Zur Prüferschen Theorie der idealen Zahlen.

Von J. v. NEUMANN in Budapest.

ERSTE MITTEILUNG.

Einleitung.

Mit Hilfe der von Herrn PRÜFER[1]) eingeführten sogenannten „idealen Zahlen" können die Teilbarkeitsverhältnisse in einem algebraischen Körper ebensogut untersucht werden, wie mit den DEDEKINDschen Idealen; sie haben aber diesen gegenüber den Vorteil, einen Ring zu bilden: d. h. es ist für sie ausser der Multiplication und einer Division auch die Addition und Subtraktion definiert. Dabei entspricht auch jeder wirklichen algebraischen Zahl eine besondere ideale Zahl, und nicht (wie bei den Idealen) bloss jeder Klasse assoziierter algebraischer Zahlen. Jedem DEDEKINDschen Ideal entspricht eine Klasse assoziierter idealer Zahlen, aber nicht umgekehrt. (Was unter diesem „Entsprechen" gemeint ist, soll später präzisiert werden.)

Das System der idealen Zahlen ist nämlich wesentlich grösser, als das der Ideale: auch wenn wir von der idealen Zahl 0 und von den Nullteilern absehen (diesen können ja offenbar keine Ideale entsprechen), gibt es noch immer ideale Zahlen, denen keine Ideale entsprechen. PRÜFER bezeichnet die letzteren als unendliche ideale Zahlen, und die übrigen (ausser der 0 und den Nullteilern) als endliche ideale Zahlen.

Für die endlichen Zahlen beweist PRÜFER (entsprechend dem analogen Satze für Ideale) den Satz von der eindeutigen Zerlegbarkeit in Primfaktoren. Die DEDEKINDsche Theorie der Ideale wird

[1]) H. PRÜFER: Neue Begründung der algebraischen Zahlentheorie, Math. Ann., Bd. 94 (1925), Seite 198—243.

von PRÜFER nicht benützt, er zeigt im Gegenteil, wie diese aus seiner Theorie gewonnen werden kann. Ihre wesentlichsten Grundtatsachen beweist er aber am Anfang der Arbeit als „Sätze über Moduln", da ohne dieselben die Untersuchung der idealen Zahlen unmöglich ist.

Der erste Teil der vorliegenden Arbeit soll die PRÜFERschen Resultate aus einem anderen Gesichtspunkte beleuchten. PRÜFER führt die idealen Zahlen als „ideale Lösungen" unendlicher Congruenzsysteme ein; wir werden durch ein Verfahren zu ihnen gelangen, das der CANTORschen Einführung der reellen Zahlen und noch mehr der KÜRSCHÁKschen[2]) resp. BAUERschen[3]) Einführung der von HENSEL geschaffenen rationalen und algebraischen p-adischen Zahlen analog ist.

Die Resultate PRÜFERS über die Struktur der idealen Zahlen werden so auf anderem Wege gewonnen. In einer Richtung gelangen wir sogar noch weiter: wir beschränken uns nämlich bei der Untersuchung der multiplikativen Zerlegung nicht auf die endlichen idealen Zahlen, und wir gewinnen dabei den Satz von der eindeutigen Möglichkeit dieser Zerlegung in einer wesentlich allgemeineren Form. Es zeigt sich nämlich, dass alle idealen Zahlen (nicht nur die endlichen und unendlichen, sondern auch die Nullteiler und die 0) als Produkte von Primfaktoren dargestellt werden können. Die endlichen idealen Zahlen unterscheiden sich nur dadurch von den übrigen, dass man dabei mit einer endlichen Anzahl von Faktoren auskommt. Wenn unendlich viele Primfaktoren auftreten, so ist die Zahl unendlich; wenn sogar ein und derselbe Primfaktor unendlich oft auftritt, so ist sie ein Nullteiler; und wenn alle Primfaktoren vorkommen, und alle unendlich oft, so ist sie die Null.

Damit das Wesentliche unserer Gedankengänge besser hervortrete, setzen wir die DEDEKINDsche Theorie der Ideale durchweg als bekannt voraus.

Während sich die Untersuchungen des ersten Teiles (ebenso wie die PRÜFERschen) immer auf algebraische Zahlen eines (durch

[2]) J. KÜRSCHÁK: Über Limesbildung und allgemeine Körpertheorie, Journal für Math., Bd. 142 (1913). Die p-adischen rationalen Zahlen behandeln §§ 19—23, Seite 229—232.

[3]) M. BAUER: Die Theorie der p-adischen bzw. $\mathfrak{P}$-adischen Zahlen, und die gewöhnlichen algebraischen Zahlkörper, Math. Zeitschrift, Bd. 14 (1922), Seite 244—249.

die Zahl ϑ erzeugten) Körpers $K(\vartheta)$ beziehen, wird im zweiten Teile die Übertragung der Theorie auf den Körper *aller* algebraischen Zahlen versucht.

Hier sind wir auf das Verfahren von PRÜFER (unendliche Congruenzsysteme) angewiesen. Das im ersten Teile benützte Verfahren versagt; und zwar im wesentlichen darum, weil es keine Primideale (genauer: Primidealpotenzen) im Körper aller algebraischen Zahlen gibt. Die Primidealpotenzen müssen vielmehr durch den komplizierteren Begriff der „Idealfolgen" ersetzt werden, der von Herrn M. BAUER[4]) aufgestellt wurde. Und während es in einem Körper $K(\vartheta)$ bloss abzählbar viele Primidealpotenzen gibt, gibt es, wie wir zeigen werden, kontinuum-viele BAUERsche Idealfolgen.

Die hier herrschenden Verhältnisse charakterisiert der folgende (im zweiten Teile zu beweisende) Satz:

Jedes DEDEKINDsche Ideal kann in einem geeignet gewählten Körper in beliebig viele, paarweise relativ-prime und von der Einheit verschiedene, Idealfaktoren zerlegt werden.

Dies gilt natürlich nur im Körper *aller* algebraischen Zahlen, wenn hier *alle* DEDEKINDschen Ideale zulassen; in einem Körper $K(\vartheta)$ gilt, wie aus der Zerlegbarkeit in Primfaktoren folgt, das Gegenteil.

ERSTER TEIL.

I. Bezeichnungen.

Sei ϑ eine algebraische Zahl, die im Folgenden als fest gegeben angenommen wird; l sei der Grad von ϑ, $K = K(\vartheta)$ der durch ϑ bestimmte Körper, d. h. die Menge aller Zahlen

$$r_0 \cdot \vartheta^{l-1} + r_1 \cdot \vartheta^{l-2} + \ldots + r_{l-2} \cdot \vartheta + r_{l-1}$$

wo $r_0, r_1, \ldots, r_{l-2}, r_{l-1}$ alle rationalen Zahlen durchlaufen. Die zu $K(\vartheta)$ gehörenden Zahlen nennen wir *reale Zahlen* (im Gegensatze zu dem später zu definierenden idealen Zahlen).

Wir werden die folgenden Bezeichnungen anwenden: ganze rationale Zahlen bezeichnen wir mit dem Buchstaben $m, n, \ldots$;

[4]) M. BAUER: Über die Erweiterung des Körpers der p-adischen Zahlen zu einem algebraisch abgeschlossenen Körper, Math. Zeitschrift, Bd. 19 (1924), Seite 308–312. Auf die zitierten Arbeiten wurde ich durch Herrn Professor J. KÜRSCHÁK aufmerksam gemacht, und so zu meinen Untersuchungen angeregt.

reale Zahlen mit $\alpha, \beta, \ldots$ oder $\xi, \eta, \ldots$ Ideale des Körpers K bezeichnen wir mit $\mathfrak{a}, \mathfrak{b}, \ldots$; Primideale mit $\mathfrak{p}, \mathfrak{q}, \ldots$; Folgen realer Zahlen bezeichnen wir mit $R, S, \ldots$; die (später zu definierenden) idealen Zahlen mit $\mathfrak{A}, \mathfrak{B} \ldots$

Unter $\alpha \mid \beta$, bzw. $\mathfrak{a} \mid \beta$, bzw. $\mathfrak{a} \mid \mathfrak{b}$ verstehen wir, (wie es allgemein üblich ist) dass die Zahl $\frac{\beta}{\alpha}$ algebraisch ganz ist, bzw. dass die Zahl β zum Ideal $\mathfrak{a}$ gehört, bzw. dass das Ideal $\frac{\mathfrak{b}}{\mathfrak{a}}$ ganz ist. Dasjenige Ideal, welches der grösste gemeinsame Teiler der realen Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_m$ ist, bezeichnen wir mit $(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

II. Grundlegende Definitionen.

Definition 1. α sei eine reale Zahl, m eine ganze rationale Zahl, $\mathfrak{p}$ ein Primideal. Wir sagen, dass α *den Faktor* $\mathfrak{p}^m$ *enthält* (oder *hat*) wenn es eine durch $\mathfrak{p}$ nicht teilbare (reale) algebraisch ganze Zahl ξ gibt, sodass $\alpha\xi$ durch $\mathfrak{p}^m$ teilbar ist.[5])

Wenn $\alpha \neq 0$ ist, so liesse sich diese Definition offenbar auch so fassen: wir bringen das Ideal (α) auf die Form

$$\mathfrak{p}^m \cdot \mathfrak{p}_1^{m_1} \cdot \mathfrak{p}_2^{m_2} \ldots \mathfrak{p}_r^{m_r}$$

($\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ sind von $\mathfrak{p}$ und voneinander verschiedene Primideale, m und $m_1, m_2, \ldots, m_r$ gleich $0, \pm 1, \pm 2, \ldots$); α enthält den Faktor $\mathfrak{p}^n$ dann und nur dann, wenn $n \leqq m$ ist. Gelegentlich ist diese Fassung der Definition die besser verwendbare.

Satz 1. Wenn α den Faktor $\mathfrak{p}^m$ hat, und $n \leqq m$ ist, so hat es auch den Faktor $\mathfrak{p}^n$.

Wenn α den Faktor $\mathfrak{p}^m$ hat, und $\alpha \mid \beta$ ist, so hat auch β den Faktor $\mathfrak{p}^m$.

