimili modo etiam casus II absolvi potest.

298.

Problema. *Designantibus* a, b, c *numeros quoscunque, quorum tamen nullus* $= 0$; *invenire conditiones resolubilitatis aequationis*

$$axx+byy+czz = 0 \ldots (\omega).$$

Sol. Sint $\alpha\alpha, \mathfrak{b}\mathfrak{b}, \gamma\gamma$ quadrata maxima ipsos bc, ac, ab resp. metientia, fiatque $\alpha a = \mathfrak{b}\gamma A$, $\mathfrak{b}b = \alpha\gamma B$, $\gamma c = \alpha\mathfrak{b}C$. Tum A, B, C erunt integri, inter se primi; aequatio (ω) autem resolubilis erit vel non erit, prout haec

$$AXX+BYY+CZZ = 0 \ldots (\Omega)$$

resolutionem admittit vel non admittit, quod per art. 294 diiudicari poterit.

Dem. Ponatur $bc = \mathfrak{A}\alpha\alpha$, $ac = \mathfrak{B}\mathfrak{b}\mathfrak{b}$, $ab = \mathfrak{C}\gamma\gamma$, eruntque $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ integri a factoribus quadratis liberi atque $\mathfrak{A} = BC$, $\mathfrak{B} = AC$, $\mathfrak{C} = AB$; hinc $\mathfrak{A}\mathfrak{B}\mathfrak{C} = (ABC)^2$, adeoque $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$ necessario integer. Sit numerorum $\mathfrak{A}$, $A\mathfrak{A}$ divisor comm. max. m, atque $\mathfrak{A} = gm$, $A\mathfrak{A} = hm$, eritque g primus ad h, nec non (quia $\mathfrak{A}$ liber a fact. qu.) ad m. Iam fit $hhm = gAA\mathfrak{A} = g\mathfrak{B}\mathfrak{C}$, unde g metietur ipsum hhm, quod manifesto impossibile est, nisi $g = \pm 1$. Hinc $\mathfrak{A} = \pm m$, $A = \pm h$, et proin integer, et perinde B, C integri erunt. *Q. E. P.* — Quum $\mathfrak{A} = BC$ factores quadratos non implicet, necessario B, C inter se primi esse debebunt; et similiter A ad C et ad B primus erit. *Q. E. S.* — Denique patet, si aequationi (Ω) satisfaciat $X = P$, $Y = Q$, $Z = R$, aequationem (ω) resolvi per $x = \alpha P$, $y = \mathfrak{b}Q$, $z = \gamma R$; et vice versa si huic satisfiat per $x = p$, $y = q$, $z = r$, illi satisfieri per $X = \mathfrak{b}\gamma p$, $Y = \alpha\gamma q$, $Z = \alpha\mathfrak{b}r$, unde vel utraque resolubilis vel neutra. *Q. E. T.*

Repraesentatio cifrae per formas ternarias quascunque.

299.

Problema. *Proposita forma ternaria*

$$f = axx+a'x'x'+a''x''x''+2bx'x''+2b'xx''+2b''xx'$$

invenire, an cifra per eam repraesentari possit (per valores indeterminatarum qui non simul $= 0$).

Sol. I. Quando $a = 0$, valores ipsorum x', x'' ad lubitum assumi possunt, patetque ex aequatione

$$a'x'x'+2bx'x''+a''x''x'' = -2x(b'x''+b''x')$$

x inde valorem determinatum rationalem nancisci; quoties pro x hoc modo fractio provenit, oportet tantummodo, valores ipsorum x, x', x'' per fractionis denominatorem multiplicare, habebunturque integri. Unice excludendi sunt tales valores ipsorum x', x'', qui reddunt $b'x''+b''x' = 0$; nisi simul faciant $a'x'x'+2bx'x''+a''x''x'' = 0$, in quo casu x ad libitum accipi poterit. Simul patet, hoc modo omnes solutiones possibiles obtineri posse. Ceterum is casus, ubi b' et $b'' = 0$, huc non pertinet; tunc enim x in f non ingreditur, sive f est forma binaria, cifraeque repraesentabilitas per f e theoria talium formarum diiudicari debet.

II. Quando vero non est $a = 0$, aequationi $f = 0$ aequivalebit haec

$$(ax+b''x'+b'x'')^2 - A''x'x'+2Bx'x''-A'x''x'' = 0$$

ponendo

$$b''b''-aa' = A'', \quad ab-b'b'' = B, \quad b'b'-aa'' = A'$$

Iam quando hic $A' = 0$, neque vero $B = 0$, manifestum est, si $ax+b''x'+b'x''$ atque x'' ad lubitum assumantur, x et x' inde rationaliter determinari, et quando integri non fiant, saltem multiplicatorem idoneum integros producturum. Pro unico valore ipsius x'' puta pro $x'' = 0$ valor ipsius $ax+b''x'+b'x''$ non est arbitrarius sed quoque $= 0$ poni debet; tunc vero x' ad lubitum assumi poterit valoremque rationalem ipsius x producet. — Quando vero simul A'' et $B = 0$, patet, si A' sit quadratum $= kk$, aequationem $f = 0$ reduci ad has duas lineares (e quibus *vel* una *vel* altera locum habere debet)

$$ax+b''x'+(b'+k)x'' = 0, \quad ax+b''x'+(b'-k)x'' = 0$$

si vero (in eadem hyp.) A' est non-quadratus, manifesto solutio aequ. propositae pendet ab his (quae *simul* locum habere debent) $x'' = 0$ et $ax+b''x' = 0$.

Ceterum vix necessarium erit observare, methodum in I etiam applicari posse, quando a' vel $a'' = 0$, methodumque in II, quando $A' = 0$.

III. Quando vero nec a nec $A'' = 0$, aequationi $f = 0$ aequivalet haec

$$A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Dax''^2 = 0$$

designando per D determinantem formae f sive per Da numerum $BB - A'A''$. Quando $D = 0$, solutio simili modo se habebit ut in fine casus praec.; scilicet si A'' est quadratum $= kk$, aequ. prop. reducitur ad has

$$kax + (kb'' - A'')x' + (kb' + B)x'' = 0, \quad kax + (kb'' + A'')x' + (kb'' - B)x'' = 0$$

si vero A'' est non-quadratus, fieri debet

$$ax + b''x' + b'x'' = 0, \quad A''x' - Bx'' = 0$$

Quando autem D non $= 0$, reducti sumus ad aequationem

$$A''tt - uu + Davv = 0$$

cuius possibilitas per art. praec. diiudicari potest. Quodsi haec aliter resolvi nequit, quam per $t = 0$, $u = 0$, $v = 0$, manifesto etiam proposita aliam solutionem non admittet, quam hanc $x = 0$, $x' = 0$, $x'' = 0$; si vero illa aliter solubilis est, e valoribus integris quibusvis ipsorum t, u, v derivabuntur per aequationes

$$ax + b''x' + b'x'' = t, \quad A''x' - Bx'' = u, \quad x'' = v$$

saltem valores rationales ipsorum x, x', x'', e quibus, si fractiones involvunt, per idoneum multiplicatorem integri elici poterunt.

