porro numerus M per F repraesentatur, faciendo $x = m$, $y = n$, *adeoque per F′ faciendo* $x' = \alpha m + \beta n = m'$, $y' = \gamma m + \delta n = n'$ *et quidem ita vt m ad n eoque ipso etiam m′ ad n′ sit primus: ambae repraesentationes aut ad eundem valorem expressionis* $\sqrt{D}$ *(mod. M) pertinebunt, aut ad oppositos, prout transformatio formae F′ in F propria est vel impropria.*

Dem. Determinentur numeri μ, ν ita vt fiat $\mu m + \nu n = 1$, ponaturque $\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu'$, $\frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$ (qui erunt integri propter $\alpha\delta - \beta\gamma = \pm 1$). Tum erit $\mu m' + \nu' n' = 1$. (Cf. art. praec. fin.). Porro sit $\mu(bm + cn) - \nu(am + bn) = V$, $\mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$, eruntque V, V' valores expr. $\sqrt{M}$ (mod. D) ad quos repraesentatio prima et secunda pertinent. Si in V' pro μ, ν, m, n valores ipsorum substituuntur; in V vero pro a, $a'\alpha\alpha + 2b'\alpha\gamma + c'\gamma\gamma$ pro b, $a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta$; pro c, $a'\beta\beta + 2b'\beta\delta + c'\delta\delta$: inuenietur euolutione 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. $\sqrt{M}$ (mod. D) 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 *diuersos* expr. $\sqrt{D}$ (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 aequiualentem.

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

Demonstr. Ex art. 155 patet, numeros integros μ, ν inueniri posse ita vt sit $m\mu + n\nu = 1$, $\mu(bm + cn) - \nu(am + bn) = N$. 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. $= D$, siue in formam aequiualentem: quae forma si ponitur $= \left(M', N', \frac{N'N' - D}{M'}\right)$, erit $M' = amm + 2bmn + cnn = M$; $N' = - m\nu a + (m\mu - n\nu)b + n\mu c = N$. Quare forma in quam (a, b, c) per transformationem illam mutatur erit $\left(M, N, \frac{NN - D}{M}\right)$. Q. E. D.

Ceterum ex aequationibus $m + n\nu = 1$, $\mu(mb + nc) - \nu(ma + nb) = N$ deducitur $\mu = \frac{nN + ma + nb}{amm + 2bmn + cnn} = \frac{nN + ma + nb}{M}$; $\nu = \frac{mb + nc - mN}{M}$, qui numeri itaque erunt integri.

Porro obseruandum, 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. $\sqrt{D}$ (mod. M), N, pertinentes (vbi valores ipsorum x, y semper inter se primos supponimus): plures etiam transformationes propriae formae (a, b, c), (F), in $\left(M, N \frac{NN - D}{M}\right)$, (G) inde deducentur. Scilicet si etiam per hos valores $x = m'$, $y = n'$ talis repraesentatio prouenit, (F) etiam per substitutionem $x = m'x' + \frac{m'N - n'b - n'c}{M} y'$, $y = n'x' + \frac{n'N + m'a + m'b}{M} y'$ in (G) transit. Vice versa, ex quauis 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. $\sqrt{D}$ (mod. M) ad quem repraesentatio pertinet erit $\mu(bm + cn) - \nu(am + bn)$ i. e. N. Ex pluribus vero transformationibus propriis diuersis, sequentur totidem repraesentationes diuersae ad N pertinentes **). — Hinc

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

**) Si ex duabus transformationibus propriis diuersis eadem repraesentatio defluere supponitur, illae ita se habere debebunt: 1) $x = mx' - \nu y'$, $y = nx' + \mu y'$; 2) $x = mx' - \nu' y'$, $y = nx'$