---

[5]) Dieser Begriff des „Enthaltens eines Faktors", der im wesentlichen schon bei HENSEL eine fundamentale Rolle spielt, wird uns gestatten sämmtliche ideale Zahlen auf einmal einzuführen, wärend PRÜFER vorerst nur die ganzen idealen Zahlen definiert und die gebrochenen idealen Zahlen sodann durch formale Division einführt.

Es ist vielleicht nicht überflüssig zu bemerken, dass trotz $\mathfrak{p}^0 = \mathfrak{q}^0$ ($\mathfrak{p}, \mathfrak{q}$ zwei verschiedene Primideale) es etwas anderes ist, den Factor $\mathfrak{p}^0$ zu enthalten, als den Factor $\mathfrak{q}^0$ zu enthalten. Wenn z. B. α eine zu $\frac{(1)}{\mathfrak{q}}$ aber nicht zu (1) gehörige reale Zahl ist, so hat α wohl den Factor $\mathfrak{p}^0$, aber nicht den Factor $\mathfrak{q}^0$.

Wenn α und β den Faktor $\mathfrak{p}^m$ haben, so hat auch $\alpha \pm \beta$ den Faktor $\mathfrak{p}^m$.

Wenn α den Faktor $\mathfrak{p}^m$ und β den Faktor $\mathfrak{p}^n$ hat, so hat $\alpha\beta$ den Faktor $\mathfrak{p}^{m+n}$.

Wenn $\mathfrak{p}^m \mid \alpha$ ist, so hat α den Faktor $\mathfrak{p}^m$. Wenn α algebraisch ganz ist, so gilt auch die Umkehrung.

Wenn $\alpha\beta$ den Faktor $\mathfrak{p}^{m+n}$ hat, und β den Faktor $\mathfrak{p}^{n+1}$ nicht hat, so enthält α den Faktor $\mathfrak{p}^m$.

Beweis: Klar.

Definition 2. $R = [\alpha_1, \alpha_2, \ldots]$ sei eine Folge realer Zahlen. Wir nennen R eine *Fundamentalfolge* wenn für jedes $\mathfrak{p}$ und m fast alle[6]) Differenzen $\alpha_r \quad \alpha_{r+1}$ den Faktor $\mathfrak{p}^m$ enthalten.

Definition 3. $R = [\alpha_1, \alpha_2, \ldots]$ und $S = [\beta_1, \beta_2, \ldots]$ seien Folgen realer Zahlen. Wir nennen R und S *äquivalent*, in Zeichen: $R \sim S$, wenn für jedes $\mathfrak{p}$ und m fast alle Differenzen $\alpha_r - \beta_r$ den Faktor $\mathfrak{p}^m$ enthalten.

Satz 2. Es ist stets $R \sim R$.

Aus $R \sim S$ folgt $S \sim R$.

Aus $R \sim S$ und $S \sim T$ folgt $R \sim T$.

Beweis: Klar.

Infolge des Satzes 2. zerfällt die Menge der Folgen realer Zahlen in paarweise elementefremde Klassen untereinander äquivelenter Folgen. D. h.: eine Folge R gehört zu einer und nur einer Klasse, und diese umfasst alle mit R äquivalenten Folgen.

Satz 3. Wenn $R \sim S$ ist, so sind entweder beide Folgen R, S fundamental, oder keine von ihnen.

Beweis: Klar.

Aus Satz 3 folgt, dass jede unserer Aequivalenzklassen entweder lauter Fundamentalfolgen enthält, oder keine einzige.

Definition 4. Eine Aequivalenzklasse, die lauter Fundamentalfolgen enthält, nennen wir eine *ideale Zahl.*[7])

Definition 5. Wenn die Fundamentalfolge R zur Aequivalenzklasse (idealen Zahl) $\mathfrak{A}$ gehört, so sagen wir, $\mathfrak{A}$ und R gehören zu einander, in Zeichen: $\mathfrak{A} \sim R$.

---

[6]) Unter „gültig für fast alle r" verstehen wir (wie es allgemein üblich ist): „gültig für alle r mit höchstens endlich vielen Ausnahmen."

[7]) Wir definieren die ideale Zahl als die aus den zu ihr gehörigen Fundamentalfolgen gebildete Menge selbst; natürlich könnte man sie auch als ein dieser Menge zugeordnetes ideales Element betrachten.

Satz 4. Jede Fundamentalfolge R gehört zu einer einzigen idealen Zahl, und zu jeder idealen Zahl $\mathfrak{A}$ gehören (unendlich viele) Fundamentalfolgen.
Beweis: Klar.

Satz 5. Aus $\mathfrak{A} \sim R, R \sim S$ folgt $\mathfrak{A} \sim S$; aus $\mathfrak{A} \sim R, \mathfrak{A} \sim S$ folgt $R \sim S$; aus $\mathfrak{A} \sim R, \mathfrak{B} \sim R$ folgt $\mathfrak{A} = \mathfrak{B}$.
Beweis: Klar.

Wir bemerken noch:

Satz 6. Wenn R eine Fundamentalfolge ist, und S eine Teilfolge von R, mit beliebiger Reihenfolge der Elemente, so ist auch S fundamental, und es ist $R \sim S$.

Beweis: Nach Satz 3. genügt es die zweite Behauptung zu beweisen. Es sei also $R = [\alpha_1, \alpha_2, \ldots]$, $S = [\alpha_{m_1}, \alpha_{m_2}, \ldots]$; $\mathfrak{p}$ und m seien beliebig gegeben.

Wir wählen p so, dass aus $r \geqq p$ folgt, dass $\alpha_r - \alpha_{r+1}$ den Faktor $\mathfrak{p}^m$ hat. Da schliesst man sofort, dass für $r \geqq p$, $s \geqq p$ auch $\alpha_r - \alpha_s$ den Faktor $\mathfrak{p}^m$ hat.

Wir wählen weiter q so, dass aus $r \geqq q$ stets $n_r \geqq p$ folgt. Dann folgt aus $r \geqq \mathrm{Max}(p, q)$ offenbar $r \geqq p$, $n_r \geqq p$, also muss $\alpha_r - \alpha_{n_r}$ den Faktor $\mathfrak{p}^m$ enthalten. D. h. es ist $R \sim S$.

III. Grundoperationen.

Satz 7. Wenn die Folgen $R = [\alpha_1, \alpha_2, \ldots]$ und $S = [\beta_1, \beta_2, \ldots]$ fundamental sind, so sind es auch die Folgen $[\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots]$, $[\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots]$, $[\alpha_1 \beta_1, \alpha_2 \beta_2, \ldots]$.

Beweis: Für die Folgen $[\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots]$ und $[\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots]$ ist die Behauptung klar. Für die Folge $[\alpha_1 \beta_1, \alpha_2 \beta_2, \ldots]$ aber stellen wir die folgende Überlegung an:

$\mathfrak{p}$ sei ein Primideal, m ein ganz-rationaler Exponent. Da für fast alle r die Differenz $\alpha_r - \alpha_{r+1}$ den Faktor $\mathfrak{p}^0$ enthält, und ebenso für fast alle r die Differenz $\beta_r - \beta_{r+1}$ den Faktor $\mathfrak{p}^0$ enthält, so findet auch für fast alle r beides zugleich statt. Wir können also p so wählen, dass für $r \geqq p$ sowohl $\alpha_r - \alpha_{r+1}$ als auch $\beta_r - \beta_{r+1}$ den Faktor $\mathfrak{p}^0$ enthält. Wir nehmen ferner n so an, dass sowohl α_p als β_p den Faktor $\mathfrak{p}^n$ enthält. Dies ist leicht durchzuführen: wir bringen (α_p), (β_p) auf die Form

$$(\alpha_p) = \mathfrak{p}^s \cdot \mathfrak{p}_1^{s_1} \cdot \mathfrak{p}_2^{s_2} \ldots \mathfrak{p}_n^{s_n}, \quad (\beta_p) = \mathfrak{p}^t \cdot \mathfrak{p}_1^{t_1} \cdot \mathfrak{p}_2^{t_2} \ldots \mathfrak{p}_n^{t_n}$$

($\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ von $\mathfrak{p}$ und voneinander verschiedene Primideale)

und wählen $n \leqq \text{Min } (s, t)$. (Wenn α_p oder $\beta_p = 0$ ist, so versagt zwar dieses Verfahren, dann sind wir aber in der Wahl von s bzw. t ganz frei.) Setzen wir insbesondere $n = \text{Min. } (0, s, t)$, so haben α_p, β_p den Faktor $\mathfrak{p}^n$, und auch jedes $\alpha_r - \alpha_{r+1}, \beta_r - \beta_{r+1}$ für $r \geqq p$. Also haben alle α_r, β_r für $r \geqq p$ diesen Faktor.

Für fast alle r enthält $\alpha_r - \alpha_{r+1}$ den Faktor $\mathfrak{p}^{m-n}$, und für fast alle r enthält $\beta_r - \beta_{r+1}$ denselben Faktor. Ferner sahen wir, dass für fast alle r α_r, β_{r+1} den Faktor $\mathfrak{p}^n$ enthalten (nämlich für $r \geqq p$). Für fast alle r gelten demnach alle drei Bedingungen zugleich.

Für diese r enthalten aber die Zahlen $\beta_{r+1}(\alpha_r - \alpha_{r+1})$ und $\alpha_r(\beta_r - \beta_{r+1})$ beide den Faktor $\mathfrak{p}^{(m-n)+n}$, d. h. $\mathfrak{p}^m$, also enthält ihn auch ihre Summe $\alpha_r\beta_r - \alpha_{r+1}\beta_{r+1}$.

Definition 6. Die im Satz 7. erwähnten Fundamentalfolgen bezeichnen wir bzw. mit $R+S$, $R-S$, RS.

Satz 8. Aus $R' \sim R'', S' \sim S''$ folgt $R'+S' \sim R''+S''$, $R'-S' \sim R''-S''$, $R'S' \sim R''S''$.

