Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0182
LOG Titel: §. 163. Theorie der Ideale eines endlichen Körpers
LOG Typ: chapter

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

§. 163.

Wir gründen die Theorie der in $\mathfrak{o}$ enthaltenen Zahlen, d. h. aller ganzen Zahlen des Körpers Ω, auf den folgenden neuen Begriff.

1. Ein System $\mathfrak{a}$ von unendlich vielen in $\mathfrak{o}$ enthaltenen Zahlen soll ein *Ideal* heissen, wenn es den beiden Bedingungen genügt;

I. Die Summe und die Differenz je zweier Zahlen in $\mathfrak{a}$ sind wieder Zahlen in $\mathfrak{a}$.

II. Jedes Product aus einer Zahl in $\mathfrak{a}$ und einer Zahl in $\mathfrak{o}$ ist wieder eine Zahl in $\mathfrak{a}$.

Ist α in $\mathfrak{a}$ enthalten, so sagen wir, α sei *theilbar durch* $\mathfrak{a}$, $\mathfrak{a}$ *gehe in* α *auf*, weil die Ausdrucksweise hierdurch an Leichtigkeit gewinnt. Wir nennen ferner zwei in $\mathfrak{o}$ enthaltene Zahlen ω, ω', deren Differenz durch $\mathfrak{a}$ theilbar ist, *congruent nach* $\mathfrak{a}$ (vergl. §. 161), und bezeichnen dies durch die Congruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$; solche Congruenzen dürfen (zufolge I.) addirt, subtrahirt und (zufolge II.) multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen auch einander congruent sind, so kann man alle Zahlen in *Classen* (mod. $\mathfrak{a}$) eintheilen, indem man je zwei congruente Zahlen in dieselbe, je zwei incongruente Zahlen in zwei verschiedene Classen wirft; da nun, wenn μ eine von Null verschiedene Zahl in $\mathfrak{a}$ bedeutet, je zwei nach μ congruente Zahlen (zufolge II.) auch nach $\mathfrak{a}$ congruent sind — woraus zugleich folgt, dass $\mathfrak{a}$ aus einer oder mehreren Classen (mod. μ) besteht — so ist (zufolge §. 162, 2.) die Anzahl der Classen (mod. $\mathfrak{a}$), in welche $\mathfrak{o}$ zerfällt, *endlich**). Wählt man aus jeder Classe ein Individuum als Repräsentanten, so bilden dieselben ein *vollständiges Restsystem* (mod. $\mathfrak{a}$); die Anzahl dieser Classen oder incongruenten Zahlen soll die *Norm* von $\mathfrak{a}$ heissen und mit $N(\mathfrak{a})$ bezeichnet werden.

Ist η eine von Null verschiedene Zahl in $\mathfrak{o}$, so bilden alle durch η theilbaren Zahlen in $\mathfrak{o}$ ein Ideal, welches mit $\mathfrak{i}(\eta)$ bezeichnet werden soll; solche Ideale sind besonders ausgezeichnet und sollen

*) Dasselbe ergiebt sich unmittelbar aus §. 161; ist nämlich ω irgend eine Zahl in $\mathfrak{o}$, so kann durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl der Quotient $\omega : \mu$ in eine ganze Zahl, also ω (zufolge II.) in eine Zahl des Ideals $\mathfrak{a}$ verwandelt werden.

Hauptideale heissen; die Norm von $\mathfrak{i}(\eta)$ ist $= \pm N(\eta)$; ist η eine Einheit, so ist $\mathfrak{i}(\eta) = \mathfrak{o}$, und umgekehrt.

2. Wenn alle Zahlen eines Ideals $\mathfrak{a}$ auch in einem Ideal $\mathfrak{b}$ enthalten sind, so besteht offenbar $\mathfrak{b}$ aus einer oder mehreren Classen (mod. $\mathfrak{a}$), und wir wollen sagen, $\mathfrak{a}$ sei ein *Multiplum von* $\mathfrak{b}$ oder *theilbar durch* $\mathfrak{b}$, $\mathfrak{b}$ sei ein *Theiler von* $\mathfrak{a}$ oder *gehe in* $\mathfrak{a}$ *auf*.

Besteht $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{a}$), so ist $N(\mathfrak{a}) = rN(\mathfrak{b})$. Durchläuft nämlich δ die Repräsentanten dieser r Classen, und γ ein vollständiges Restsystem (mod. $\mathfrak{b}$), so bilden die $rN(\mathfrak{b})$ Zahlen $\gamma + \delta$ ein vollständiges Restsystem (mod. $\mathfrak{a}$); denn erstens ist jede Zahl in $\mathfrak{o}$ congruent einer Zahl γ (mod. $\mathfrak{b}$), also $\equiv \gamma + \delta$ (mod. $\mathfrak{a}$), und zweitens folgt aus $\gamma + \delta \equiv \gamma' + \delta'$ (mod. $\mathfrak{a}$), wo γ', δ' ähnliche Bedeutung haben wie γ, δ, successive $\gamma + \delta \equiv \gamma' + \delta'$ (mod. $\mathfrak{b}$), $\gamma \equiv \gamma'$ (mod. $\mathfrak{b}$), $\gamma = \gamma'$, also $\delta \equiv \delta'$ (mod. $\mathfrak{a}$), $\delta = \delta'$, d. h. die sämmtlichen Zahlen $\gamma + \delta$ sind incongruent (mod. $\mathfrak{a}$).