Quamprimum autem *una* solutio aequationis $f = 0$ in integris inventa est, problema ad casum I reduci, et perinde ac illic solutiones omnes exhiberi poterunt sequenti modo. Satisfaciant aequationi $f = 0$ valores ipsorum x, x', x'' hi α, α', α'', quos a factoribus communibus liberos supponimus, accipiantur (per artt. 40, 279) integri $\mathfrak{b}$, $\mathfrak{b}'$, $\mathfrak{b}''$, γ, γ', γ'' tales, ut sit

$$\alpha(\mathfrak{b}'\gamma'' - \mathfrak{b}''\gamma') + \alpha'(\mathfrak{b}''\gamma - \mathfrak{b}\gamma'') + \alpha''(\mathfrak{b}\gamma' - \mathfrak{b}'\gamma) = 1$$

transeatque f per substitutionem

$$x = \alpha y + \mathfrak{b}y' + \gamma y'', \quad x' = \alpha' y + \mathfrak{b}'y' + \gamma' y'', \quad x'' = \alpha'' y + \mathfrak{b}''y' + \gamma'' y'' \dots (S)$$

in

$$g = cyy + c'y'y' + c''y''y'' + 2d'y'y'' + 2d''yy'' + 2d'''yy'$$

Tunc manifesto erit $c = 0$, atque g ipsi f aequivalens, unde facile concluditur, ex omnibus solutionibus aequationis $g = 0$ derivari (per S) omnes solutiones aequationis $f = 0$ in integris. Iam ex I sequitur, omnes solutiones aequ. $g = 0$ contineri sub formulis

$$y = -z(c'pp + 2d''pq + c''qq), \quad y' = 2z(d''pp + d'pq), \quad y'' = 2z(d''pq + d'qq)$$

designantibus p, q integros indefinitos, z numerum indefinitum, pro quo etiam fractiones accipi possunt, modo ita ut y, y', y'' integri maneant. His valoribus ipsorum y, y', y'' in (S) substitutis, omnes solutiones aequ. $f = 0$ in integris habebuntur. — Ita *e. g.* si

$$f = xx + x'x' + x''x'' - 4x'x'' + 2xx'' + 8xx'$$

atque una solutio aequationis $f = 0$ habetur $x = 1$, $x' = -2$, $x'' = 1$: faciendo $\mathfrak{b}$, $\mathfrak{b}'$, $\mathfrak{b}''$, γ, γ', γ'' $= 0, 1, 0, 0, 0, 1$ prodit

$$g = y'y' + y''y'' - 4y'y'' + 12yy''$$

Hinc omnes solutiones aequ. $g = 0$ in integris contentae erunt sub formula

$$y = -z(pp - 4pq + qq), \quad y' = 12zpq, \quad y'' = 12zqq$$

et proin omnes solutiones aequ. $f = 0$ sub hac

$$\begin{aligned} x &= -z(pp - 4pq + qq) \\ x' &= 2z(pp + 2pq + qq) \\ x'' &= -z(pp - 4pq - 11qq) \end{aligned}$$

Solutio generalis aequationum indeterminatarum secundi gradus duas incognitas implicantium per quantitates rationales.

300.

E problemata art. praec. sponte defluit solutio aequationis indeterminatae

$$axx + 2bxy + cyy + 2dx + 2ey + f = 0$$

si valores tantummodo rationales desiderantur, quam, si integri postulantur, supra (art. 216 sqq.) iam absolvimus. Nam omnes valores rationales ipsorum x, y exhiberi possunt per $\frac{t}{v}$, $\frac{u}{v}$, ita ut t, u, v sint integri, unde patet, solutionem illius aequationis per numeros rationales identicam esse cum solutione aequationis

$$att+2btu+cuu+2dtv+2euv+fvv=0$$

per numeros integros; haec vero convenit cum aequ. in art. praec. tractata. Excludi debent eae solae solutiones ubi $v=0$; tales autem provenire nequeunt, quando $bb-ac$ est numerus non-quadratus. Ita *e. g.* omnes solutiones aequationis (in art. 221 per integros generaliter solutae)

$$xx+8xy+yy+2x-4y+1=0$$

per numeros rationales contentae erunt sub formula

$$x=\frac{pp-4pq+qq}{pp-4pq-11qq},\quad y=-\frac{2pp+4pq+2qq}{pp-4pq-11qq}$$

designantibus p, q integros quoscunque. — Ceterum de his duobus problematibus arctissimo nexu coniunctis breviter tantummodo hic egimus, multasque observationes huc pertinentes suppressimus, tum ne nimis prolixi fieremus, tum quod solutionem aliam probl. art. praec. habemus, principiis generalioribus innixam, cuius expositionem, quia penitiorem formarum ternariarum disquisitionem postulat, ad aliam occasionem nobis reservare debemus.

De multitudine mediocri generum.

301.

Revertimus ad formas binarias, de quibus adhuc plures proprietates singulares recensere oportet. Et primo quasdam observationes circa multitudinem generum et classium in ordine proprie primitivo (positivo pro det. neg.) adiiciemus, ad quem brevitatis caussa disquisitionem restringimus.

Multitudo generum, in quae omnes formae (pr. prim. pos.) determinantis dati positivi vel negativi $\pm D$ distribuuntur, semper est 1, 2, 4 vel altior potestas numeri 2, cuius exponens pendet a factoribus ipsius D, et per disquisitiones praecc. omnino a priori inveniri potest. Iam quum in serie numerorum naturali numeri primi cum magis minusque compositis permixti sint, evenit, ut pro pluribus determinantibus successivis $\pm D$, $\pm(D+1)$, $\pm(D+2)$ etc. multitudo generum nunc crescat nunc decrescat, nullusque in hac serie perturbata ordo adesse videatur. Nihilominus si multitudines generum multis dett. successivis