Beweis: Es sei

$$R' = [\alpha_1', \alpha_2', \ldots], \; S' = [\beta_1', \beta_2', \ldots],$$
$$R'' = [\alpha_1'', \alpha_2'', \ldots], \; S'' = [\beta_1'', \beta_2'', \ldots].$$

Die Behauptungen

$$[\alpha_1', \alpha_2', \ldots] + [\beta_1', \beta_2', \ldots] \sim [\alpha_1'', \alpha_2'', \ldots] + [\beta_1'', \beta_2'', \ldots]$$
$$[\alpha_1', \alpha_2', \ldots] - [\beta_1', \beta_2', \ldots] \sim [\alpha_1'', \alpha_2'', \ldots] - [\beta_1'', \beta_2'', \ldots]$$

sind offenbar trivial. Es bleibt nur übrig

$$[\alpha_1', \alpha_2', \ldots] \cdot [\beta_1', \beta_2', \ldots] \sim [\alpha_1'', \alpha_2'', \ldots] \cdot [\beta_1'', \beta_2'', \ldots]$$

zu beweisen.

Es sei also $\mathfrak{p}$ und m gegeben. Wir wählen n, p so, dass so oft $r \geqq p$ ist, α_r' und β_r'' den Faktor $\mathfrak{p}^n$ immer enthalten. (Dass es solche n, p gibt, und wie sie zu konstruieren sind, wurde beim Beweise des Satzes 7. gezeigt.)

Da nun $R' \sim R''$ und $S' \sim S''$ ist, so enthalten fast alle $\alpha_r' - \alpha_r''$ sowie fast alle $\beta_r' - \beta_r''$ den Faktor $\mathfrak{p}^{m-n}$. Ausserdem sahen wir soeben, dass fast alle α_r' und fast alle β_r'' den Faktor $\mathfrak{p}^n$ enthalten. Also sind für fast alle r alle vier Bedingungen zugleich erfüllt. Wenn sie aber für ein r sämtlich erfüllt sind, so werden die beiden Produkte $\beta_r''(\alpha_r' - \beta_r')$, $\alpha_r'(\alpha_r'' - \beta_r'')$ den Faktor $\mathfrak{p}^{(m-n)+n}$, d. h. $\mathfrak{p}^m$ enthalten. Also enthält ihn auch ihre Summe $\alpha_r'\alpha_r'' - \beta_r'\beta_r''$.

Damit ist $R' \cdot S' \sim R'' \cdot S''$ bewiesen.

Wenn also $\mathfrak{A} \sim R, \mathfrak{B} \sim S$ ist, so hängen die bzw. zu $R+S$, $R-S$, $R.S$ gehörigen idealen Zahlen nur von $\mathfrak{A}, \mathfrak{B}$ (und nicht von R, S) ab.

Definition 7. Die soeben erwähnten idealen Zahlen bezeichnen wir bzw. mit $\mathfrak{A}+\mathfrak{B}$, $\mathfrak{A}-\mathfrak{B}$, $\mathfrak{A}.\mathfrak{B}$.

Satz 9. Für die durch Definition 7 beschriebene Addition, Subtraktion, und Multiplikation gelten die kommutativen, assoziativen, und distributiven Gesetze, und die Subtraktion ist die inverse Operation der Addition.

Beweis: Für reale Zahlen sind alle diese Gesetzte natürlich gültig. Hieraus folgen sie aber, mit Hilfe der Definition 6., sofort für Fundamentalfolgen; und mit Hilfe der Definition 7. für ideale Zahlen.

Satz 10. Die Folge $[\alpha, \alpha, \ldots]$ ist stets fundamental.

Beweis: Klar.

Definition 8. Die zur Folge $[\alpha, \alpha, \ldots]$ gehörende ideale Zahl bezeichnen wir mit $\overline{\alpha}$.

Satz 11. Es ist stets

$$\overline{\alpha}+\overline{\beta}=\overline{\alpha+\beta},\ \overline{\alpha}-\overline{\beta}=\overline{\alpha-\beta},\ \overline{\alpha}.\overline{\beta}=\overline{\alpha.\beta}.$$

Ferner ist

$$\mathfrak{A}+\overline{0}=\mathfrak{A}-\overline{0}=\mathfrak{A},\ \mathfrak{A}-\mathfrak{A}=\overline{0},\ \mathfrak{A}.\overline{1}=\mathfrak{A},\ \mathfrak{A}.\overline{0}=\overline{0}.$$

Beweis: Klar.

IV. Ganze ideale Zahlen und Teilbarkeit.

Definition 9. Wir nennen eine ideale Zahl $\mathfrak{A}$ *ganz*, wenn es unter den zu ihr gehörigen Fundamentalfolgen $[\alpha_1, \alpha_2 \ldots]$ mindestens eine solche gibt, bei der alle α_r algebraisch ganz sind.[8])

Satz 12. Wenn $\mathfrak{A}$, $\mathfrak{B}$ ganze ideale Zahlen sind, so sind auch die idealen Zahlen $\mathfrak{A}+\mathfrak{B}$, $\mathfrak{A}-\mathfrak{B}$, $\mathfrak{A}.\mathfrak{B}$ ganz.

Beweis: Klar.

Satz 13. $\overline{\alpha}$ ist dann und nur dann ganz, wenn α algebraisch ganz ist.

Beweis: Wenn α algebraisch ganz ist, so ist $\overline{\alpha}$ auch ganz, da $[\alpha, \alpha, \ldots]$ zu $\overline{\alpha}$ gehört. Wenn hingegen α nicht ganz ist, so schliessen wir folgendermassen:

[8]) Eine andere Fassung der Definition der ganzen idealen Zahl ist die folgende: $\mathfrak{A}$ ist ganz, wenn es alle Factoren $\mathfrak{p}^0$ enthält. Die Aequivalenz der beiden Definitionen wird im Satze 56. ausgesprochen.

Das Ideal

$$(\alpha) = \mathfrak{p}_1^{m_1} \cdot \mathfrak{p}_2^{m_2} \ldots \mathfrak{p}_n^{m_n}$$

($\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ sind voneinander verschiedene Primideale) ist auch nicht ganz, folglich ist mindestens einer der Exponenten $m_1, m_2, \ldots, m_n$ negativ. Es sei etwa $m_\nu < 0$. Dann hat α gewiss nicht den Faktor $\mathfrak{p}_\nu^0$.

Nun sei $\overline{\alpha} \sim [\alpha_1, \alpha_2, \ldots]$. Dann ist $[\alpha, \alpha, \ldots] \sim [\alpha_1, \alpha_2, \ldots]$ und also muss ein $\alpha - \alpha_r$ den Faktor $\mathfrak{p}_\nu^0$ haben. Da α ihn nicht hat, so hat ihn auch α_r nicht. Also kann auch nicht $\mathfrak{p}_\nu^0 \mid \alpha_r$, d. h. $1 \mid \alpha_r$ sein. Folglich ist α_r nicht algebraisch ganz. Da das für alle zu $\overline{\alpha}$ gehörigen $[\alpha_1, \alpha_2, \ldots]$ gilt, kann auch $\overline{\alpha}$ nicht ganz sein.

Nachdem wir den Begriff der ganzen idealen Zahl definiert, haben, können wir zur Definition der Teilbarkeit bei idealen Zahlen übergehen.

Definition 10. Wenn es zu den zwei idealen Zahlen $\mathfrak{A}, \mathfrak{B}$ eine ganze ideale Zahl $\mathfrak{C}$ gibt, sodass $\mathfrak{B} = \mathfrak{A} \cdot \mathfrak{C}$ ist, so sagen wir, dass $\mathfrak{B}$ *durch* $\mathfrak{A}$ *teilbar ist*, in Zeichen $\mathfrak{A} \mid \mathfrak{B}$.

Satz 14. Aus $\mathfrak{A} \mid \mathfrak{B}$, $\mathfrak{B} \mid \mathfrak{C}$ folgt $\mathfrak{A} \mid \mathfrak{C}$.

Aus $\mathfrak{A} \mid \mathfrak{B}_1$, $\mathfrak{A} \mid \mathfrak{B}_2$ folgt $\mathfrak{A} \mid \mathfrak{B}_1 \pm \mathfrak{B}_2$.

Es ist stets $\mathfrak{A} \mid \overline{0}$ und $\mathfrak{A} \mid \mathfrak{A}$. $\overline{1} \mid \mathfrak{A}$ ist damit gleichbedeutend, dass $\mathfrak{A}$ ganz ist.

Beweis: Klar.

Satz 15. $\overline{\alpha} \mid \overline{\beta}$ ist mit $\alpha \mid \beta$ (im Sinne der gewöhnlichen Teilbarkeit) gleichbedeutend.

Beweis: Aus $\alpha \mid \beta$ folgt: $\frac{\beta}{\alpha}$ ganz, also auch $\overline{\left(\frac{\beta}{\alpha}\right)}$ ganz, und wegen $\overline{\alpha} \cdot \overline{\left(\frac{\beta}{\alpha}\right)} = \overline{\left(\alpha \cdot \frac{\beta}{\alpha}\right)} = \overline{\beta}$ ist dann $\overline{\alpha} \mid \overline{\beta}$.

Aus $\overline{\alpha} \mid \overline{\beta}$ hingegen folgt: $\overline{\alpha} \cdot \mathfrak{C} = \overline{\beta}$, wobei $\mathfrak{C}$ ganz ist, also $\mathfrak{C} \sim [\gamma_1, \gamma_2, \ldots]$ mit lauter algebraisch ganzen γ_r ist. Folglich ist:

$$\overline{\alpha} \cdot \mathfrak{C} \sim [\alpha, \alpha, \ldots] \cdot [\gamma_1, \gamma_2, \ldots] = [\alpha\gamma_1, \alpha\gamma_2, \ldots]$$
$$\overline{\beta} \sim [\beta, \beta, \ldots]$$
$$[\alpha\gamma_1, \alpha\gamma_2, \ldots] \sim [\beta, \beta, \ldots]$$

Wenn α den Faktor $\mathfrak{p}^m$ hat, so haben ihn auch alle $\alpha\gamma_r$ (weil alle ganz sind); und da mindestens ein $\alpha\gamma_r - \beta$ auch diesen Faktor hat, so hat ihn auch β. Hieraus folgt aber $\alpha \mid \beta$, denn wenn wir α und β in der Form

$$(\alpha) = \mathfrak{p}_1^{s_1} \cdot \mathfrak{p}_2^{s_2} \ldots \mathfrak{p}_n^{s_n}, \quad (\beta) = \mathfrak{p}_1^{t_1} \cdot \mathfrak{p}_2^{t_2} \ldots \mathfrak{p}_n^{t_n}$$

($\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ voneinander verschiedene Primideale) schreiben, so sehen wir: α hat jeden der Faktoren $\mathfrak{p}_\nu^{s_\nu}$ also auch β; also muss stets $s_\nu \leqq t_\nu$ sein, folglich ist $\alpha \mid \beta$. (Eigentlich müssten die Fälle $\alpha = 0$ und $\beta = 0$ noch für sich erledigt werden. Im Falle $\beta = 0$ ist aber offenbar $\alpha \mid \beta$; und wenn $\alpha = 0$ ist, so muss auch $\beta = 0$ sein, was wieder $\alpha \mid \beta$ ergibt. Dass aus $\alpha = 0$, $\beta = 0$ folgt, sieht man folgendermassen ein: α enthält alle Faktoren $\mathfrak{p}^m$, wäre nun $\beta \neq 0$, so hätte (β) die Form $\mathfrak{p}_1^{t_1} \cdot \mathfrak{p}_2^{t_2} \ldots \mathfrak{p}_n^{t_n}$ es enthielte also z. B. den Faktor $\mathfrak{p}_1^{t_1+1}$ nicht.)

