rationales euaderent; per art. 42 autem cuncti hi coëfficientes necessario forent integri. Hinc etiam p, p', p'' etc. omnes integri forent, quorum productum quum sit n^λ, multitudo vero $n - 1 > \lambda$, necessario quidam ex ipsis (saltem $n - 1 - \lambda$) esse debebunt $= 1$, reliqui vero ipsi n vel potestati ipsius n aequales. Quodsi itaque g ex ipsis sunt $= 1$, summa $p + p' +$ etc. manifesto erit $\equiv g$ (mod. n) adeoque certo per n non diuisibilis. Quare suppositio consistere nequit.

II. Quando $\mathfrak{P}$ et $\mathfrak{R}$ non quidem coincidunt, attamen quasdem radices communes continent, sit $\mathfrak{T}$ harum complexus atque $T = 0$ aequatio cuius radices sunt. Tunc T erit diuisor communis maximus functionum P, R (vt e theoria aequationum constat). Manifesto autem binae semper radices in $\mathfrak{T}$ reciprocae erunt, vnde per ante demonstrata omnes coëfficientes in T rationales esse nequeunt. Hoc vero certo eueniret, si omnes in P adeoque etiam omnes in R rationales essent, vt e natura operationis, diuisorem comm. max. inuestigandi sponte sequitur. Quare suppositio est absurda.

III. Quando $\mathfrak{Q}$ et $\mathfrak{S}$ vel coincidunt, vel saltem radices communes implicant, prorsus eodem modo omnes coëfficientes in Q rationales esse nequeunt; fierent vero rationales, si omnes in P rationales essent; hoc itaque est impossibile.

IV. Si vero neque $\mathfrak{P}$ cum $\mathfrak{R}$, neque $\mathfrak{Q}$ cum $\mathfrak{S}$ vllam radicem communem habet, omnes radices $\mathfrak{P}$ necessario reperientur in $\mathfrak{S}$, omnesque $\mathfrak{Q}$ in $\mathfrak{R}$, vnde erit $P = S$ et $Q = R$. Quamobrem $X = PQ$ erit productum ex P in R, i. e. ex $x^\lambda + Ax^{\lambda-1} \ldots + Kx + L$ in $x^\lambda + \frac{K}{L}x^{\lambda-1} \ldots + \frac{A}{L}x + \frac{1}{L}$, vnde statuendo $x = 1$, fit $nL = (1 + A \ldots + K + L)^2$. Iam si omnes coëfficientes in P rationales, adeoque per art. 42 etiam integri essent, L qui coëfficientem vltimum in X i. e vnitatem metiri deberet necessario foret $= \pm 1$, vnde $\pm n$ esset numerus quadratus. Quod quum hypothesi repugnet, suppositio consistere nequit.

Ex hoc itaque theoremate liquet, quomodocunque X in factores resoluatur, horum coëfficientes partim saltem irrationales fieri, adeoque aliter, quam per aequationem eleuatam, determinari non posse.

342. Propositum disquisitionum sequentium, quod paucis declarauisse haud inutile erit, eo tendit, vt X in factores continuo plures GRADATIM resoluatur, et quidem ita, vt horum coëfficientes per aequationes ordinis quam infimi determinentur, vsque dum hoc modo ad factores simplices siue ad radices Ω ipsas perueniatur. Scilicet ostendemus, si numerus $n - 1$ quomodocunque in factores integros α, β, γ etc. resoluatur (pro quibus singulis numeros primos accipere licet), X in α factores $\frac{n-1}{\alpha}$ dimensionum resolui posse, quorum coëfficientes per ae-

quationem α^{ti} gradus determinentur; singulos hos factores iterum in β alios $\frac{n-1}{\alpha\beta}$ dimensionum adiumento aequationis β^{ti} gradus etc., ita vt designante ν multitudinem factorum α, β, γ etc. inuentio radicum Ω ad resolutionum ν aequationum α^{ti}, β^{ti}, γ^{ti} etc. gradus reducatur. E. g. pro $n = 17$, vbi $n - 1 = 2.2.2.2$, quatuor aequationes quadraticas soluere oportebit; pro $n = 73$ tres quadraticas duasque cubicas.

Quum in sequentibus persaepe tales potestates radicis r considerandae sint, quarum exponentes rursus sunt dignitates, huiusmodi expressiones autem non sine molestia typis describantur: ad facilitandam impressionem sequenti in posterum abbreuiatione vtemur. Pro r, rr, r^3 etc. scribemus [1], [2], [3] etc., generaliterque pro r^λ, denotante λ integrum quemcunque, $[\lambda]$. Tales itaque expressiones penitus determinatae nondum sunt, sed fiunt, simulac pro r siue [1] radix determinata ex Ω accipitur. Erunt itaque generaliter $[\lambda]$, $[\mu]$ aequales vel inaequales, prout λ, μ secundum modulum n congrui sunt vel incongrui; porro $[0] = 1$; $[\lambda].[\mu] = [\lambda + \mu]$; $[\lambda]^\nu = [\lambda\nu]$; summa $[0] + [\lambda] + [2\lambda] \ldots + [(n-1)\lambda]$ vel o vel n, prout λ per n non diuisibilis est vel diuisibilis.

343. Si, pro modulo n, g est numerus talis, qualem in sect. III radicem primitiuam diximus, $n - 1$ numeri $1, g, gg \ldots g^{n-2}$ his $1, 2, 3 \ldots n - 1$ secundum mod. n congrui erunt, etsi alio ordine, puta quiuis numerus vnius seriei