$$\pm D,\quad \pm(D+1)\quad \ldots\quad \pm(D+m)$$

respondentes adduntur, summaque per determinantium multitudinem dividitur, *multitudo generum mediocris* provenit, quae circa medium determinantium $\pm(D+\frac{1}{2}m)$ locum habere censeri poterit, progressionemque valde regularem constituit. Supponimus autem, non modo m esse satis magnum, sed etiam D multo maiorem, ut ratio determinantium extremorum D, $D+m$ non nimis a ratione aequalitatis discrepet. Regularitas illius progressionis ita intelligenda est: si D' est numerus multo maior quam D, multitudo generum mediocris circa determinantem $\pm D'$ sensibiliter maior erit quam circa D; si vero D, D' non nimis differunt, etiam generum multitudines mediocres circa D et D' fere aequales erunt. Ceterum multitudo mediocris generum circa determinantem positivum $+D$ semper fere aequalis invenitur multitudini mediocri circa negativum, eoque exactius quo maior est D, quum pro valore parvo prior paullulum maior evadat quam posterior. Hae observationes magis illustrabuntur per exempla sequentia, e tabula classificationis formarum binariarum plures quam 4000 determinantes complectente excerpta. Inter centum determinantes a 801 usque ad 900 reperiuntur 7 quibus unicum genus respondet; 32, 52, 8, 1 quibus resp. 2, 4, 8, 16 genera respondent; hinc omnino emergunt genera 359, unde multitudo mediocris $=3{,}59$. Centum determinantes negativi a -801 usque ad 900 producunt genera 360. Exempla sequentia omnia desumuntur a determinantibus negativis. In centade 16 (a -1501 usque ad -1600) mult. med. generum invenitur 3,89; in centade 25 est 4,03; in centade 51 prodit 4,24; e sexcentis dett. -9401 . . . -10000 computatur 4,59. Ex his exemplis patet, multitudinem generum mediocrem multo lentius crescere, quam determinantes ipsos; sed quaeritur, quaenam sit lex huius progressionis? — Per disquisitionem theoreticam satis difficilem, quam hic explicare nimis prolixum foret, inventum est, multitudinem generum mediocrem circa determinantem $+D$ vel $-D$ quam proxime exhiberi per formulam

$$\alpha \log D+\vec{6}$$

ubi α, $\vec{6}$ sunt quantitates constantes, et quidem

$$\alpha = \frac{4}{\pi\pi} = 0{,}4052847346$$

(designante π semiperipheriam circuli cuius radius 1),

$$\vec{6} = 2\alpha g + 3\alpha\alpha h - \tfrac{1}{6}\alpha \log 2 = 0{,}8830460462$$

ubi g est summa seriei

$$1 - \log(1+1) + \tfrac{1}{2} - \log(1+\tfrac{1}{2}) + \tfrac{1}{3} - \log(1+\tfrac{1}{3}) + \text{etc.} = 0{,}5772156649$$

(V. Euler Inst. Calc. Diff. p. 444); h vero summa seriei

$$\tfrac{1}{4}\log 2 + \tfrac{1}{9}\log 3 + \tfrac{1}{16}\log 4 + \text{etc.}$$

quae per approximationem inventa est $= 0{,}9375482543$. Ex hac formula patet, multitudinem mediocrem generum crescere in progressione arithmetica, si determinantes augeantur in geometrica. Valores huius formulae pro $D = 850\frac{1}{2}$, $1550\frac{1}{2}$, $2450\frac{1}{2}$, $5050\frac{1}{2}$, $9700\frac{1}{2}$ inveniuntur 3,617; 3,86; 4,046; 4,339; 4,604, qui a multitudinibus mediocribus supra datis parum discrepant. Quo maior fuerit determinans medius, et e quo pluribus multitudo mediocris computetur, eo minus a valore formulae differet. Adiumento huius formulae etiam aggregatum multitudinum generum determinantibus successivis $\pm D, \pm(D+1) \ldots \pm(D+m)$ respondentium quam proxime erui potest, si multitudines mediocres singulis respondentes computantur et in summam colliguntur, quantumvis diversi sint extremi D, $D+m$. Haec summa erit

$$= \alpha\left(\log D + \log(D+1) + \text{etc.} + \log(D+m)\right) + \vec{6}(m+1)$$

sive satis exacte

$$= \alpha\left((D+m)\log(D+m) - (D-1)\log(D-1)\right) + (\vec{6}-\alpha)(m+1)$$

Hoc modo summa mult. gen. pro dett. -1 usque ad -100 invenitur $= 234{,}4$, quum revera sit 233; similiter, a -1 usque ad -2000, $= 7116{,}6$, quum sit 7112; a -9001 usque ad -10000 ubi est 4595 formula praebet 4594,9, qualis consensus vix exspectari potuisset.

De multitudine mediocri classium.

302.

Respectu *multitudinis classium* (pr. primit. posit., quod semper subintelligendum) determinantes positivi prorsus aliter se habent quam negativi; quamobrem utrosque seorsim considerabimus. In eo hi cum illis conveniunt, quod pro determinante dato in singulis generibus classes aeque multae continentur, adeoque multitudo omnium classium aequalis est producto e multitudine generum in multitudinem classium in singulis generibus contentarum.

Quod primo attinet ad determinantes negativos, multitudo classium pluribus dett. successivis $-D$, $-(D+1)$, $-(D+2)$ etc. respondentium progressionem aeque perturbatam constituit, ac multitudo generum. Multitudo classium mediocris autem (cui definitione opus non erit) valde regulariter crescit, ut ex exemplis sequentibus apparebit. Centum determinantes a -500 usque ad -600 suppeditant classes 1729, unde multitudo mediocris $= 17{,}29$. Similiter in centade 15 multitudo classium mediocris invenitur 28,26; e centadibus duabus 24 et 25 computatur 36,28; e tribus 61, 62 et 63 prodit 58,50 e quinque 91...95, fit 71,56; denique e quinque 96...100 fit 73,54. Haec exempla ostendunt, classium multitudinem mediocrem lentius quidem crescere, quam determinantes, multo tamen citius, quam multitudinem mediocrem generum; levi autem attentione cognoscetur, illam satis exacte crescere in ratione radicum quadratarum e determinantibus mediis. Revera per disquisitionem theoreticam invenimus, classium multitudinem mediocrem circa determinantem $-D$ proxime exprimi per:

$$\gamma\sqrt{D} - \delta$$

ubi

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7e}$$

denotante e summam seriei

$$1 + \tfrac{1}{8} + \tfrac{1}{27} + \tfrac{1}{64} + \tfrac{1}{125} \text{ etc.}$$

$$\delta = 0{,}2026423673 = \frac{2}{\pi\pi}$$

valores mediocres secundum hanc formulam computati ab iis, quos supra e tabula classificationum exscripsimus, parum differunt. Adiumento huius formulae etiam aggregatum multitudinum omnium classium (pr. pr. pos.) determinantibus suc-

cessivis $-D$, $-(D+1)$, $-(D+2)\ldots-(D+m-1)$ respondentium quum proxime assignari potest, quantumvis extremi sint diversi, summando multitudines mediocres illis determinantibus secundum formulam respondentes, unde erit

$$= \gamma(\sqrt{D}+\sqrt{(D+1)}+\text{etc.}+\sqrt{(D+m-1)})-\delta m$$

sive quam proxime

$$= \tfrac{2}{3}\gamma((D+m-\tfrac{1}{2})^{\frac{3}{2}}-(D-\tfrac{1}{2})^{\frac{3}{2}})-\delta m$$

Ita *e. g.* illud aggregatum pro centum dett. $-1\ldots-100$ ex formula computatur $= 481{,}1$, quum revera sit 477; mille determinantes $-1\ldots-1000$ secundum tabulam suppeditant 15533 classes, formula dat 15551,4; millias secunda sistit classes 28595 secundum tabulam, formula praebet 28585,7; similiter millias tertia revera suggerit 37092 classes, formula dat 37074,3; millias decima dat 72549 per tabulam, formula 72572.