Ein Ideal besitzt folglich nur eine *endliche* Anzahl von Theilern. Ist $\mathfrak{m}$ theilbar durch $\mathfrak{a}$, $\mathfrak{a}$ durch $\mathfrak{b}$, so ist auch $\mathfrak{m}$ durch $\mathfrak{b}$ theilbar. Das Hauptideal $\mathfrak{o}$ selbst geht in jedem Ideal auf und ist zugleich das *einzige* Ideal, welches die Zahl 1 oder überhaupt Einheiten enthält, und dessen Norm $= 1$ ist.

Das System aller derjenigen Zahlen, welche gleichzeitig in zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, ist das *kleinste gemeinschaftliche Multiplum* $\mathfrak{m}$ von $\mathfrak{a}$, $\mathfrak{b}$, insofern jedes gemeinschaftliche Multiplum von $\mathfrak{a}$, $\mathfrak{b}$ durch das Ideal $\mathfrak{m}$ theilbar ist. Durchläuft α alle Zahlen in $\mathfrak{a}$, β alle Zahlen in $\mathfrak{b}$, so ist das System aller Zahlen $\alpha + \beta$ der *grösste gemeinschaftliche Theiler* $\mathfrak{b}$ der Ideale $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideale $\mathfrak{b}$ aufgeht*).

Ist r die Anzahl der in $\mathfrak{b}$ enthaltenen Zahlen, welche (mod. $\mathfrak{a}$) incongruent sind, so besteht $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{m}$), und $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{a}$); also ist $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{b})$, und $N(\mathfrak{m})N(\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Ist $\mathfrak{b}$ ein Hauptideal $= \mathfrak{i}(\eta)$, so ist die Anzahl r der in $\mathfrak{b}$ enthaltenen Zahlen $\beta = \eta\omega$, welche (mod. $\mathfrak{a}$) incongruent sind, zugleich die Norm des aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehenden Ideals $\mathfrak{r}$, weil zwei Zahlen ω, ω' stets und nur dann congruent (mod. $\mathfrak{r}$) sind, wenn $\eta\omega \equiv \eta\omega'$ (mod $\mathfrak{a}$) ist. Mithin ist in diesem Falle $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{b})$.

*) Die Erweiterung dieser Definitionen von $\mathfrak{m}$ und $\mathfrak{b}$ für mehr als zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ . . . liegt auf der Hand.

3. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$, welches keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Theiler besitzt, soll ein *Primideal* heissen. Dann gilt folgender Satz:

Ist $\eta\varrho \equiv 0$ *(mod.* $\mathfrak{p}$*), so ist wenigstens eine der beiden Zahlen* η, ϱ *durch* $\mathfrak{p}$ *theilbar.* Ist nämlich η nicht $\equiv 0$ (mod. $\mathfrak{p}$), so bilden die sämmtlichen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{p}$) offenbar ein in $\mathfrak{p}$ aufgehendes Ideal, welches, da es die Zahl 1 nicht enthält, von $\mathfrak{o}$ verschieden und folglich mit $\mathfrak{p}$ identisch ist, was zu beweisen war.

Dieser Satz ist charakteristisch für ein Primideal, da er sich folgendermaassen umkehren lässt: *Enthält jedes durch ein (von* $\mathfrak{o}$ *verschiedenes) Ideal* $\mathfrak{p}$ *theilbare Product mindestens einen durch* $\mathfrak{p}$ *theilbaren Factor, so ist* $\mathfrak{p}$ *ein Primideal.* Ist nämlich $\mathfrak{q}$ ein Theiler des Ideals $\mathfrak{p}$, aber verschieden von $\mathfrak{p}$, so giebt es in $\mathfrak{q}$ eine nicht in $\mathfrak{p}$ enthaltene Zahl ω; dann ist (zufolge der Annahme) auch keine der Potenzen ω^2, ω^3 . . . durch $\mathfrak{p}$ theilbar; da aber nur eine endliche Anzahl von incongruenten Zahlen (mod. $\mathfrak{p}$) existirt, so muss einmal für zwei *verschiedene* Exponenten m und $m + s > m$ nothwendig $\omega^{m+s} \equiv \omega^m$ (mod. $\mathfrak{p}$), also das Product $\omega^m(\omega^s - 1)$ durch $\mathfrak{p}$ theilbar sein; da nun ω^m nicht durch $\mathfrak{p}$ theilbar ist, so muss (zufolge der Annahme) der andere Factor $\omega^s - 1$ durch $\mathfrak{p}$, und folglich auch durch $\mathfrak{q}$ theilbar sein; nun ist ω und, weil $s > 0$ ist, auch $\omega^s \equiv 0$ (mod. $\mathfrak{q}$), mithin ist auch die Zahl 1 in $\mathfrak{q}$ enthalten, also $\mathfrak{q} = \mathfrak{o}$, was zu beweisen war.

