primitiuo (positiuo) 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 vti, in qua continetur forma huius ordinis simplicissima. Quam itaque pro K et L assumendo, res eo reducta et, vt omnes classes proprie primitiuae 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 primitiua 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 $A\ (aq''q'' - 2bqq'' + cqq) = A^3$, vnde $AA = aq''q'' - 2bqq'' + cqq$. Q. E. P.

II. Si *supponitur*, A per f repraesentari posse, designentur valores indeterminatarum per quos hoc efficitur per q'', $-q$, siue sit $AA = aq''q'' - 2bqq'' + cqq$, ponaturque $q''a - q(b + B) = Ap$, $-qC = Ap'$, $q''(b - B) - qc = Ap''$, $-q''C = Ap'''$, $q''a - q(b - B) = Aq'$, $q''(b + B) - qc = Aq'''$. 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, A est vel o vel $\frac{1}{2}B$; adeoque $\frac{2B}{A}$ integer; ibinde patet, $\frac{C}{A}$ semper esse integrum. Hinc $q' - p$, p', $q''' - p''$, p''' erunt integri, superestque adeo tantummodo, vt probetur p et p'' esse integros. Fit autem $pp + \frac{2pqB}{A} = a$, $p''p'' + \frac{2p''q''B}{A} = c$; quamobrem si $B = 0$, fit $pp = a$, $p''p'' = c$, et proin p, p'' integri; si vero $B = \frac{1}{2}A$, fit $pp + pq = a$, $p''p'' + p''q'' = c$, vnde 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, vt omnes classes proprie primitiuas determinantis D assignare oporteat, per quarum formas repraesentari potest AA. Manifesto AA repraesentari potest per quamuis 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 diuisor communis maximus e, forma f per substitutionem α, β, γ, δ transibit in formam cuius terminus primus $\frac{A}{ee}$, formaque haec proprie aequiualebit formae f, si β, δ ita accipiuntur vt fiat $\alpha\delta - \beta\gamma = 1$; vnde

patet, in quauis classe, per cuius formas repraesentari possit AA, inueniri formas, quarum terminus primus sit AA vel quadratum partis aliquotae ipsius A. Res itaque in eo versatur, vt omnes classes proprie primitiuae det. D eruantur, in quibus huiusmodi formae occurrant; quod obtinetur sequenti modo: Sint a, a', a'' etc. omnes diuisores (positiui) ipsius A; inuestigentur omnes valores expr. $\sqrt{D}$ (mod. aa) inter 0 et $aa - 1$ incl. siti, qui sint b, b', b'' etc. statuaturque $bb - D = aac$, $b'b' - D = aac'$, $b''b'' - D = aac''$ etc.; complexus formarum (aa, b, c), (aa, b', c') etc. designetur per V. Tunc facile perspicitur, in quauis 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 primitiuae, reducantur reliquae in classes, et, si forte plures adsint ad eandem classem pertinentes, in singulis classibus vna tantum retineatur. Hoc modo omnes classes quaesitae habebuntur, eritque harum multitudo ad vnitatem, vt multitudo omnium classium proprie primitiuarum (positiuarum) ad multitudinem classium in ordine O.

Ex. Sit $D = -531$, atque O ordo positiuus deriuatus ex ordine improprie primitiuo det. -59, in quo forma simplicissima $(6, 3, 90)$