Jetzt definieren wir noch für ideale Zahlen, das „Enthalten eines (Primidealpotenz-) Faktors".

Satz 16. Sein $R = [\alpha_1, \alpha_2, \ldots]$ und $S = [\beta_1, \beta_2, \ldots]$ Fundamentalfolgen, u. zw. sei $R \sim S$; $\mathfrak{p}$ bedeute ein Primideal. Unter diesen Voraussetzungen enthalten dann und nur dann fast alle α_r den Faktor $\mathfrak{p}^m$, wenn fast alle β_r denselben enthalten.

Beweis: Klar.

Also enthalten bei einer idealen Zahl $\mathfrak{A}$ entweder für jede zu $\mathfrak{A}$ gehörige Fundamentalfolge R fast alle α_r den Faktor $\mathfrak{p}^m$, oder für keine einzige solche Fundamentalfolge.

Definition 11. Wenn für jede zu $\mathfrak{A}$ gehörige Fundamentalfolge $R = [\alpha_1, \alpha_2, \ldots]$ fast alle α_r den Faktor $\mathfrak{p}^m$ enthalten, so sagen wir, $\mathfrak{A}$ *enthält den Faktor* $\mathfrak{p}^m$.[9])

Satz 17. Wenn $\mathfrak{A}$ den Faktor $\mathfrak{p}^m$ enthält und $n \leqq m$ ist, so enthält es auch den Faktor $\mathfrak{p}^n$.

Wenn $\mathfrak{A}$ den Faktor $\mathfrak{p}^m$ enthält, und $\mathfrak{A} \mid \mathfrak{B}$ ist, so enthält auch $\mathfrak{B}$ den Faktor $\mathfrak{p}^m$.

Wenn $\mathfrak{A}$ und $\mathfrak{B}$ den Faktor $\mathfrak{p}^m$ enthält, so enthält auch $\mathfrak{A} \pm \mathfrak{B}$ den Faktor $\mathfrak{p}^m$.

Wen $\mathfrak{A}$ den Faktor $\mathfrak{p}^m$ und $\mathfrak{B}$ den Faktor $\mathfrak{p}^n$ enthält, so enthält $\mathfrak{A} \cdot \mathfrak{B}$ den Faktor $\mathfrak{p}^{m+n}$.

Beweis: Klar.

Satz 18. $\overline{\alpha}$ enthält den Faktor $\mathfrak{p}^m$ dann und nur dann (im Sinne der Definition 11.) wenn ihn α enthält (im Sinne der Definition 1.).

Beweis: Klar.

[9]) Auch hier gilt die Bemerkung am Ende der Fussnote [5]).

Bemerkung.

Ehe wir weiter gehen, wollen wir noch eins feststellen.

In allen Operationen und Relationen, die wir sowohl für reale, als auch für ideale Zahlen definiert haben, u. zw. unter Benützung desselben Zeichens (das sind die Addition, Subtraktion, Multiplikation, Teilbarkeit, und das Enthalten eines Faktors p^m), spielt die reale Zahl α und die ideale Zahl $\overline{\alpha}$ genau dieselbe Rolle. (Vergl. die Sätze 11, 13, 15, 18.) Ausserdem gilt der folgende Satz:

Satz 19. $\overline{\alpha}=\overline{\beta}$ ist mit $\alpha=\beta$ gleichbedeutend.

Beweis: Aus $\alpha=\beta$ folgt jedenfalls $\overline{\alpha}=\overline{\beta}$. Ist umgekehrt $\overline{\alpha}=\overline{\beta}$, so ist

$$\overline{\alpha-\beta}=\overline{\alpha}-\overline{\beta}=\overline{0}$$

also gilt für jedes $\overline{\gamma}$ die Beziehung $\overline{\gamma}\,|\,\overline{\alpha-\beta}$, d. h. $\gamma\,|\,\alpha-\beta$. Folglich muss $\alpha-\beta=0$, $\alpha=\beta$ sein.

Es besteht demnach kein zwingender Grund α und $\overline{\alpha}$ voneinander zu unterscheiden; wir werden deshalb im Folgenden den Querstrich stets fortlassen, und die ideale Zahl $\overline{\alpha}$ kurz mit α bezeichnen.

V. Der Limes.

Definition 12. $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ und $\mathfrak{A}$ seien beliebige ideale Zahlen.

Wir sagen, dass die Folge $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ gegen $\mathfrak{A}$ *konvergiert*, in Zeichen: $\mathfrak{A}_r \to \mathfrak{A}$ für $r \to \infty$, wenn für jedes p und m fast alle $\mathfrak{A}-\mathfrak{A}_r$ den Faktor p^m enthalten.[10])

Satz 20. $\mathfrak{A}$ ist dann und nur dann $=0$, wenn es alle p^m als Faktoren enthält.

Beweis: Wegen $p^m\,|\,0$ enthält 0 alle p^m als Faktoren. Wenn umgekehrt $\mathfrak{A}$ alle p^m als Faktoren enthält, so sei $\mathfrak{A} \sim [\alpha_1, \alpha_2, \ldots]$. Dann ist jedes p^m in fast allen α_r, also in fast allen $\alpha_r - 0$ als Faktor enthalten. Also ist $[\alpha_1, \alpha_2, \ldots]$ mit $[0, 0, \ldots]$ äquivalent, also $\mathfrak{A} \sim [0, 0, \ldots]$. Wegen $0 \sim [0, 0, \ldots]$ muss demnach $\mathfrak{A}=0$ sein.

Satz 21. Wenn $\mathfrak{A}_r \to \mathfrak{A}$ und $\mathfrak{A}_r \to \mathfrak{B}$ für $r \to \infty$, so ist $\mathfrak{A}=\mathfrak{B}$.

---

[10]) Diese Definition des Limes ist im wesentlichen gleichbedeutend mit der PRÜFERschen Definition der Summe von unendlich vielen idealen Zahlen. Das Multiplizieren mit einem Generalnenner erübrigt sich hier infolge der Anwendung des Begriffes des „Faktor-Enthalten"-s.

Beweis: Für jedes $\mathfrak{p}$ und m muss es ein r geben, sodass sowohl $\mathfrak{A}-\mathfrak{A}_r$ als auch $\mathfrak{B}-\mathfrak{A}_r$ den Faktor $\mathfrak{p}^m$ enthält. Also enthält ihn auch $\mathfrak{A}-\mathfrak{B}=(\mathfrak{A}-\mathfrak{A}_r)-(\mathfrak{B}-\mathfrak{A}_r)$. Da dies für alle $\mathfrak{p}, m$ gilt, muss nach dem soeben bewiesenen Satze $\mathfrak{A}-\mathfrak{B}=0$, $\mathfrak{A}=\mathfrak{B}$ sein.

Definition 13. Wir nennen eine Folge $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ idealer Zahlen *konvergent*, wenn eine Zahl $\mathfrak{A}$ existiert, zu der sie konvergiert. In diesem Falle existiert aber auch nur eine solche Zahl (wegen Satz 21.), und diese bezeichnen wir mit $\lim\limits_{r\to\infty} \mathfrak{A}_r$.

Satz 22. Seien die Folgen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ und $\mathfrak{B}_1, \mathfrak{B}_2, \ldots$ beide konvergent. Dann sind auch die Folgen $\mathfrak{A}_1+\mathfrak{B}_1$, $\mathfrak{A}_2+\mathfrak{B}_2 \ldots$; $\mathfrak{A}_1-\mathfrak{B}_1$, $\mathfrak{A}_2-\mathfrak{B}_2, \ldots$; $\mathfrak{A}_1\mathfrak{B}_1$, $\mathfrak{A}_2\mathfrak{B}_2, \ldots$ konvergent.

Dabei gelten die Gleichungen

$$\lim_{r\to\infty}(\mathfrak{A}_r \pm \mathfrak{B}_r) = \lim_{r\to\infty}\mathfrak{A}_r + \lim_{r\to\infty}\mathfrak{B}_r$$

$$\lim_{r\to\infty}(\mathfrak{A}_r \quad \mathfrak{B}_r) = \lim_{r\to\infty}\mathfrak{A}_r \cdot \lim_{r\to\infty}\mathfrak{B}_r$$

Beweis: Wenn wir $\lim\limits_{r\to\infty}\mathfrak{A}_r$ und $\lim\limits_{r\to\infty}\mathfrak{B}_r$ mit $\mathfrak{A}$ bzw. $\mathfrak{B}$ bezeichnen, so müssen wir zeigen, dass aus $\mathfrak{A}_r \to \mathfrak{A}$ und $\mathfrak{B} \to \mathfrak{B}$ für $r\to\infty$ immer $(\mathfrak{A}_r \pm \mathfrak{B}_r)\to(\mathfrak{A}\pm\mathfrak{B})$ und $(\mathfrak{A}_r . \mathfrak{B}_r)\to(\mathfrak{A}.\mathfrak{B})$ für $r\to\infty$ folgt.

Die beiden ersten Behauptungen sind trivial; die letzte beweisen wir folgendermassen:

Das Primideal $\mathfrak{p}$ und der ganze rationale Exponent m seien beliebig gegeben. Es sei $\mathfrak{A}\sim[\alpha_1, \alpha_2, \ldots]$, $\mathfrak{B}\sim[\beta_1, \beta_2, \ldots]$. Es wurde beim Beweise des Satzes 8. gezeigt, dass es ein n gibt, sodass fast alle α_r und β_r den Faktor $\mathfrak{p}^n$ enthalten. Dann enthält auch $\mathfrak{A}$ und $\mathfrak{B}$ den Faktor $\mathfrak{p}^n$.