Nennt man ein von $\mathfrak{o}$ verschiedenes Ideal *zusammengesetzt*, wenn es kein Primideal ist, so lässt sich dieser Satz auch so aussprechen: *Ist* $\mathfrak{a}$ *ein zusammengesetztes Ideal, so giebt es zwei durch* $\mathfrak{a}$ *nicht theilbare Zahlen* η, ϱ, *deren Product* $\eta\varrho$ *durch* $\mathfrak{a}$ *theilbar ist.* Wir beweisen ihn zum zweiten Male auf folgende Art. Es sei $\mathfrak{e}$ ein von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedener Theiler von $\mathfrak{a}$, so giebt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht theilbare Zahl η, und der grösste gemeinschaftliche Theiler $\mathfrak{d}$ von $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ ist theilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, mithin ist $N(\mathfrak{d}) > 1$. Das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehende Ideal $\mathfrak{r}$ ist ein Theiler von $\mathfrak{a}$, und da (zufolge 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d}) > N(\mathfrak{r})$ ist, so ist $\mathfrak{r}$ verschieden von $\mathfrak{a}$ und enthält folglich eine durch $\mathfrak{a}$ nicht theilbare Zahl ϱ, was zu beweisen war.

Es leuchtet nun ein, dass die kleinste (von Null verschiedene) rationale Zahl p, welche in einem Primideale $\mathfrak{p}$ enthalten ist, nothwendig eine *Primzahl* (im rationalen Zahlkörper) sein muss; da

ferner $\mathfrak{p}$ in $\mathfrak{i}(p)$ aufgeht, so ist $N(\mathfrak{p})$ ein Theiler von $N(p) = p^n$, also ebenfalls eine Potenz $p^{f'}$ der rationalen Primzahl p, und man findet leicht (vergl. §. 162, 3.), dass jede in $\mathfrak{o}$ enthaltene Zahl ω der Congruenz

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}}$$

genügt*). Auch hat es keine Schwierigkeit, die allgemeinen Sätze der §§. 26, 27, 29, 30, 31 auf Congruenzen in Bezug auf den Modul $\mathfrak{p}$ zu übertragen.

Ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ *der Ideale* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ *durch das Primideal* $\mathfrak{p}$ *theilbar, so geht* $\mathfrak{p}$ *wenigstens in einem der Ideale* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ *auf.* Ist nämlich *keins* dieser Ideale durch $\mathfrak{p}$ theilbar, giebt es also in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ resp. Zahlen $\alpha, \beta, \gamma \ldots$, die nicht durch $\mathfrak{p}$ theilbar sind, so ist das in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$, also auch in

---

*) Hierauf beruht das Eingreifen der *Theorie der höheren Congruenzen* (vergl. §. 26), welche zur Bestimmung der Primideale dient. Für die Körper vom Grade $n = \varphi(m)$, welche aus den primitiven Wurzeln θ der Gleichung $\theta^m = 1$ entspringen, ist dieselbe zuerst ausgeführt, und zwar von *Kummer*, dem Schöpfer der Theorie der idealen Zahlen; den hierauf bezüglichen Theil seiner Untersuchungen findet man am vollständigsten zusammengestellt in den Abhandlungen: *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers* (Journ. de Math. p. p. Liouville, T. XVI. 1851). — *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist* (Abh. der Berliner Ak. 1856). Das Hauptresultat ergiebt sich mit grösster Leichtigkeit aus unserer Theorie und lautet in unserer Ausdrucksweise folgendermassen: Ist p eine rationale Primzahl und m' der grösste durch p nicht theilbare Divisor von $m = p'm'$, *gehört* ferner p zum Exponenten $f \pmod{m'}$, wo $\varphi(m') = ef$ (§. 28), so ist $\mathfrak{i}(p) = (\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e)^{\varphi(p')}$, wo $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_e$ von einander verschiedene Primideale bedeuten, deren Normen $= p^f$ sind; wenn $p' > 1$, so ist $\mathfrak{i}(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e$. — Für complexe Zahlen einer höheren Stufe vergl. *Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist* (Abh. der Berliner Ak. 1859). — Für diejenigen Körper Ω, deren conjugirte Körper mit Ω identisch sind, und welche ich *Galois'sche Körper* nennen möchte, vergl. *Selling: Ueber die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductibelen Gleichung rational gebildet sind* (Schlömilch's Zeitschr. für Math. u. Phys. Bd. 10. 1865). — Ein specieller Fall biquadratischer Körper ist vollständig durchgeführt von *Bachmann: Die Theorie der complexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind.* 1867. — Für eine gewisse Classe cubischer Körper vergl. *Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken* (Crelle's Journ. XXVIII).