303.

Tabula determinantium negativorum secundum diversitatem classificationum ipsis respondentium digesta multas alias observationes singulares offert. Pro determinantibus formae $-(8n+3)$ multitudo classium (tum earum quae in omnibus, tum earum quae in singulis generibus pr. primitivis contentae sunt) semper divisibilis est per 3, unico determinante -3 excepto, cuius rei ratio ex art. 256, VI sponte sequitur. Pro iis determinantibus, quorum formae unicum genus conficiunt, multitudo classium semper impar est; quum enim pro tali determinante unica tantum classis anceps detur, puta principalis, multitudo classium reliquarum, e quibus binae semper oppositae erunt, necessario erit par, adeoque multitudo omnium impar; ceterum haec posterior proprietas etiam pro determinantibus positivis valet. — Porro series determinantium, quibus eadem classificatio data (*i. e.* multitudo data tum generum tum classium) respondet, semper abrumpi videtur, quam observationem satis miram per aliquot exempla illustramus. (Numerus primus, romanus, indicat multitudinem generum pr. prim. pos.; sequens multitudinem classium in singulis generibus contentarum; tunc sequitur series determinantium, quibus illa classificatio respondet, et quorum signum negativum brevitatis caussa omittitur).

I. 1 ... 1, 2, 3, 4, 7
I. 3 ... 11, 19, 23, 27, 31, 43, 67, 163
I. 5 ... 47, 79, 103, 127
I. 7 ... 71, 151, 223, 343, 463, 487
II. 1 ... 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58
II. 2 ... 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193
IV. 1 ... 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
VIII. 1 ... 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760
XVI. 1 ... 840, 1320, 1365, 1848

Similiter 20 determinantes reperiuntur (maximus $= -1423$), quibus classificatio I. 9 respondet; 4 (maximus $= -1303$), quibus respondet classificatio I. 11 etc.; classificationes II. 3; II. 4; II. 5; IV. 2 respondent determinantibus non pluribus quam 48, 31, 44, 69 resp., e quibus maximi -652, -862, -1318, -1012. Quum tabula, ex qua haec exempla sumsimus, longe ultra maximos determinantes hic occurentes producta sit*), nec ulli amplius prodierint ad illas classificationes pertinentes: nullum dubium esse videtur, quin series adscriptae revera abruptae sint, et per analogiam conclusionem eandem ad quasvis alias classificationes extendere licebit. *E. g.* quum in tota milliade decima determinantium nullus se obtulerit, cui multitudo classium infra 24 responderet: maxime est verisimile, classificationes I. 23; I. 21 etc.; II. 11; II. 10 etc. IV. 5; IV. 4; IV. 3; VIII. 2 iam ante -9000 desiisse, aut saltem perpaucis determinantibus ultra -10000 competere. Demonstrationes autem *rigorosae* harum observationum perdifficiles esse videntur. — Non minus admiratione dignum est, quod omnes determinantes, quorum formae in 32 aut plura genera distribuantur, ad minimum binas classes in singulis generibus habeant, adeoque classificationes XXXII. 1. LXIV. 1 etc. omnino excidant (minimo ex huiusmodi dett., -9240, respondet XXXII. 2); satisque probabile videtur, multitudine generum crescente continuo plures classificationes excidere. Hoc respectu 65 determinantes supra traditi,

*) Dum haec imprimuntur, usque ad -3000 *uno tractu*, nec non per totam milliadem decimam, plurosque alias centades dispersas, quibus accedunt permulti determinantes singulares sedulo electi.

quibus classificationes I. 1; II. 1; IV. 1; VIII. 1; XVI. 1 respondent, valde sunt memorabiles, perspiciturque facile, illos omnes ac solos his duabus proprietatibus insignibus gaudere, ut omnes classes formarum ad ipsos pertinentes ancipites sint, et formae quaecunque in eodem genere contentae necessario tum proprie tum improprie aequivaleant. Ceterum iidem 65 numeri (sub aspectu paullulum diverso cuius mentio infra fiet et cum criterio demonstratu facili) iam ab ill. Eulero traditi sunt *Nouv. Mém. de l'Ac. de Berlin* 1776 *p.* 338.

304.

Multitudo classium pr. primitivarum, quas formae binariae det. positivi *quadrati* kk constituunt, omnino a priori assignari potest, multitudinique numerorum ad $2k$ primorum ipsoque minorum aequalis est; unde per ratiocinia non difficilia sed hic supprimenda deducitur, multitudinem mediocrem classium ad tales determinantes circa kk pertinentium proxime exprimi per $\frac{8k}{\pi\pi}$. — Determinantes positivi non-quadrati autem hoc respectu phaenomena prorsus singularia offerunt. Scilicet quum classium multitudo parva, *e. g.* classificatio I. 1 aut I. 3 aut II. 1 etc. pro determinantibus negativis et quadratis parvis tantum et mox omnino cessantibus locum habeat: contra e determinantibus positivis non-quadratis, saltem non permagnis, pars longe maxima tales classificationes praebent, ubi unica classis in quovis genere continetur, ita ut hae I. 3; I. 5; II. 2; II. 3; IV. 2 etc. sint rarissimae. Ita *e. g.* inter 90 dett. non-qu. infra 100 reperiuntur 11, 48, 27, quibus respondent classificationes I. 1, II. 1, IV. 1 resp.; unicus tantum (37) habet I. 3; duo (34 et 82) habent II. 2; unus (79) II. 3. Attamen, determinantibus crescentibus, classium multitudines maiores sensim frequentiores fiunt; ita inter 96 dett. non-qu. a 101 usque ad 200 duo (101, 197) habent I. 3; quatuor (145, 146, 178, 194) II. 2; tres (141, 148, 189) II. 3. Ex 197 dett. a 801 usque ad 1000 tres habent I. 3; quatuor II. 2; quatuordecim II. 3; duo II. 5; duo II. 6; quindecim IV. 2; sex IV. 3; duo IV. 4; quatuor VIII. 2; reliqui 145 unam classem in quovis genere. — Quaestio curiosa foret, nec geometrarum sagacitate indigna, secundum quam legem determinantes unam classem in quovis genere habentes continuo rariores fiant, investigare; hactenus nec per theoriam decidere possumus, nec per observationem satis certo coniectare, utrum tandem omnino abrumpantur (quod tamen parum probabile videtur), aut saltem *infinite rari* evadant, an ipsorum frequentia ad limitem fixum continuo magis accedat. Multitudo classium mediocris in ratione parum maiori increscit, quam multitudo generum, longeque lentius quam radices quadratae e determinantibus; inter 800 et 1000 illa invenitur $= 5{,}01$. Liceat his observationibus aliam adiicere, quae analogiam inter determinantes positivos et negativos quodammodo restituit. Scilicet invenimus, pro determinante positivo D non tam multitudinem classium ipsam, quam potius hanc multitudinem per logarithmum quantitatis $t+u\sqrt{D}$ multiplicatam (designantibus t, u numeros minimos, praeter 1, 0, aequationi $tt-Duu=1$ satisfacientes) multitudini classium pro determinante negativo pluribus rationibus hic fusius non explicandis analogam esse, atque valorem mediocrem illius producti aeque exacte exprimi per formulam talem $m\sqrt{D}-n$; sed valores quantitatum constantium m, n hactenus per theoriam determinare non licuit; si quid ex aliquot centadibus determinantium inter se comparatis concludere permissum est, m parum a $2\frac{1}{4}$ differre videtur. — Ceterum de principiis disquisitionum praecedentium circa valores mediocres quantitatum lege analytica non progredientium, sed ad talem legem asymptotice continuo magis approximantium alia occasione fusius agere nobis reservamus. Transimus iam ad aliam disquisitionem, qua classes diversae pr. prim. eiusdem det. inter se comparabuntur, finisque huic longae sectioni imponetur.