Ferner enthält für fast alle r die Differenz $\mathfrak{A}-\mathfrak{A}_s$ den Faktor $\mathfrak{p}^{m-n}$, und für fast alle r enthält die Differenz $\mathfrak{B}-\mathfrak{B}_r$ den Faktor $\mathfrak{p}^{\mathrm{Max}(m-n,\,n)}$. Also gilt auch für fast alle r all dies zugleich.

Für jedes derartige r enthält also $\mathfrak{A}-\mathfrak{A}_r$ und $\mathfrak{B}-\mathfrak{B}_r$ den Faktor $\mathfrak{p}^{m-n}$; ferner enthält $\mathfrak{B}$ und $\mathfrak{B}-\mathfrak{B}_r$ den Faktor $\mathfrak{p}^n$, also enthält ihn auch $\mathfrak{B}_r$. Und schliesslich enthält $\mathfrak{A}$ auch den Faktor $\mathfrak{p}^n$ Folglich enthalten die Zahlen $\mathfrak{B}_r(\mathfrak{A}-\mathfrak{A}_r)$ und $\mathfrak{A}(\mathfrak{B}-\mathfrak{B}_r)$ beide den Faktor $\mathfrak{p}^{(m-n)+n}$, d. h. $\mathfrak{p}^m$, also enthält ihn auch ihre Summe $\mathfrak{A}\mathfrak{B}-\mathfrak{A}_r\mathfrak{B}_r$.

Satz 23. Wenn $\mathfrak{p}_1^{m_1}, \mathfrak{p}_2^{m_2}, \ldots, \mathfrak{p}_n^{m_n}$ beliebig gegebene Primidealpotenzen sind, und $\mathfrak{A}$ eine ideale Zahl, so gibt es eine reale Zahl α, sodass $\mathfrak{A}-\alpha$ jeden der Faktoren $\mathfrak{p}_1^{m_1}, \mathfrak{p}_2^{m_2}, \ldots, \mathfrak{p}_n^{m_n}$ enthält.

Wenn insbesondere $\mathfrak{A}$ ganz ist, so kann auch α (algebraisch) ganz gewählt werden.

Beweis: Wenn $\mathfrak{A} \sim [\alpha_1, \alpha_2, \ldots]$ ist, so enthalten fast alle α_r den Faktor $\mathfrak{p}_1^{m_1}$, fast alle den Faktor $\mathfrak{p}_2^{m_2}, \ldots$, und fast alle den Faktor $\mathfrak{p}_n^{m_n}$. Also gibt es ein r für welches alle n Bedingungen erfüllt sind, entsprechend unserer Behauptung.

Wenn $\mathfrak{A}$ ganz ist, so können wir $[\alpha_1, \alpha_2, \ldots]$ so wählen, dass alle α_r ganz sind.

Satz 24. Wenn zu jeder Primidealpotenz $\mathfrak{p}^m$ ein algebraisch ganzes α existiert, sodass $\mathfrak{A} - \alpha$ den Faktor $\mathfrak{p}^m$ enthält, dann ist $\mathfrak{A}$ selbst ganz.

Beweis: Die abzählbar vielen Primideale schreiben wir in einer Folge $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$

Wir können für jedes r ein System von algebraisch ganzen $\beta_1^{(r)}, \beta_2^{(r)}, \ldots, \beta_s^{(r)}$ angeben, sodass $\mathfrak{A} - \beta_s^{(r)}$ allgemein den Faktor $\mathfrak{p}_s^r$ enthält. Wir bestimmen nun eine weitere algebraisch ganze Zahl α_r derart, dass sie den Kongruenzen

$$\begin{aligned} \alpha_r &\equiv \beta_1^{(r)} \pmod{\mathfrak{p}_1^r} \\ \alpha_r &\equiv \beta_2^{(r)} \pmod{\mathfrak{p}_2^r} \\ &\cdots\cdots\cdots \\ \alpha_r &\equiv \beta_r^{(r)} \pmod{\mathfrak{p}_r^r} \end{aligned}$$

genügt, was offenbar möglich ist. Dann ist für jedes $s = 1, 2, \ldots, r$ $\mathfrak{p}_s^r \mid \alpha_r - \beta_s^{(r)}$, d. h. $\alpha_r - \beta_s^{(r)}$ enthält den Faktor $\mathfrak{p}_s^r$; folglich enthält $\mathfrak{A} - \alpha_r$ alle Faktoren $\mathfrak{p}_1^r, \mathfrak{p}_2^r, \ldots, \mathfrak{p}_r^r$.

Nun bilden wir die Folge $[\alpha_1, \alpha_2, \ldots]$. Wir werden beweisen, dass sie fundamental ist und zu $\mathfrak{A}$ gehört; da alle α_r ganz sind, folgt hieraus, dass $\mathfrak{A}$ ganz ist.

Es sei $\mathfrak{A} \sim [\beta_1, \beta_2, \ldots]$; dann genügt es

$$[\alpha_1, \alpha_2, \ldots] \sim [\beta_1, \beta_2, \ldots]$$

zu zeigen.

Da für fast alle s die Differenz $\beta_s - \beta_{s+1}$ den Faktor $\mathfrak{p}_1^r$ enthält, für fast alle s dieselbe den Faktor $\mathfrak{p}_2^r$ enthält, ..., für fast alle s den Faktor $\mathfrak{p}_r^r$ enthält; so gelten auch für fast alle s sämtliche r Bedingungen zugleich. Wir können also $u = u(r)$ so wählen, dass aus $s \geqq u(r)$ stets folgt, dass $\beta_s - \beta_{s+1}$ alle Faktoren $\mathfrak{p}_1^r, \mathfrak{p}_2^r, \ldots, \mathfrak{p}_r^r$ enthält. Hieraus schliessen wir leicht, das für $s \geqq u(r)$, $t \geqq u(r)$ auch $\beta_s - \beta_t$ diese Faktoren enthält.

Nun sei die Primidealpotenz $\mathfrak{p}^m$, $\mathfrak{p} = \mathfrak{p}_n$ fest gegeben. Es sei $r \geqq \text{Max.}(m, n)$. Dann enthält

$$\mathfrak{A}-\alpha_r \sim [\beta_1, \beta_2, \ldots] - [\alpha_r, \alpha_r, \ldots] = [\beta_1 - \alpha_r,\ \beta_2 - \alpha_r, \ldots]$$

den Faktor $\mathfrak{p}^m$. Also muss für fast alle s die Differenz $\beta_s - \alpha_r$ den Faktor $\mathfrak{p}^m$ enthalten. Also auch für ein $s \geqq u$ (Max. (m, n)), da aber für $s \geqq u$ (Max. (m, n)), $t \geqq u$ (Max. (m, n)) die Differenz $\beta_s - \beta_t$ den Faktor $\mathfrak{p}^m$ stets enthält, ist das für alle $\beta_t - \alpha_r$, $t \geqq u$ (Max. (m, n)) der Fall. Wenn also insbesondere $r \geqq$ Max. (Max. (m, n), u (Max. (m, n)) ist, so enthält $\beta_r - \alpha_r$ auch den Faktor $\mathfrak{p}^m$.

Da diese Relation für fast alle r gilt, ist damit unsere Behauptung bewiesen.

Satz 25. Wenn alle Glieder einer konvergenten Folge $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ ganz sind, so ist es auch $\lim_{r \to \infty} \mathfrak{A}_r$.

Beweis: Wir können r so wählen, dass $\mathfrak{A} - \mathfrak{A}_r$ den Faktor $\mathfrak{p}^m$ enthält, und da $\mathfrak{A}_r$ ganz ist, α so dass $\mathfrak{A}_r - \alpha$ den Faktor $\mathfrak{p}^m$ enthält. Dann enthält auch $\mathfrak{A} - \alpha = (\mathfrak{A} - \mathfrak{A}_r) + (\mathfrak{A}_r - \alpha)$ den Faktor $\mathfrak{p}^m$.

Da dies für alle $\mathfrak{p}$ und m gilt, muss $\mathfrak{A}$ ganz sein.

Satz 26. Die Folge $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ ist dann und nur dann konvergent, wenn für jede Primidealpotenz $\mathfrak{p}^m$, für fast alle r die Differenz $\mathfrak{A}_0 - \mathfrak{A}_{r+1}$ den Faktor $\mathfrak{p}^m$ enthält.

Beweis: Wenn $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ konvergent ist, so enthält $\mathfrak{A} - \mathfrak{A}_r$ für fast alle r den Faktor $\mathfrak{p}^m$. Also gilt dasselbe für fast alle r von $\mathfrak{A} - \mathfrak{A}_{r+1}$. Folglich findet für fast alle r auch beides zugleich statt. Für solche r aber enthält auch $\mathfrak{A}_r - \mathfrak{A}_{r+1} = (\mathfrak{A} - \mathfrak{A}_{r+1}) - (\mathfrak{A} - \mathfrak{A}_r)$ den Faktor $\mathfrak{p}^m$.

Nun wollen wir umgekehrt aus unserer Bedingung die Konvergenz von $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ herleiten.

Wir bezeichnen die Folge der Primideale wieder mit $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ Wir wählen die Zahl α_r allgemein so, dass $\mathfrak{A}_r - \alpha_r$ die Faktoren $\mathfrak{p}_1^r, \mathfrak{p}_2^r, \ldots, \mathfrak{p}_r^r$ enthält; und dann bilden wir die Folge $[\alpha_1, \alpha_2, \ldots]$.