$\mathfrak{m}$ enthaltene Product $\alpha\beta\gamma\ldots$ nicht theilbar durch das Primideal $\mathfrak{p}$, und folglich geht $\mathfrak{p}$ *nicht* in $\mathfrak{m}$ auf, was zu beweisen war.

Ist die Zahl η nicht theilbar durch das Ideal $\mathfrak{a}$, so giebt es immer eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{a}$) ein Primideal bilden. Alle Wurzeln β der Congruenz $\eta\beta \equiv 0$ (mod. $\mathfrak{a}$) bilden ein in $\mathfrak{a}$ aufgehendes Ideal $\mathfrak{b}$, welches von $\mathfrak{o}$ verschieden ist, weil es die Zahl 1 nicht enthält; ist $\mathfrak{b}$ ein Primideal, so ist der Satz bewiesen. Ist $\mathfrak{b}$ kein Primideal, giebt es also zwei durch $\mathfrak{b}$ nicht theilbare Zahlen η', ϱ', deren Product $\eta'\varrho' \equiv 0$ (mod. $\mathfrak{b}$) ist, so bilden alle Wurzeln γ der Congruenz $\eta'\gamma \equiv 0$ (mod. $\mathfrak{b}$), d. h. der Congruenz $\eta\eta'\gamma \equiv 0$ (mod. $\mathfrak{a}$), ein in $\mathfrak{b}$ aufgehendes Ideal $\mathfrak{c}$, und zwar ist (zufolge 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, weil ϱ' in $\mathfrak{c}$, aber nicht in $\mathfrak{b}$ enthalten ist; ausserdem ist $\mathfrak{c}$ von $\mathfrak{o}$ verschieden, weil η' nicht in $\mathfrak{b}$, und folglich die Zahl 1 nicht in $\mathfrak{c}$ enthalten ist; ist $\mathfrak{c}$ ein Primideal, so ist der Satz bewiesen. Ist aber $\mathfrak{c}$ kein Primideal, so kann man in derselben Weise fortfahren; endlich muss in der Reihe der Ideale $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}\ldots$, deren Normen immer kleiner werden, aber stets > 1 bleiben, ein Primideal $\mathfrak{p}$ auftreten, welches aus allen Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{a}$) besteht, wo $\nu = \eta\eta'\eta''\ldots$ durch η theilbar ist.

4. Ist μ eine von Null verschiedene Zahl in $\mathfrak{o}$ und keine Einheit, so existirt zufolge des zuletzt bewiesenen Satzes (in welchem man $\eta = 1$ nehmen kann) jedenfalls eine Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. μ) ein Primideal $\mathfrak{p}$ bilden; Primideale, welche aus den sämmtlichen Wurzeln einer solchen Congruenz bestehen, wollen wir vorläufig *einfache* Ideale nennen. Ist nun r irgend ein ganzer rationaler, nicht negativer Exponent, so bilden alle Wurzeln ϱ der Congruenz $\varrho\nu^r \equiv 0$ (mod. μ^r) ein Ideal, welches die $r$te *Potenz* von $\mathfrak{p}$ heissen und mit $\mathfrak{p}^r$ bezeichnet werden soll. Diese Definition ist unabhängig von dem zur Definition von $\mathfrak{p}$ benutzten Zahlenpaar μ, ν; ist nämlich μ' irgend eine von Null verschiedene, durch $\mathfrak{p}$ theilbare Zahl, also $\nu\mu' = \mu\nu'$, so folgt aus $\varrho\nu^r \equiv 0$ (mod. μ^r) durch Multiplication mit μ'^r und Division durch μ^r auch $\varrho\nu'^r \equiv 0$ (mod. μ'^r), und umgekehrt. Von der grössten Wichtigkeit sind aber die folgenden Sätze über einfache Ideale $\mathfrak{p}$:

Ist $s \geqq r$, so ist $\mathfrak{p}^s$ theilbar durch $\mathfrak{p}^r$. Ist nämlich σ in $\mathfrak{p}^s$ enthalten, also $\sigma\nu^s = \tau\mu^s$, so folgt, dass

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^r\sigma^{s-r}$$

eine ganze Zahl ist; mithin ist (nach §. 160, 3.) der jedenfalls dem Körper Ω angehörige Quotient $\sigma\nu^r : \mu^r$ ebenfalls eine *ganze* Zahl, also in $\mathfrak{o}$ enthalten, weil $\mathfrak{o}$ *alle* ganzen Zahlen des Körpers Ω umfasst*); also ist jede Zahl σ des Ideals $\mathfrak{p}^s$ auch in $\mathfrak{p}^r$ enthalten.