Algorithmus singularis classium proprie primitivarum: determinantes regulares et irregulares etc.

305.

Theorema. *Designante K classem principalem formarum determinantis dati D, C classem quamcunque aliam e genere principali formarum eiusdem det.; $2C$, $3C$, $4C$ etc. classes resp. e duplicatione, triplicatione, quadruplicatione etc. classis C ortas (ut in art. 249): in progressione C, $2C$, $3C$ etc. satis continuata tandem ad classem cum K identicam pervenitur; supponendoque, mC esse primam cum K identicam, atque multitudinem omnium classium in genere principali $= n$, erit vel $m = n$, vel m pars aliquota ipsius n.*

Dem. I. Quum omnes classes K, C, $2C$, $3C$ etc. necessario ad genus principale pertineant (art. 247), classes $n+1$ priores huius seriei K, C, $2C \ldots nC$ manifesto omnes diversae esse nequeunt. Erit itaque vel K cum aliqua classium C, $2C$, $3C \ldots nC$ identica, vel saltem duae ex his classibus inter se identicae.

Sit $rC = sC$ atque $r > s$, eritque etiam

$$(r-1)C = (s-1)C, \quad (r-2)C = (s-2)C \text{ etc. et } (r+1-s)C = C$$

unde $(r-s)C = K$. *Q. E. P.*

II. Hinc etiam protinus sequitur, esse vel $m = n$ vel $m < n$, superestque tantummodo, ut ostendamus, in casu posteriori m esse partem aliquotam ipsius n. Quum classes

$$K, \; C, \; 2C \ldots (m-1)C, \text{ quarum complexum per } \mathfrak{C}$$

designabimus, totum genus principale in hoc casu nondum exhauriant, sit C' aliqua classis huius generis in $\mathfrak{C}$ non contenta, designeturque complexus classium, quae ex compositione ipsius C' cum singulis classibus in $\mathfrak{C}$ oriuntur, puta

$$C', \; C'+C, \; C'+2C \ldots C'+(m-1)C \text{ per } \mathfrak{C}'$$

Iam facile perspicitur, omnes classes in $\mathfrak{C}'$ tum inter se tum ab omnibus in $\mathfrak{C}$ diversas esse et ad genus principale pertinere; quodsi itaque $\mathfrak{C}$ et $\mathfrak{C}'$ hoc genus omnino exhauriunt, habebimus $n = 2m$; sin minus, erit $2m < n$. Sit in casu posteriori C'' aliqua classis generis principalis nec in $\mathfrak{C}$ nec in $\mathfrak{C}'$ contenta, designeturque complexus classium ex compositione ipsius C'' cum singulis classibus in $\mathfrak{C}$ prodeuntium *i. e.* harum

$$C'', \; C''+C, \; C''+2C \ldots C''+(m-1)C \text{ per } \mathfrak{C}''$$

patetque facile, has omnes inter se et ab omnibus in $\mathfrak{C}$ et $\mathfrak{C}'$ diversas esse, et ad genus principale pertinere. Quare si $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ hoc genus exhauriunt, erit $n = 3m$; sin minus, $n > 3m$, in quo casu classis alia C''' in genere principali contenta, neque vero in $\mathfrak{C}$, $\mathfrak{C}'$ vel $\mathfrak{C}''$, simili modo tractata docebit, esse vel $n = 4m$ vel $n > 4m$, et sic porro. Iam quum n et m sint numeri finiti, genus principale necessario tandem exhaurietur, eritque n multiplum ipsius m, sive m pars aliquota ipsius n. *Q. E. S.*

Ex. Sit $D = -356$, $C = (5, 2, 72)$ *), invenieturque $2C = (20, 8, 21)$, $3C = (4, 0, 89)$, $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Hic

*) Classes hic semper per *formas* (simplicissimas) in ipsis contentas exprimuntur.

itaque est $m = 6$, n vero pro hoc determinante est 12. Accipiendo pro C' classem $(8, 2, 45)$, classes quinque reliquae in $\mathfrak{C}'$ erunt $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

306.

Demonstratio theor. praec. omnino analoga invenietur demonstrationibus in artt. 45, 49, reveraque theoria multiplicationis classium cum argumento in Sect. III. tractato permagnam undique affinitatem habet. At limites huius operis non permittunt, illam theoriam ea qua digna est ubertate hic persequi; quocirca paucas tantummodo observationes hic adiiciemus, eas quoque demonstrationes, quae apparatum prolixiorem requirerent, supprimemus, disquisitionemque ampliorem ad aliam occasionem nobis reservabimus.

I. Si series $K, \; C, \; 2C, \; 3C$ etc. ultra $(m-1)C$ producitur, eaedem classes iterum comparent,

$$mC = K, \quad (m+1)C = C, \quad (m+2)C = 2C \text{ etc.}$$

generaliterque (spectando concinnitatis caussa K tamquam $0C$) classes $gC, g'C$ identicae erunt vel diversae, prout g et g' secundum modulum m congrui sunt vel incongrui. Classis itaque nC semper identica est cum principali K.