Diese Folge ist fundamental. Es sei nämlich eine Primidealpotenz $\mathfrak{p}^m$, $\mathfrak{p} = \mathfrak{p}_n$ gegeben. Ferner bestimmen wir p so, dass für $s \geqq p$ $\mathfrak{A}_s - \mathfrak{A}_{s+1}$ den Faktor $\mathfrak{p}^m$ enthält. Für $r \geqq$ Max. (m, n, p) enthält dann $\mathfrak{A}_r - \alpha_r$ den Faktor $\mathfrak{p}_n^r$, also auch den Faktor $\mathfrak{p}^m$. Ebenso enthält $\mathfrak{A}_{r+1} - \alpha_{r+1}$ diesen Faktor, und auch $\mathfrak{A}_r - \mathfrak{A}_{r+1}$; folglich enthält ihn

$$\alpha_r - \alpha_{r+1} = (\mathfrak{A}_{r+1} - \alpha_{r+1}) - (\mathfrak{A}_r - \alpha_r) + (\mathfrak{A}_r - \mathfrak{A}_{r+1})$$

ebenfalls.

Die zu $[\alpha_1, \alpha_2, \ldots]$ gehörende ideale Zahl sei $\mathfrak{A}$. Wir behaupten nun: es ist $\mathfrak{A}_r \to \mathfrak{A}$ für $r \to \infty$.

$\mathfrak{p} = \mathfrak{p}_n$ und m seien wie vorhin. Für $r \geqq \text{Max.}(m, n)$ (d. h. für fast alle r) hat $\mathfrak{A}_r - \alpha_r$ den Faktor $\mathfrak{p}^m$. Ferner hat wegen $\mathfrak{A} \sim [\alpha_1, \alpha_2, \ldots]$ auch $\mathfrak{A} - \alpha_r$ für fast alle r diesen Faktor. Folglich findet für fast alle r beides zugleich statt, und für solche r hat auch $\mathfrak{A} - \mathfrak{A}_r = (\mathfrak{A} - \alpha_r) - (\mathfrak{A}_r - \alpha_r)$ den Faktor $\mathfrak{p}^m$.

VI. Unendliche Summen und Produkte.

Definition 14. Für

$$\mathfrak{A}_m + \mathfrak{A}_{m+1} + \ldots + \mathfrak{A}_n \text{ und } \mathfrak{A}_m \cdot \mathfrak{A}_{m+1} \ldots \cdot \mathfrak{A}_n \; (m \leqq n)$$

schreiben wir kurz $\sum_m^n{}_r \mathfrak{A}_r$ bzw. $\left[\!\left[\prod_m^n{}_r \right]\!\right] \mathfrak{A}_r$.

Definition 15. Wir sagen, dass die unendliche Summe $\sum_m^\infty{}_r \mathfrak{A}_r$ oder das unendliche Product $\left[\!\left[\prod_m^\infty{}_r \right]\!\right] \mathfrak{A}_r$ *konvergiert*, wenn die Folge $\sum_m^m{}_r \mathfrak{A}_r, \sum_m^{m+1}{}_r \mathfrak{A}_r, \sum_m^{m+2}{}_r \mathfrak{A}_r, \ldots$ bzw. $\left[\!\left[\prod_m^m{}_r \right]\!\right] \mathfrak{A}_r, \left[\!\left[\prod_m^{m+1}{}_r \right]\!\right] \mathfrak{A}_r, \left[\!\left[\prod_m^{m+2}{}_r \right]\!\right] \mathfrak{A}_r, \ldots$ konvergiert. Unter $\sum_m^\infty{}_r \mathfrak{A}_r$ bzw. $\left[\!\left[\prod_m^\infty{}_r \right]\!\right] \mathfrak{A}_r$ verstehen wir in diesem Falle die Zahlen $\lim_{s \to \infty} \sum_m^{m+s-1}{}_r \mathfrak{A}_r$ bzw. $\lim_{s \to \infty} \left[\!\left[\prod_m^{m+s-1}{}_r \right]\!\right] \mathfrak{A}_r$.

Satz 27. Wenn die Summe $\sum_m^\infty{}_r \mathfrak{A}_r$ konvergiert, so konvergiert auch die Summe $\sum_m^\infty{}_r (\mathfrak{C} \cdot \mathfrak{A}_r)$; es ist

$$\sum_m^\infty{}_r (\mathfrak{C} \cdot \mathfrak{A}_r) = \mathfrak{C} \sum_m^\infty{}_r \mathfrak{A}_r.$$

Wenn die Summen $\sum_m^\infty{}_r \mathfrak{A}_r$ und $\sum_m^\infty{}_r \mathfrak{B}_r$ konvergieren, so konvergieren auch die Summen $\sum_m^\infty{}_r (\mathfrak{A}_r \pm \mathfrak{B}_r)$; es ist

$$\sum_m^\infty{}_r (\mathfrak{A}_r \pm \mathfrak{B}_r) = \sum_m^\infty{}_r \mathfrak{A}_r \pm \sum_m^\infty{}_r \mathfrak{B}_r.$$

Wenn die Produkte $\left[\!\left[\prod_m^\infty{}_r \right]\!\right] \mathfrak{A}_r$ und $\left[\!\left[\prod_m^\infty{}_r \right]\!\right] \mathfrak{B}_r$ konvergieren, so konvergiert auch das Produkt $\left[\!\left[\prod_m^\infty{}_r \right]\!\right] (\mathfrak{A}_r \cdot \mathfrak{B}_r)$; es ist

$$\left[\!\left[\prod_m^\infty{}_r \right]\!\right] (\mathfrak{A}_r \cdot \mathfrak{B}_r) = \left[\!\left[\prod_m^\infty{}_r \right]\!\right] \mathfrak{A}_r \quad \left[\!\left[\prod_m^\infty{}_r \right]\!\right] \mathfrak{B}_r.$$

Beweis: Klar auf Grund des Satzes 22.

Satz 28. Die Summe $\sum_{m}^{\infty} {}_r \mathfrak{A}_r$ konvergiert dann und nur dann, wenn $\mathfrak{A}_r \to 0$ für $r \to \infty$.

Beweis: Nach Satz 26. ist es notwendig und hinreichend, dass für fast alle s die Differenz

$$-\sum_{m}^{m+(s+1)-1} {}_r \mathfrak{A}_r + \sum_{m}^{m+s-1} {}_r \mathfrak{A}_r = -\mathfrak{A}_{m+s}$$

den Faktor $\mathfrak{p}^n$ enthalte d. h. dass $\mathfrak{A}_{m+s}$ den Faktor $\mathfrak{p}^n$ enthalte. Das ist damit gleichbedeutend, dass $\mathfrak{A}_t$ für fast alle t diesen Faktor enthält: und dies ist nichts anderes, als unsere Bedingung $\mathfrak{A}_t \to 0$ für $t \to \infty$.

VII. Ein Hilfssatz über Systeme von Faktor-Bedingungen.

Ehe wir weitergehen, müssen wir einen Satz über Systeme von Bedingungen von der Form

$$\beta \cdot \xi - \alpha \text{ enthält den Faktor } \mathfrak{p}^m \ (\beta \neq 0)$$

beweisen. In den später folgenden Konstruktionen idealer Zahlen wird es nämlich meistens auf die Lösung derartiger Bedingungen herauskommen.

Unser Satz lautet folgendermassen:

Satz 29. Ein System von Bedingungen

$$\begin{aligned}
&\beta_1 \cdot \xi - \alpha_1 \text{ enthält den Faktor } \mathfrak{p}_1^{r_1} \ (\beta_1 \neq 0)\\
&\beta_2 \cdot \xi - \alpha_2 \text{ enthält den Faktor } \mathfrak{p}_2^{r_2} \ (\beta_2 \neq 0)\\
&\quad \cdots\cdots\cdots\cdots\cdots\cdots\\
&\beta_u \cdot \xi - \alpha_u \text{ enthält den Faktor } \mathfrak{p}_u^{r_u} \ (\beta_u \neq 0)
\end{aligned}$$

($\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_u$ voneinander verschiedene Primideale) ist immer lösbar.

Wenn für jedes $\nu = 1, 2, \ldots, u$ alle Faktoren $\mathfrak{p}_\nu^{r}$, $r \leqq r_\nu$ die in β_ν enthalten sind, auch in α_ν enthalten sind, so ist es sogar durch ein algebraisch ganzes ξ lösbar.

Beweis: Wir zeigen zuerst, wie der erste Teil unseres Satzes auf den zweiten zurückgeführt werden kann.

Zu jeder Zahl $\gamma \neq 0$ und jedem Primideal $\mathfrak{p}$ gibt es ein s sodass γ den Faktor $\mathfrak{p}^s$ noch enthält, den Faktor $\mathfrak{p}^{s+1}$ aber nicht mehr: wir brauchen bloss das Ideal (γ) auf die Form eines Primidealpotenzproduktes bringen, und für s den Exponenten von $\mathfrak{p}$ zu wählen (0, wenn $\mathfrak{p}$ nicht vorkommt), dieser leistet das Gewünschte.

Für die β_ν seien diese Exponenten s_ν, $(\nu = 1, 2, \ldots, u)$. Die Prämisse des zweiten Teiles unseres Satzes ist offenbar die, dass α_ν stets den Faktor $\mathfrak{p}^{\text{Min.}(s_\nu, r_\nu)}$ hat.

Wenn nun dieser Teil des Satzes bewiesen ist, so verfahren wir so:

Wir wählen die t_ν so, dass α_ν den Faktor $\mathfrak{p}_\nu^{t_\nu}$ enthält, und setzen dann $x_\nu = s_\nu - t_\nu$. Sodann bestimmen wir die Zahl ϱ so, dass sie jeden der Faktoren $\mathfrak{p}_\nu^{x_\nu}$ enthalte, aber keinen der Faktoren $\mathfrak{p}_\nu^{x_\nu+1}$.

Dies ist unschwer durchführbar: nach einem bekannten Satze der Idealtheorie gibt es ja eine Zahl ϱ, für die

$$\frac{(\varrho)}{\mathfrak{p}_1^{x_1} \cdot \mathfrak{p}_2^{x_2} \cdot \ldots \cdot \mathfrak{p}_u^{x_u}}$$

ganz ist, und mit jedem der Ideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_u$ relativ prim. ϱ erfüllt offenbar unsere Bedingung.

Aus der genannten Eigenschaft des ϱ folgt aber, dass $\beta_\nu \cdot \xi - \alpha_\nu$ sicher den Faktor $\mathfrak{p}_\nu^{r_\nu}$ enthält, wenn

$$\varrho(\beta_\nu \cdot \xi - \alpha_\nu) = \beta_\nu \cdot (\varrho\xi) - \varrho\alpha_\nu$$

den Faktor $\mathfrak{p}_\nu^{r_\nu + x_\nu}$ enthält. D. h. unser System ist lösbar, wenn es das folgende System ist:

$\beta_\nu \quad \eta - \varrho\alpha_\nu$ enthält den Faktor $\mathfrak{p}^{r_\nu + x_\nu}$, $\nu = 1, 2, \ldots, u$. (Dann können wir wegen $\varrho \neq 0$ offenbar $\xi = \frac{\eta}{\varrho}$ setzen.)