Ist ϱ eine von Null verschiedene Zahl in $\mathfrak{o}$, so giebt es immer eine höchste in ϱ aufgehende Potenz von $\mathfrak{p}$. Wäre nämlich für unendlich viele Exponenten r das Product $\varrho\nu^r$ theilbar durch μ^r, so müsste, da nur eine endliche Anzahl incongruenter Zahlen (mod. ϱ) existirt, für zwei *verschiedene* solche Exponenten r, s nothwendig einmal

$$\frac{\varrho\nu^r}{\mu^r} \equiv \frac{\varrho\nu^s}{\mu^s} \text{ (mod. } \varrho), \quad \left(\frac{\nu}{\mu}\right)^r = \left(\frac{\nu}{\mu}\right)^s + \omega$$

werden, wo ω eine ganze Zahl; hieraus würde aber (nach §. 160, 3.) folgen, dass ν durch μ theilbar wäre, was nicht der Fall ist, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre.

Sind $\mathfrak{p}^r$, $\mathfrak{p}^s$ resp. die höchsten in ϱ, σ aufgehenden Potenzen, so ist $\mathfrak{p}^{r+s}$ die höchste in $\varrho\sigma$ aufgehende Potenz von $\mathfrak{p}$. Denn da $\varrho\nu^r = \varrho'\mu^r$, $\sigma\nu^s = \sigma'\mu^s$, und keins der Producte $\nu\varrho'$, $\nu\sigma'$ durch μ theilbar ist, so folgt $\varrho\sigma\nu^{r+s} = \varrho'\sigma'\mu^{r+s}$, und $\nu\varrho'\sigma'$ kann nicht durch μ theilbar sein, weil $\mathfrak{p}$ ein Primideal ist.

Ist $e \geqq 1$ der Exponent der höchsten in μ selbst aufgehenden Potenz von $\mathfrak{p}$, also $\mu\nu^e = \varkappa\mu^e$, wo $\nu\varkappa$ *nicht* theilbar durch μ, so folgt $\nu^e = \varkappa\mu^{e-1}$, d. h. der Exponent der höchsten in ν aufgehenden Potenz von $\mathfrak{p}$ ist $= e-1$. Das Ideal $\mathfrak{p}^e$ besteht aus den sämmtlichen Wurzeln θ der Congruenz $\varkappa\theta \equiv 0$ (mod. μ). Die ganze Zahl $\lambda = \varkappa\mu : \nu = \sqrt[e]{\mu\varkappa^{e-1}}$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar; mithin ist λ^r durch $\mathfrak{p}^r$, aber nicht durch $\mathfrak{p}^{r+1}$ theilbar, woraus beiläufig folgt, dass die Ideale $\mathfrak{p}^r$ und $\mathfrak{p}^{r+1}$ wirklich *verschieden* sind. Endlich leuchtet folgender Satz ein:

Jede Potenz $\mathfrak{p}^r$ eines einfachen Ideals $\mathfrak{p}$ ist durch kein von $\mathfrak{p}$ verschiedenes Primideal theilbar. Ist nämlich π irgend eine Zahl in $\mathfrak{p}$, so muss ein in $\mathfrak{p}^r$ aufgehendes Primideal in π^r, also (zufolge 3.) in π selbst, d. h. in $\mathfrak{p}$ aufgehen und folglich mit $\mathfrak{p}$ identisch sein.

5. Die Wichtigkeit der einfachen Ideale und ihre Analogie mit den rationalen Primzahlen tritt unmittelbar hervor in dem folgenden Hauptsatz:

---

*) Sobald diese Bedingung nicht erfüllt ist, verlieren auch die obigen Sätze ihre *allgemeine* Gültigkeit; dies ist von Wichtigkeit für die Erweiterung der Definition der Ideale (vergl. §. 165, 4.).

Wenn alle in einer von Null verschiedenen Zahl μ aufgehenden Potenzen einfacher Ideale auch in einer Zahl η aufgehen, so ist η durch μ theilbar. Ist η *nicht* theilbar durch μ, so giebt es (zufolge 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein in μ aufgehendes einfaches Ideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in μ aufgehende Potenz, so ist (nach 4.) $\mathfrak{p}^{e-1}$ die höchste in ν aufgehende Potenz, und da ν durch η theilbar ist, so kann η *nicht* durch $\mathfrak{p}^e$ theilbar sein, was zu beweisen war. Derselbe Satz lässt sich offenbar auch so aussprechen: *Jedes Hauptideal* $\mathfrak{i}(\mu)$ *ist das kleinste gemeinschaftliche Multiplum aller in* μ *aufgehenden Potenzen von einfachen Idealen.* Es folgt zunächst:

Jedes Primideal $\mathfrak{p}$ *ist ein einfaches Ideal.* Es sei μ irgend eine von Null verschiedene Zahl in $\mathfrak{p}$, so muss $\mathfrak{p}$ (zufolge 3.) in einer der Potenzen einfacher Ideale aufgehen, deren kleinstes gemeinschaftliches Multiplum $\mathfrak{i}(\mu)$ ist; mithin ist $\mathfrak{p}$ selbst (zufolge 4.) ein einfaches Ideal. — Wir sprechen daher künftig nur noch von Primidealen, nicht mehr von einfachen Idealen.