II. Complexum classium $K, \; C, \; 2C \ldots (m-1)C$, quem supra per $\mathfrak{C}$ designavimus, vocabimus *periodum* classis C, quae expressio non est confundenda cum *periodis formarum* reductarum det. positivi non-quadrati in art. 186 sqq. tractatis. Patet itaque, e compositione classium quotcunque in eadem periodo contentarum oriri classem in ea periodo quoque contentam

$$gC + g'C + g''C \text{ etc.} = (g + g' + g'' + \text{etc.})C$$

III. Quum $C + (m-1)C = K$, classes C et $(m-1)C$ oppositae erunt, et perinde $2C$ et $(m-2)C$, $3C$ et $(m-3)C$ etc. Si itaque m est par, classis $\frac{1}{2}mC$ sibi ipsa opposita erit adeoque *anceps*; vice versa, si in $\mathfrak{C}$ praeter K adhuc alia classis anceps occurrit, puta gC, erit $gC = (m-g)C$ adeoque $g = m - g = \frac{1}{2}m$. Hinc sequitur, si m sit par, praeter duas K et $\frac{1}{2}mC$,

si vero m sit impar, praeter unam K, aliam classem ancipitem in $\mathfrak{C}$ contentam esse non posse.

IV. Si periodus alicuius classis hC in $\mathfrak{C}$ contentae supponitur esse

$$K,\ hC,\ 2hC,\ 3hC \ldots (m'-1)hC$$

manifestum est, $m'h$ esse multiplum minimum ipsius h per m divisibile. Si itaque m et h inter se primi sunt, erit $m' = m$, duaeque periodi easdem classes sed ordine diverso dispositas continebunt; generaliter autem designante μ divisorem comm. max. ipsorum m, h, erit $m' = \frac{m}{\mu}$. Hinc patet, multitudinem classium in periodo cuiusvis classis ex $\mathfrak{C}$ contentarum esse vel m vel partem aliquotam ipsius m; et quidem tot classes in $\mathfrak{C}$ habebunt periodos m terminorum, quot numeri ex his $0, 1, 2 \ldots m-1$ ad m primi sunt, sive φm, utendo signo art. 39; generaliter vero tot classes in $\mathfrak{C}$ habebunt periodos $\frac{m}{\mu}$ terminorum, quot numeri ex his $0, 1, 2 \ldots m-1$ divisorem maximum μ cum m communem habent, quorum multitudinem esse $\varphi\frac{m}{\mu}$ facile perspicitur. Si itaque $m = n$, sive *totum* genus principale sub $\mathfrak{C}$ contentum, dabuntur in hoc genere omnino φn classes, quarum periodi idem genus totum includunt, et φe classes, quarum periodi ex e terminis constant, denotante e divisorem quemcunque ipsius n. Haec conclusio generaliter valet, quando in genere principali ulla classis datur, cuius periodus ex n terminis constat.

V. Sub eadem suppositione, systema classium generis principalis aptius disponi nequit, quam aliquam classem, periodum n terminorum habentem, quasi pro *basi* adoptando, generisque principalis classes eodem ordine collocando, quo in illius periodo progrediuntur. Quodsi tunc classi principali *index* 0 adscribitur, classi, quae pro basi accepta est, index 1 et sic porro: per solam indicum additionem inveniri poterit, quaenam classis e compositione classium quarumcunque generis principalis oriatur. Ecce exemplum pro determinante -356, ubi classam $(9, 2, 40)$ pro basi accepimus:

0	(1, 0, 356)	4	(20, 8, 21)
1	(9, 2, 40)	5	(17, 1, 21)
2	(5, 2, 72)	6	(4, 0, 89)
3	(8, −2, 45)	7	(17, −1, 21)
8	(20, −8, 21)		
9	(8, 2, 45)		
10	(5, −2, 72)		
11	(9, −2, 40)		

VI. Quamquam vero tum analogia cum Sect. III, tum inductio circa plures quam 200 determinantes negativos, longeque adhuc plures positivos non-quadratos instituta maximam probabilitatem afferre videantur, illam suppositionem pro *omnibus* determinantibus locum habere: talis conclusio nihilominus falsa foret, et per tabulae classificationum continuationem refelleretur. Liceat, brevitatis caussa, eos determinantes, pro quibus totum genus principale unicae periodo includi potest, *regulares* vocare, reliquos vero, pro quibus hoc fieri nequit, *irregulares*. Hoc argumentum, quod ad arithmeticae sublimioris mysteria maxime recondita pertinere, disquisitionibusque difficillimis locum relinquere videtur, paucis tantum observationibus hic illustrare possumus, quibus sequentem generalem praemittimus.

VII. Si in genere principali classes C, C' occurrunt, quarum periodi ex m, m' classibus constant, atque M est numerus minimus per m et m' divisibilis: in eodem genere etiam classes dabuntur, quarum periodi M terminos contineant. Resolvatur M in duos factores r, r' inter se primos, quorum alter (r) metiatur ipsum m, alter (r') ipsum m' (v. art. 73), habebitque classis $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ proprietatem praescriptam. Supponamus enim, periodum classis C'' constare ex g terminis, eritque

$$K = grC'' = gmC + \frac{grm'}{r'}C' = K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C'$$

unde $\frac{grm'}{r'}$ per m' divisibilis esse debebit sive gr per r', adeoque etiam g per r'. Prorsus simili modo g per r divisibilis invenitur, unde etiam per $rr' = M$ divisibilis erit. Sed quum manifesto sit $MC'' = K$, erit etiam M per g divisibilis; quare necessario $M = g$. Hinc nullo negotio sequitur, multitudinem *maximam* classium, in ulla periodo contentarum (pro det. dato), divisibilem esse per multitudinem classium in quavis alia periodo (classis ex eodem genere principali). Simul ibinde methodus derivari potest, talem classem cuius periodus sit quam maxima (adeoque pro det. regulari totum genus principale complectatur) eruendi, methodo artt. 73, 74 prorsus analoga, etsi in praxi laborem per plura artificia contrahere liceat. Quotiens e divisione numeri n per multitudinem classium in periodo maxima, qui pro determinantibus regularibus est 1, pro irregularibus semper fit integer maior quam 1, et pro his imprimis commodus est ad diversas irregularitatis species exprimendas; quamobrem *exponens irregularitatis* dici poterit.