Dieses System fällt aber unter den zweiten Teil unseres Satzes. Denn wenn β_ν den Faktor $\mathfrak{p}_\nu^r$ enthält, so ist $r \leqq s_\nu$; und da ϱ den Faktor $\mathfrak{p}_\nu^{x_\nu}$ und α_ν den Faktor $\mathfrak{p}_\nu^{t_\nu}$ enthält, so enthält $\alpha\varrho_\nu$ den Faktor $\mathfrak{p}_\nu^{t_\nu + x_\nu}$, d. h. $\mathfrak{p}_\nu^{s_\nu}$, also auch $\mathfrak{p}_\nu^r$.

Wir können also zum Beweise des zweiten Teiles übergehen. s_ν bedeute dasselbe, wie vorhin, nach Annahme enthält also α_ν den Faktor $\mathfrak{p}_\nu^{\text{Min.}(s_\nu, r_\nu)}$. Unter ξ verstehen wir von nun an eine (algebraisch) ganze Zahl.

$\beta_\nu \cdot \xi - \alpha_\nu = \beta_\nu \cdot \left(\xi - \frac{\alpha_\nu}{\beta_\nu}\right)$ enthält sicher den Faktor $\mathfrak{p}_\nu^{r_\nu}$, wenn $\xi - \frac{\alpha_\nu}{\beta_\nu}$ den Faktor $\mathfrak{p}_\nu^{r_\nu - s_\nu}$ enthält (da β_ν den Faktor $\mathfrak{p}_\nu^{s_\nu}$ enthält).

Da $\alpha_\nu = \beta_\nu \cdot \frac{\alpha_\nu}{\beta_\nu}$ den Faktor $\mathfrak{p}^{\text{Min.}(s_\nu, r_\nu)}$ enthält, und β_ν den Fak-

tor $p^{s_\nu+1}$ nicht enthält, muss $\frac{\alpha_\nu}{\beta_\nu}$ den Faktor $p_\nu^{\text{Min.}(s_\nu, r_\nu)\ s_\nu}$ enthalten.

Wir haben also ein System von Bedingungen der folgenden Form:

$\xi - \alpha'_\nu$ enthält den Faktor $p_\nu^{r'_\nu}$, $\nu = 1, 2, \ldots, u$, wobei α'_ν den Faktor $p_\nu^{\text{Min.}(0, r'_\nu)}$ enthält. (Diese Bedingungen haben wir nur als *hinreichend* erkannt, sie sind zwar auch notwendig, was uns aber hier nicht interessiert.) Hier genügt es aber zu zeigen, dass jede dieser u Bedingungen für sich allein lösbar ist: denn wenn sie bzw. die ganzen Lösungen $\xi_1, \xi_2, \ldots, \xi_u$ haben, so ist ein ξ sicher eine gemeinsame Lösung aller, welches den folgenden Kongruenzen genügt:

$$\begin{aligned} \xi &\equiv \xi_1 \pmod{p_1^{r'_1}} \\ \xi &\equiv \xi_2 \pmod{p_2^{r'_2}} \\ &\cdots\cdots\cdots \\ \xi &\equiv \xi_u \pmod{p_u^{r'_u}} \end{aligned}$$

Und dieses System von Kongruenzen ist offenbar durch ein ganzes ξ lösbar.

Es bleibt also noch übrig, zu zeigen, dass der Bedingung

$$\xi - \alpha \text{ hat den Faktor } p^r$$

wobei α den Faktor $p^{\text{Min.}(0, r)}$ hat, durch ein ganzes ξ genügt werden kann.

Für $r \leqq 0$ ist dies trivial: wegen $\text{Min.}(0, r) = r$ hat α den Faktor p^r, also kommt die Bedingung darauf heraus, dass ξ den Faktor p^r enthalte. Und wegen $r \leqq 0$ ist das für jedes ganze ξ der Fall.

Für $r > 0$ ist $\text{Min.}(0, r) = 0$, d. h. α enthält den Faktor p^0. Also ist $\alpha = \frac{\varkappa}{\lambda}$, wobei $\varkappa, \lambda$ algebraisch ganz sind, und λ nicht durch p teilbar ist. Wir können deshalb die Kongruenz

$$\lambda\eta \equiv 1 \pmod{p^r}$$

(durch ein ganzes η!) lösen. $\lambda\eta$ ist durch p nicht teilbar und dabei ganz, also enthält es den Faktor p^1 nicht. Folglich enthält $\xi - \alpha$ den Faktor p^r, wenn

$$\lambda\eta(\xi - \alpha) = \lambda\eta \cdot \xi - \varkappa\eta$$

ihn enthält. Da aber aus $\lambda\eta \equiv 1 \pmod{p^r}$ die Kongruenz

$$\lambda\eta \cdot \varkappa\eta \equiv \varkappa\eta \pmod{p^r}$$

folgt, enthält $\lambda\eta \cdot \varkappa\eta - \varkappa\eta$ sicher den Faktor p^r. Also ist $\xi = \varkappa\eta$ eine, offenbar ganze, Lösung.

VIII. p-adische Zahlen.

Definition 16. $\mathfrak{p}$ sei ein Primideal. Wir nennen eine ideale Zahl $\mathfrak{A}$ eine $\mathfrak{p}$-*adische Zahl,* wenn für jedes von $\mathfrak{p}$ verschiedene Primideal $\mathfrak{q}$ und für jedes m die Zahl $\mathfrak{A}$ den Faktor $\mathfrak{q}^m$ enthält.

Satz 30. $\mathfrak{A}$ sei eine ideale Zahl, $\mathfrak{p}$ ein beliebiges Primideal. Es gibt dann eine und nur eine $\mathfrak{p}$-adische Zahl $\mathfrak{B}$, sodass $\mathfrak{A}-\mathfrak{B}$ für alle m den Faktor $\mathfrak{p}^m$ enthält.

Beweis: Dass es höchstens ein solches $\mathfrak{B}$ geben kann, sehen wir sofort. Denn wenn $\mathfrak{B}_1$ und $\mathfrak{B}_2$ diese Eigenschaften haben, so ist jeder Faktor $\mathfrak{q}^m$, $\mathfrak{q} \neq \mathfrak{p}$, wegen der $\mathfrak{p}$-adizität von $\mathfrak{B}_1$ und $\mathfrak{B}_2$ in $\mathfrak{B}_1$ und in $\mathfrak{B}_2$ enthalten, also auch in $\mathfrak{B}_1-\mathfrak{B}_2$. Und jeder Faktor $\mathfrak{p}^m$ ist in $\mathfrak{A}-\mathfrak{B}_1$ und in $\mathfrak{A}-\mathfrak{B}_2$ enthalten, also auch in $\mathfrak{B}_1-\mathfrak{B}_2=(\mathfrak{A}-\mathfrak{B}_2)-(\mathfrak{A}-\mathfrak{B}_1)$. Nach Satz 20. ist also $\mathfrak{B}_1-\mathfrak{B}_2=0$, d. h. $\mathfrak{B}_1=\mathfrak{B}_2$.

Wir müssen nun zeigen, dass es ein solches $\mathfrak{B}$ gibt.

Zu diesem Zwecke schreiben wir die von $\mathfrak{p}$ verschiedenen Primideale irgendwie in einer Folge $\mathfrak{q}_1, \mathfrak{q}_2, \ldots$ Sodann wählen wir die Zahlen $\alpha_1, \alpha_2, \ldots$ so, dass allgemein $\mathfrak{A}-\alpha_r$ den Faktor $\mathfrak{p}^r$ enthalte (nach Satz 23.); und die Zahlen $\xi_1, \xi_2, \ldots$ so, dass allgemein ξ_r den Bedingungen

$$\begin{aligned}
&\xi_r \quad \text{enthält den Faktor } \mathfrak{q}_1^r\\
&\xi_r \quad \text{enthält den Faktor } \mathfrak{q}_2^r\\
&\ldots\ldots\ldots\ldots\ldots\\
&\xi_r \quad \text{enthält den Faktor } \mathfrak{q}_r^r\\
&\xi_r-\alpha_r \text{ enthält den Faktor } \mathfrak{p}^r
\end{aligned}$$

genügt (nach Satz 29.). Wir behaupten nun: die Folge $[\xi_1, \xi_2, \ldots]$ ist fundamental und die zu ihr gehörige Zahl $\mathfrak{B}$ genügt den Bedingungen des Satzes.

Um nachzuweisen, dass $[\xi_1, \xi_2, \ldots]$ fundamental ist, betrachten wir zuerst die Faktoren $\mathfrak{p}^m$. Für $r \geqq m$ hat $\xi_r-\alpha_r$ den Faktor $\mathfrak{p}^r$, also auch den Faktor $\mathfrak{p}^m$; ebenso hat auch $\xi_{r+1}-\alpha_{r+1}$ diesen Faktor. Ferner hat $\mathfrak{A}-\alpha_r$ ebenfalls den Faktor $\mathfrak{p}^r$, d. h. $\mathfrak{p}^m$; und $\mathfrak{A}-\alpha_{r+1}$ dessgleichen. Also hat auch

$$\xi_r-\xi_{r+1}=(\xi_{r+1}-\alpha_{r+1})-(\xi_r-\alpha_r)+(\mathfrak{A}-\alpha_r)-(\mathfrak{A}-\alpha_{r+1})$$

den Faktor $\mathfrak{p}^m$.