Wenn alle in einem Ideal $\mathfrak{m}$ *aufgehenden Potenzen von Primidealen auch in einer Zahl η aufgehen, so ist η theilbar durch* $\mathfrak{m}$. Ist η *nicht* theilbar durch $\mathfrak{m}$, so giebt es (nach 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mathfrak{m}}$ ein Primideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in $\mathfrak{m}$ aufgehende Potenz von $\mathfrak{p}$, so giebt es in $\mathfrak{m}$ eine nicht durch $\mathfrak{p}^{e+1}$ theilbare Zahl μ, und das aus allen Wurzeln ϱ der Congruenz $\nu\varrho \equiv 0 \pmod{\mu}$ bestehende Ideal $\mathfrak{r}$ ist theilbar durch $\mathfrak{p}$, weil $\nu\varrho \equiv 0 \pmod{\mathfrak{m}}$ ist. Sind nun $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ die sämmtlichen höchsten in μ aufgehenden Potenzen verschiedener Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \ldots$, so besteht $\mathfrak{r}$ zufolge des obigen Hauptsatzes aus allen gemeinschaftlichen Wurzeln ϱ der Congruenzen $\nu\varrho \equiv 0 \pmod{\mathfrak{p}^e}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}'^{e'}}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}''^{e''}}$ u. s. w., d. h. $\mathfrak{r}$ ist das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}'' \ldots$, welche resp. aus den Wurzeln jeder einzelnen dieser Congruenzen bestehen; da nun die Ideale $\mathfrak{q}', \mathfrak{q}'' \ldots$ als Theiler von $\mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ nicht durch $\mathfrak{p}$ theilbar sind, so muss, weil $\mathfrak{r}$ durch $\mathfrak{p}$ theilbar ist, auch $\mathfrak{q}$ (zufolge 3.) durch $\mathfrak{p}$ theilbar sein; es kann folglich $\mathfrak{p}^e$ nicht in ν aufgehen (weil sonst $\mathfrak{q} = \mathfrak{o}$, also nicht durch $\mathfrak{p}$ theilbar wäre), und da ν durch η theilbar ist, so kann $\mathfrak{p}^e$ auch *nicht* in η aufgehen, was zu beweisen war.

Dieser *Fundamentalsatz* lässt sich offenbar auch so aussprechen: *Jedes Ideal ist das kleinste gemeinschaftliche Multiplum aller in ihm aufgehenden Potenzen von Primidealen.* Er entspricht durchaus

dem Fundamentalsatze der rationalen Zahlentheorie über die Zusammensetzung der Zahlen aus Primzahlen (§. 8); denn ihm zufolge ist jedes Ideal $\mathfrak{m}$ *vollständig bestimmt*, sobald die höchsten in $\mathfrak{m}$ aufgehenden Potenzen $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ... von Primidealen gegeben sind; aus ihm ergiebt sich auch ohne Weiteres der folgende Satz: *Ein Ideal* $\mathfrak{m}$ *ist stets und nur dann durch ein Ideal* $\mathfrak{b}$ *theilbar, wenn alle in* $\mathfrak{b}$ *aufgehenden Potenzen von Primidealen auch in* $\mathfrak{m}$ *aufgehen.* Dies folgt unmittelbar aus dem Begriffe des kleinsten gemeinschaftlichen Multiplums.

Ist $\mathfrak{m}$ *das kleinste gemeinschaftliche Multiplum von* $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ..., *wo* $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... *von einander verschiedene Primideale bedeuten, so ist* $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{p}')^{e'} N(\mathfrak{p}'')^{e''} \ldots$ Es giebt immer (zufolge 4.) eine durch $\mathfrak{p}^{e-1}$, aber nicht durch $\mathfrak{a} = \mathfrak{p}^e$ theilbare Zahl η; das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehende Ideal $\mathfrak{r}$ ist verschieden von $\mathfrak{o}$ (weil es die Zahl 1 nicht enthält) und ein Theiler von $\mathfrak{p}$ (zufolge 4.), folglich identisch mit $\mathfrak{p}$; da ferner der grösste gemeinschaftliche Theiler $\mathfrak{d}$ der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{i}(\eta)$ zufolge des eben bewiesenen Fundamentalsatzes $= \mathfrak{p}^{e-1}$ ist, so folgt (aus 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$, d. h. $N(\mathfrak{p}^e) = N(\mathfrak{p})N(\mathfrak{p}^{e-1})$, und hieraus allgemein $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. — Nun ist (zufolge der Definition 2.) das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ... zugleich auch das der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{b}$, wo $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ... bedeutet; da ferner (zufolge des Fundamentalsatzes) $\mathfrak{o}$ der grösste gemeinschaftliche Theiler von $\mathfrak{a}$ und $\mathfrak{b}$ ist, so folgt (aus 2.) $N(\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{b})$, d. h. $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{b})$ und hieraus ergiebt sich offenbar der zu beweisende Satz.