VIII. Hactenus regula generalis non habetur, per quam determinantes regulares ab irregularibus a priori distingui possent, praesertim quum inter posteriores numeri tum primi tum compositi reperiantur; sufficiat itaque quasdam observationes particulares hic adiunxisse. Quando in genere principali plures quam duae classes ancipites continentur, determinans certo est irregularis atque exponens irregularitatis par; quando vero una tantum aut duae in illo genere adsunt, det. aut regularis erit aut saltem exp. irr. impar. Omnes determinantes negativi formae $-(216k+27)$, unico -27 excepto, irregulares sunt, et exp. irr. per 3 divisibilis; idem valet de dett. negg. formae $-(1000k+75)$ et $-(1000k+675)$, unico -75 excepto, infinitisque aliis. Si exp. irr. est numerus primus p, aut saltem per p divisibilis, n per pp divisibilis erit, unde sequitur, si n nullum divisorem quadratum implicet, determinantem certo esse regularem. Pro solis determinantibus *quadratis* positivis ee a priori semper dignosci potest, utrum regulares sint an irregulares; scilicet illud evenit, quando e est 1 aut 2 aut numerus primus impar aut potestas numeri primi imparis; hoc in omnibus reliquis casibus. Pro dett. negg., irregulares continuo frequentiores evadunt, quo maiores fiunt determinantes; *e. g.* in tota milliade prima tredecim irregulares reperiuntur, (signo negativo omisso) 576, 580, 820, 884, 900, quorum exp. irr. est 2, atque 243, 307, 339, 459, 675, 755, 891, 974, quorum exp. irr. 3; in milliade secunda reperti sunt 13, quorum exp. irr. 2, atque 15, quorum exp. irr. 3; in milliade decima 31 cum exp. irr. 2 atque 32 cum exp. irr. 3. Num determinantes cum exp. irr. maiori quam 3 infra -10000 occurrant, decidere nondum licet; ultra hunc limitem exponentes quicunque dati provenire possunt. Frequentiam determinantium negativorum irregularium ad frequentiam regularium continuo magis, dett. crescentibus, ad rationem constantem appropinquare valde probabile est, cuius determinatio geometrarum sagacitate magnopere digna foret. — Pro determinantibus positivis non-quadratis irregulares multo rariores sunt; tales, quorum exp. irr. par sit, infinite multi certo dantur (*e. g.* 3026 pro quo est 2); nullum quoque dubium videtur, quin tales exstent, quorum exp. irr. sit impar, etsi fateri oporteat, nullum se hactenus nobis obtulisse.

IX. De adornatione maxime commoda systematis classium, in genere principali pro determinante irregulari contentarum, hic agere propter brevitatem non licet; observamus tantummodo, quum unica basis hic non sufficiat, duas

vel adeo plures adhuc classes hic esse accipiendas, e quarum multiplicatione et compositione omnes producantur. Hinc *indices duplices aut multiplices* emergent, qui eundem fere usum praestabunt ac simplices pro regularibus. Sed hanc rem alio tempore fusius tractabimus.

X. Denique observamus, quum omnes proprietates in hoc art. et pracc. consideratae imprimis a numero n pendeant, qui simile quid est ac $p-1$ in Sect. III, hunc numerum summa attentione dignum esse; quamobrem quam maxime optandum esset, ut inter ipsum atque determinantem, ad quem pertinet, nexus generalis detegatur. De qua re gravissima eo minus desperandum censemus, quoniam iam successit, valorem mediocrem producti ex n in multitudinem generum (quae a priori assignari potest) saltem pro determinantibus negativis formulae analyticae subiicere (art. 302).

307.

Disquisitiones artt. praecc. solas classes generis principales complectuntur, adeoque sufficiunt tum pro dett. poss., ubi unicum omnino genus datur, tum pro negativis, ubi unicum genus positivum adest, si ad genus negativum respicere nolumus. Superest, ut de reliquis quoque generibus (pr. primitivis) quaedam adiiciamus.

I. Quando in genere G' a principali G (eiusdem det.) diverso ulla classis anceps datur, totidem in ipso aderunt ac in G. Sint in G classes ancipites L, M, N etc. (inter quas etiam erit classis principalis K), in G' vero hae L', M', N' etc., designeturque illarum complexus per A, complexus harum per A'. Quum manifesto omnes classes $L+L'$, $M+L'$, $N+L'$ etc. ancipites diversaeque sint, et ad G' pertineant, adeoque sub A' contentae esse debeant: multitudo classium in A' certo nequit esse minor quam in A; similiter quum classes $L'+L$, $M'+L$, $N'+L$ etc. diversae ancipitesque sint et ad G pertineant, adeoque sub A contineantur, multitudo classium in A nequit esse minor quam in A'; quare multitudines classium in A et A' necessario aequales erunt.

II. Quum multitudo omnium classium ancipitum multitudini generum aequalis sit (artt. 261, 287 III); manifestum est, si in G una tantum classis anceps

detur, in *quovis* genere unam classem ancipitem contentam esse debere; si in G duae ancipites exstent, in semissi omnium generum binas dari, in reliquis nullas; denique si in G plures ancipites contineantur, puta a*), partem a^{tam} omnium generum a classes ancipites continere, reliqua nullas.

III. Sint, pro eo casu, ubi G duas classes ancipites continet, G, G', G'' etc. ea genera, quae binas, atque H, H', H'' etc. ea quae nullas continent, designeturque complexus illorum per $\mathfrak{G}$, complexus horum per $\mathfrak{H}$. Quum e compositione duarum classium ancipitum semper proveniat classis anceps (art. 249), nullo negotio perspicietur, e compositione duorum generum ex $\mathfrak{G}$ semper prodire genus ex $\mathfrak{G}$. Hinc porro sequitur, e compositione generis ex $\mathfrak{G}$ cum genere ex $\mathfrak{H}$ prodire genus ex $\mathfrak{H}$; si enim *e. g.* $G'+H$ non ad $\mathfrak{H}$ sed ad $\mathfrak{G}$ pertineret, etiam $G'+H+G'$ ad $\mathfrak{G}$ referendum esset, *Q. E. A.*, quoniam $G'+G'=G$ adeoque $G'+H+G'=H$. Denique facillime intelligitur, genera $G+H$, $G'+H$, $G''+H$ etc., una cum his $H+H$, $H'+H$, $H''+H$ etc. omnia diversa fore adeoque cum $\mathfrak{G}$ et $\mathfrak{H}$ simul sumtis identica; sed, per ea quae modo demonstrata sunt, genera $G+H$, $G'+H$, $G''+H$ etc. omnia pertinent ad $\mathfrak{H}$ adeoque hunc complexum exhauriunt; quare necessario reliqua $H+H$, $H'+H$, $H''+H$ etc. omnia ad $\mathfrak{G}$ pertinebunt, *i. e.* e compositione duorum generum ex $\mathfrak{H}$ semper oritur genus ex $\mathfrak{G}$.

IV. Si E est classis generis V, a principali G diversi, patet, $2E$, $4E$, $6E$ etc. omnes pertinere ad G; has vero $3E$, $5E$, $7E$ etc. ad V. Si itaque periodus classis $2E$ ex m terminis constat: manifesto in serie E, $2E$, $3E$ etc. classis $2mE$, nec ulla prior, cum K identica erit, sive periodus classis E ex $2m$ terminis constabit. Hinc multitudo terminorum in periodo classis cuiuscunque, ex alio genere quam principali, erit vel $2n$ vel pars aliquota ipsius $2n$, designante n multitudinem classium in singulis generibus.