6. Multiplicirt man alle Zahlen eines Ideals $\mathfrak{a}$ mit allen Zahlen eines Ideals $\mathfrak{b}$, so bilden diese Producte und deren Summen ein durch $\mathfrak{a}$ und $\mathfrak{b}$ theilbares Ideal, welches das *Product aus den Factoren* $\mathfrak{a}$ *und* $\mathfrak{b}$ heissen und mit $\mathfrak{ab}$ bezeichnet werden soll. Aus dieser Erklärung leuchtet sofort ein, dass $\mathfrak{ao} = \mathfrak{a}$, $\mathfrak{ab} = \mathfrak{ba}$, ferner $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ ist (vergl. §§. 1, 2, 147). Zugleich gilt folgender Satz:

Sind $\mathfrak{p}^a$, $\mathfrak{p}^b$ *resp. die höchsten in* $\mathfrak{a}$, $\mathfrak{b}$ *aufgehenden Potenzen des Primideals* $\mathfrak{p}$, *so ist* $\mathfrak{p}^{a+b}$ *die höchste in* $\mathfrak{ab}$ *aufgehende Potenz von* $\mathfrak{p}$; *und es ist* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Aus der Erklärung folgt nämlich unmittelbar (mit Rücksicht auf 4.), dass $\mathfrak{ab}$ durch $\mathfrak{p}^{a+b}$ theilbar ist; da ferner in $\mathfrak{a}$ eine durch $\mathfrak{p}^{a+1}$ nicht theilbare Zahl α, in $\mathfrak{b}$ eine durch $\mathfrak{p}^{b+1}$ nicht theilbare

Zahl β existirt, so giebt es in $\mathfrak{a}\mathfrak{b}$ eine durch $\mathfrak{p}^{a+b+1}$ nicht theilbare Zahl $\alpha\beta$, womit der erste Theil des Satzes bewiesen ist. Ist also $\mathfrak{a}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$ ... der von einander verschiedenen Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ..., und $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^b$, $\mathfrak{p}'^{b'}$, $\mathfrak{p}''^{b''}$..., so ist $\mathfrak{a}\mathfrak{b}$ dasjenige der Potenzen $\mathfrak{p}^{a+b}$, $\mathfrak{p}'^{a'+b'}$, $\mathfrak{p}''^{a''+b''}$..., woraus (mit Rücksicht auf 5.) auch der zweite Theil des Satzes folgt.

Da aus diesem Satze auch $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$ folgt, so ist die oben (in 4.) gewählte Ausdrucks- und Bezeichnungsweise gerechtfertigt. Sind ferner $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... von einander verschiedene Primideale, so ist $\mathfrak{p}^a\mathfrak{p}'^{a'}\mathfrak{p}''^{a''}$ ... das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$ ... Auch leuchtet ein, dass der Begriff der Potenz durch die Definition $\mathfrak{a}^{r+1} = \mathfrak{a}\mathfrak{a}^r$ auf jedes Ideal $\mathfrak{a}$ ausgedehnt werden kann. Ist endlich $\mathfrak{a}$ *theilbar* durch $\mathfrak{b}$, so giebt es immer ein und nur ein Ideal $\mathfrak{r}$ der Art, dass $\mathfrak{a} = \mathfrak{r}\mathfrak{b}$ wird; sind nämlich $\mathfrak{p}^a$, $\mathfrak{p}^d$ die höchsten resp. in $\mathfrak{a}$, $\mathfrak{b}$ aufgehenden Potenzen eines Primideals $\mathfrak{p}$, so ist $d \leqq a$, und $\mathfrak{r}$ ist das Product aus allen Potenzen $\mathfrak{p}^{a-d}$. Mit Rücksicht hierauf erkennt man leicht, dass die früheren Sätze (in 2.) sich jetzt einfacher aussprechen lassen.

7. Wir nennen nun $\mathfrak{a}$ und $\mathfrak{b}$ *relative Primideale*, wenn ihr grösster gemeinschaftlicher Theiler $= \mathfrak{o}$ ist; ebenso soll η *relative Primzahl zum Ideal* $\mathfrak{a}$ heissen, wenn $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ relative Primideale sind. Es leuchtet dann ein, dass die Sätze der rationalen Zahlentheorie über relative Primzahlen sich leicht auf die Theorie der Ideale übertragen lassen; wir begnügen uns aber hier, folgenden wichtigen Satz zu beweisen (vergl. §. 25):

Sind $\mathfrak{a}$, $\mathfrak{b}$ *relative Primideale, und* μ, ν *zwei gegebene Zahlen, so giebt es immer eine und nur eine Classe von Zahlen* η *(mod.* $\mathfrak{a}\mathfrak{b}$*), welche den Bedingungen* $\eta \equiv \mu$ *(mod.* $\mathfrak{a}$*),* $\eta \equiv \nu$ *(mod.* $\mathfrak{b}$*) genügen.* Durchlaufen nämlich μ, ν, η vollständige Restsysteme resp. für die drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, so entspricht jeder Zahl η eine und nur eine Combination μ, ν der Art, dass $\mu \equiv \eta$ (mod. $\mathfrak{a}$), $\nu \equiv \eta$ (mod. $\mathfrak{b}$) ist; entspräche ferner zwei verschiedenen Zahlen η, η' des Restsystems für den Modul $\mathfrak{a}\mathfrak{b}$ eine und dieselbe Combination μ, ν, so wäre $\eta - \eta'$ theilbar sowohl durch $\mathfrak{a}$ als durch $\mathfrak{b}$, also auch durch $\mathfrak{a}\mathfrak{b}$ (weil $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind), mithin wäre $\eta \equiv \eta'$ (mod. $\mathfrak{a}\mathfrak{b}$), was gegen die Voraussetzung streitet. Durchläuft daher η alle seine Werthe, deren Anzahl $= N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ ist, so entstehen ebensoviele *verschiedene* Combinationen μ, ν; und da genau ebensoviele ver-

schiedene Combinationen μ, ν wirklich existiren, so muss auch umgekehrt jede Combination μ, ν einer Zahl η entsprechen, was zu beweisen war.

Bedeutet $\psi(\mathfrak{a})$ die Anzahl der (mod. $\mathfrak{a}$) incongruenten relativen Primzahlen zu $\mathfrak{a}$, so ist $\psi(\mathfrak{ab}) = \psi(\mathfrak{a})\,\psi(\mathfrak{b})$, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten. Ist ferner $\mathfrak{p}$ ein Primideal, und $e \geqq 1$, so ist $\psi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}) = N(\mathfrak{p})^{e-1}(N(\mathfrak{p}) - 1)$; denn, wenn δ alle r durch $\mathfrak{p}$ theilbaren und nach dem Modul $\mathfrak{p}^e$ incongruenten Zahlen, wenn ferner γ ein vollständiges Restsystem (mod. $\mathfrak{p}$) durchläuft, so bilden die Zahlen $\gamma + \delta$ (zufolge 2.) ein vollständiges Restsystem (mod. $\mathfrak{p}^e$), und es ist $N(\mathfrak{p}^e) = rN(\mathfrak{p})$, also $r = N(\mathfrak{p}^{e-1})$; nun ist aber eine solche Zahl $\gamma + \delta$ stets und nur dann relative Primzahl zu $\mathfrak{p}^e$, wenn γ nicht $\equiv 0$ (mod. $\mathfrak{p}$) ist, und folglich ist die Anzahl der Zahlen $\gamma + \delta$, welche relative Primzahlen zu $\mathfrak{p}^e$ sind, gleich $r(N(\mathfrak{p}) - 1)$, was zu beweisen war.

Bedeutet $\mathfrak{p}$ ein Primideal, so giebt es (zufolge 4.) immer eine Zahl λ, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar ist, mithin auch eine Zahl λ^e, welche durch $\mathfrak{p}^e$, aber nicht durch $\mathfrak{p}^{e+1}$ theilbar ist. Sind nun $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... von einander verschiedene Primideale, und haben λ', λ'' ... ähnliche Bedeutung für $\mathfrak{p}'$, $\mathfrak{p}''$ ..., wie λ für $\mathfrak{p}$, so existirt immer, wenn e, e', e'' ... gegebene Exponenten bedeuten, eine Zahl η, welche den gleichzeitigen Congruenzen

$$\eta \equiv \lambda^e \pmod{\mathfrak{p}^{e+1}}, \quad \eta \equiv \lambda'^{e'} \pmod{\mathfrak{p}'^{e'+1}},$$
$$\eta \equiv \lambda''^{e''} \pmod{\mathfrak{p}''^{e''+1}} \ldots$$

genügt, weil die Moduln relative Primideale sind. Dann ist offenbar $\mathfrak{i}(\eta) = \mathfrak{m}\mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''} \ldots$, und das Ideal $\mathfrak{m}$ ist durch keines der Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ theilbar. Hieraus folgt unmittelbar der Satz:

Sind $\mathfrak{a}$, $\mathfrak{b}$ *zwei beliebige Ideale, so giebt es immer ein solches relatives Primideal* $\mathfrak{m}$ *zu* $\mathfrak{b}$, *dass* $\mathfrak{am}$ *ein Hauptideal wird.* Sind nämlich $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... alle von einander verschiedenen in $\mathfrak{ab}$ aufgehenden Primideale, und ist $\mathfrak{a} = \mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''} \ldots$ (wo die Exponenten $e, e', e'' \ldots$ auch $= 0$ sein können), so giebt es, wie eben gezeigt ist, ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{i}(\eta) = \mathfrak{am}$ der Art, dass $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale sind.

Hieraus folgt auch, dass jedes Ideal $\mathfrak{a}$, welches kein Hauptideal ist, immer als der grösste gemeinschaftliche Theiler von *zwei* Hauptidealen angesehen werden kann; hat man nämlich nach Belieben ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{i}(\eta') = \mathfrak{ab}$ gewählt, so kann man immer ein zweites $\mathfrak{i}(\eta) = \mathfrak{am}$ so wählen, dass $\mathfrak{b}$ und $\mathfrak{m}$ re-