V. Sit C classis data generis principalis G; E classis generis V, e cuius duplicatione C oriatur (qualis semper dabitur, art. 286), atque omnes classes ancipites (pr. prim. eiusdem det.) K, K', K'' etc., eruntque *omnes* classes, e quarum

*) Hoc pro solis determinantibus irregularibus evenire potest, eritque a semper potestas binarii.

duplicatione C oritur, hae: $E\,(=E+K)$, $E+K'$, $E+K''$ etc., quarum complexus exprimatur per Ω; multitudo harum classium aequalis erit multitudini classium ancipitum sive multitudini generum. Manifestum est, e classibus in Ω tot ad genus V pertinere, quot ancipites dentur in G; designando itaque harum multitudinem per a, patet, in quovis genere vel a classes ex Ω dari vel nullas. Hinc facile colligitur, quando sit $a=1$, in quovis genere contineri unam classem ex Ω; quando $a=2$, semissem omnium generum binas classes ex Ω continere, reliqua nullas, et quidem semissem priorem vel totam cum $\mathfrak{G}$ coincidere (in eadem significatione ut supra III), posteriorem cum $\mathfrak{H}$, vel hanc cum $\mathfrak{G}$, illam cum $\mathfrak{H}$. — Quando a adhuc maior est, semper pars a^{ta} omnium generum classes Ω includent (singula a classes).

VI. Supponamus iam, C esse talem classem, cuius periodus ex n terminis constet, perspicieturque facile, in eo casu, ubi $a=2$ adeoque n par, nullam ex Ω ad G pertinere posse (tunc enim talis classis in periodo classis C contenta foret; si itaque esset $=rC$, sive $2rC=C$, foret $2r\equiv 1 \pmod{n}$. *Q. E. A.*); quamobrem quum G ad $\mathfrak{G}$ pertineat, necessario omnes classes Ω inter genera $\mathfrak{H}$ distributae erunt. Hinc colligitur, quoniam (pro det. reg.) in G omnino dantur φn classes periodos n terminorum habentes, pro eo casu ubi $a=2$ inveniri in quovis genere $\mathfrak{H}$ omnino $2\varphi n$ classes, quarum periodi $2n$ terminos, adeoque tum genus suum tum principale, complectantur; quando vero $a=1$, in quovis genere a principali diverso φn huiusmodi classes dabuntur.

VII. His observationibus methodum sequentem superstruimus, systema *omnium* classium pr. prim. pro quolibet determinante regulari dato (irregulares enim omnino seponimus) quam aptissime construendi. Eligatur ad lubitum classis E, cuius periodus $2n$ terminos, adeoque tum genus suum quod sit V tum principale G complectatur; classes horum duorum generum ita disponantur, ut in illa periodo progrediuntur. Hoc modo res iam absoluta erit, quando plura genera quam haec duo omnino non adsunt, sive reliqua adiicere non necesse videtur (*e. g.* pro tali det. neg., ubi duo tantum genera positiva dantur). Quando vero quatuor aut plura genera construenda sunt, reliqua hoc modo tractentur. Sit V' aliquod e reliquis atque $V+V'=V'''$, dabunturque in V' et V''' duae classes ancipites (puta vel in utroque una, vel in altero duae, in altero nulla); ex his eli-

gatur una A ad lubitum, patetque facile, si A cum singulis classibus in G et V componatur, prodire $2n$ classes diversas ad V' et V'' pertinentes, adeoque haec genera omnino exhaurientes; ita haec quoque genera ordinari poterunt. — Si praeter haec quatuor genera alia adhuc supersunt, sit V''' unum e reliquis, atque V'''', V''''', V'''''' genera ea, quae prodeunt e compositione generis V''' cum V, V' et V''. Haec quatuor genera $V'''\ldots V''''''$ quatuor classes ancipites continebunt, patetque, si ex his una A' eligatur atque cum singulis classibus in G, V, V', V'' componatur, omnes classes in $V'''\ldots V''''''$ prodire. — Si adhuc plura genera supersunt, simili modo continuetur, donec omnia exhausta sint. Patet, si multitudo omnium generum construendorum sit 2^μ, omnino opus fore $\mu - 1$ classibus ancipitibus, et quamvis classem horum generum produci posse vel e multiplicatione classis E, vel e compositione classis, e tali multiplicatione ortae, cum una pluribusve ancipitibus. Ecce duo exempla, per quae haec praecepta illustrabuntur; plura de usu talis constructionis vel de artificiis, per quae labor sublevari potest, hic adiicere non licet.

I. Determinans -161.

Quatuor genera positiva; in singulis quaternae classes.

G	V
1,4; $R7$; $R23$	3,4; $N7$; $R23$
$(1, 0, 161) = K$	$(3, 1, 54) = E$
$(9, 1, 18) = 2E$	$(6, -1, 27) = 3E$
$(2, 1, 81) = 4E$	$(6, 1, 27) = 5E$
$(9, -1, 18) = 6E$	$(3, -1, 54) = 7E$

V'	V''
3,4; $R7$; $N23$	1,4; $N7$; $N23$
$(7, 0, 23) = A$	$(10, 3, 17) = A+E$
$(11, -2, 15) = A+2E$	$(5, 2, 33) = A+3E$
$(14, 7, 15) = A+4E$	$(5, -2, 33) = A+5E$
$(11, 2, 15) = A+6E$	$(10, -3, 17) = A+7E$

II. Determinans -546.

Octo genera positiva; in singulis ternae classes.

G	V
1 et 3, 8; $R3$; $R7$; $R13$	5 et 7, 8; $N3$; $N7$; $N13$
$(1, 0, 546) = K$	$(5, 2, 110) = E$
$(22, -2, 25) = 2E$	$(21, 0, 26) = 3E$
$(22, 2, 25) = 4E$	$(5, -2, 110) = 5E$

V'	V''
1 et 3, 8; $N3$; $R7$; $N13$	5 et 7, 8; $R3$; $N7$; $R13$
$(2, 0, 273) = A$	$(10, 2, 55) = A+E$
$(11, -2, 50) = A+2E$	$(13, 0, 42) = A+3E$
$(11, 2, 50) = A+4E$	$(10, -2, 55) = A+5E$

V'''	V''''
1 et 3, 8; $N3$; $N7$; $R13$	5 et 7, 8; $R3$; $R7$; $N13$
$(3, 0, 182) = A'$	$(15, -3, 37) = A'+E$
$(17, 7, 35) = A'+2E$	$(7, 0, 78) = A'+3E$
$(17, -7, 35) = A'+4E$	$(15, 3, 37) = A'+5E$

V'''''	V''''''
1 et 3, 8; $R3$; $N7$; $N13$	5 et 7, 8; $N3$; $R7$; $R13$
$(6, 0, 91) = A+A'$	$(23, 11, 29) = A+A'+E$
$(19, 9, 33) = A+A'+2E$	$(14, 0, 39) = A+A'+3E$
$(19, -9, 33) = A+A'+4E$	$(23, -11, 29) = A+A'+5E$