Zweitens betrachten wir die Faktoren $\mathfrak{q}^m$, $\mathfrak{q} \neq \mathfrak{p}$. Es ist $\mathfrak{q}=\mathfrak{q}_n$;

für $r \geqq \text{Max. } (m, n)$ haben ξ_r, ξ_{r+1} und mit ihnen $\xi_r - \xi_{r+1}$ den Faktor q_n^r, d. h. q^r, also auch den Faktor q^m

Es bleibt noch zu zeigen, dass für $\mathfrak{B} \sim [\xi_1, \xi_2, \ldots]$ die Zahl $\mathfrak{B}$ jeden Faktor q_n^m und die Zahl $\mathfrak{A} - \mathfrak{B}$ jeden Faktor p^m hat. Es ist aber

$$\mathfrak{B} \sim [\xi_1, \xi_2, \ldots];$$

und wenn $s \geqq \text{Max. } (m, n)$ ist, so hat ξ_s den Faktor q_n^s, also auch q_n^m, woraus die erste Behauptung folgt. Ferner ist

$$\alpha_r - \mathfrak{B} \sim [\alpha_r, \alpha_r, \ldots] - [\xi_1, \xi_2, \ldots] = [\alpha_r - \xi_1, \alpha_r - \xi_2, \ldots].$$

Nun hat $\alpha_m - \xi_m = -(\xi_m - \alpha_m)$ den Faktor p^m, und für $s \geqq m$ hat auch $\xi_s - \xi_{s+1}$ den Faktor p^m; also haben für $s \geqq m$ alle Differenzen $\alpha_m - \xi_s$ den Faktor p^m. Folglich hat $\alpha_m - \mathfrak{B}$ den Faktor p^m, und da $\mathfrak{A} - \alpha_m$ ihn auch hat, so muss $\mathfrak{A} - \mathfrak{B} = (\mathfrak{A} - \alpha_m) + (\alpha_m - \mathfrak{B})$ denselben ebenfalls enthalten. Damit ist auch die zweite Bahauptung bewiesen.

Definition 17. Die im Satze 30. erwähnte p-adische Zahl nennen wir *die p-adische Komponente von* $\mathfrak{A}$, und bezeichnen sie mit $(\mathfrak{A})_p$.

Satz 31. Wenn die idealen Zahlen $\mathfrak{A}$ und $\mathfrak{B}$ für jedes Primideal p dieselbe p-adische Komponente haben, so ist $\mathfrak{A} = \mathfrak{B}$.

Beweis: Für alle p und m hat sowohl $\mathfrak{A} - (\mathfrak{A})_p$ als auch $\mathfrak{B} - (\mathfrak{B})_p$ den Faktor p^m. Wegen $(\mathfrak{A})_p = (\mathfrak{B})_p$ aber ist $\mathfrak{A} - \mathfrak{B} = (\mathfrak{A} - (\mathfrak{A})_p) - (\mathfrak{B} - (\mathfrak{B})_p)$, sodass auch $\mathfrak{A} - \mathfrak{B}$ den Faktor p^m hat. Nach Satz 20 ist also $\mathfrak{A} - \mathfrak{B} = 0$, $\mathfrak{A} = \mathfrak{B}$.

Definition 18. Die (abzählbar vielen) Primideale seien irgendwie in eine Folge geordnet, die wir mit $\bar{p}_1, \bar{p}_2, \ldots$ bezeichnen werden.

Satz 32. Die Zahl $\mathfrak{A}_m^{[\bar{p}_m]}$ sei $\bar{p}_m$-adisch, $m = 1, 2, \ldots$ Dann ist die Summe $\sum_1^\infty {}_m \mathfrak{A}_m^{[\bar{p}_m]}$ konvergent.

Beweis: Nach Satz 28. müssen wir beweisen, dass $\mathfrak{A}_m^{[\bar{p}_m]} \to 0$ für $m \to \infty$. Es sei irgendein p^m gegeben, $p = \bar{p}_n$. Für alle $r \neq n$ ist $\bar{p}_r \neq \bar{p}_n$. $\mathfrak{A}_r^{[\bar{p}_r]}$ ist $\bar{p}_r$-adisch, also hat $\mathfrak{A}_r^{[\bar{p}_r]}$ den Faktor $\bar{p}_n^m$, d. h. $\bar{p}^m$. Hieraus folgt unsere Behauptung.

Satz 33. Die Zahl $\mathfrak{A}_m^{[\bar{p}_m]}$ sei $\bar{p}_m$-adisch, $m = 1, 2, \ldots$ Dann ist $\mathfrak{A}_m^{[\bar{p}_m]}$ die $\bar{p}_m$-adische Komponente von $\sum_1^\infty {}_m \mathfrak{A}_m^{[\bar{p}_m]}$.

Beweis: Da $\mathfrak{A}^{[\bar{\mathfrak{p}}_m]}$ gewiss $\bar{\mathfrak{p}}_m$-adisch ist, brauchen wir nur zu zeigen, dass $\sum_1^\infty {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]} - \mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$ jeden der Faktoren $\bar{\mathfrak{p}}_m^p$ enthält.

Wegen $\sum_1^r {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]} \to \sum_1^\infty {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]}$ für $r \to \infty$ gibt es ein $r \geqq p$, so dass $\sum_1^\infty {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]} - \sum_1^r {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]}$ den Faktor $\bar{\mathfrak{p}}_m^p$ hat. Also müssen wir zeigen, dass $\sum_1^r {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]} - \mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$ diesen Faktor hat. Nun ist

$$\sum_1^r {}_n\,\mathfrak{A}_n^{[\bar{\mathfrak{p}}_n]} - \mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]} = \mathfrak{A}_1^{[\bar{\mathfrak{p}}_1]} + \ldots + \mathfrak{A}_{m-1}^{[\bar{\mathfrak{p}}_{m-1}]} + \mathfrak{A}_{m+1}^{[\bar{\mathfrak{p}}_{m+1}]} + \ldots + \mathfrak{A}_r^{[\bar{\mathfrak{p}}_r]}.$$

Jeder Summand ist $\bar{\mathfrak{p}}_n$-adisch, $n \neq m$, d. h. $\bar{\mathfrak{p}}_n \neq \bar{\mathfrak{p}}_m$, hat also den Faktor $\bar{\mathfrak{p}}_m^p$; folglich hat ihn auch die Summe.

Satz 34. Jeder Folge $\mathfrak{A}_1^{[\bar{\mathfrak{p}}_1]}, \mathfrak{A}_2^{[\bar{\mathfrak{p}}_2]}, \ldots$ ($\mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$ ist $\bar{\mathfrak{p}}_m$-adisch) entspricht eine einzige ideale Zahl $\mathfrak{A}$, für die $(\mathfrak{A})_{\bar{\mathfrak{p}}_m} = \mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$ ist; nämlich die Zahl $\mathfrak{A} = \sum_1^\infty {}_m\,\mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$.

Beweis: Folgt aus den Sätzen 31, 32 und 33.

Definition 19. Wenn $\mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$ allgemein $\bar{\mathfrak{p}}_m$-adisch ist für $m = 1, 2, \ldots$, so schreiben wir für $\sum_1^\infty {}_m\,\mathfrak{A}_m^{[\bar{\mathfrak{p}}_m]}$ auch $\{\mathfrak{A}_1^{[\mathfrak{p}_1]}, \mathfrak{A}_2^{[\mathfrak{p}_2]}, \ldots\}$.

IX. $\mathfrak{p}$-adische Komponenten und die Grundoperationen.

Satz 35. Wenn die Zahlen $\mathfrak{A}^{[\mathfrak{p}]}$ und $\mathfrak{B}^{[\mathfrak{p}]}$ beide $\mathfrak{p}$-adisch sind, so sind es auch die Zahlen $\mathfrak{A}^{[\mathfrak{p}]} \pm \mathfrak{B}^{[\mathfrak{p}]}$.

Wenn $\mathfrak{A}^{[\mathfrak{p}]}$ $\mathfrak{p}$-adisch ist, und $\mathfrak{C}$ eine beliebige ideale Zahl ist so ist auch $\mathfrak{C} \cdot \mathfrak{A}^{[\mathfrak{p}]}$ $\mathfrak{p}$-adisch.

Beweis: Die erste Behauptung ist trivial; die zweite sehen wir folgendermassen ein:

Wir gezeigt, beim Beweise des Satzes 22 dass für jede ideale Zahl und jedes Primideal $\mathfrak{q}$ ein Faktor $\mathfrak{q}^n$ in der Zahl enthalten sein muss. Wenn nun eine Primidealpotenz $\mathfrak{q}^m$, $\mathfrak{q} \neq \mathfrak{p}$, gegeben ist, so enthält $\mathfrak{C}$ einen Faktor $\mathfrak{q}^n$, während $\mathfrak{A}^{[\mathfrak{p}]}$ den Faktor $\mathfrak{q}^{m-n}$ enthält. Folglich enthält $\mathfrak{C} \cdot \mathfrak{A}^{[\mathfrak{p}]}$ den Faktor $\mathfrak{q}^{n+(m-n)}$, d. h. $\mathfrak{q}^m$

Satz 36. Wenn die Zahlen $\mathfrak{A}^{[\mathfrak{p}]}$ und $\mathfrak{B}^{[\mathfrak{q}]}$ $\mathfrak{p}$-adisch bezw. $\mathfrak{q}$-adisch sind, $\mathfrak{p} \neq \mathfrak{q}$, dann ist $\mathfrak{A}^{[\mathfrak{p}]} \cdot \mathfrak{B}^{[\mathfrak{q}]} = 0$.

Beweis: Nach Satz 35. mus $\mathfrak{A}^{[p]} . \mathfrak{B}^{[q]}$ sowohl p-adisch als auch q-adisch sein. Da jedes Primideal $\mathfrak{r}$ unbedingt $\neq \mathfrak{p}$ oder $\neq \mathfrak{q}$ ist, so enthält $\mathfrak{A}^{[p]} . \mathfrak{B}^{[q]}$ jeden Faktor $\mathfrak{r}^m$. Nach Satz 20. ist es also $= 0$.

Satz 37. Es gelten die Gleichungen:

$$\{\mathfrak{A}_1^{[\mathfrak{p}_1]}, \mathfrak{A}_2^{[\mathfrak{p}_2]}, \ldots\} \pm \{\mathfrak{B}_1^{[\mathfrak{p}_1]}, \mathfrak{B}_2^{[\mathfrak{p}_2]}, \ldots\} = \{\mathfrak{A}_1^{[\mathfrak{p}_1]} \pm \mathfrak{B}_1^{[\mathfrak{p}_1]}, \mathfrak{A}_2^{[\mathfrak{p}_2]} \pm \mathfrak{B}_2^{[\mathfrak{p}_2]}, \ldots\}$$

$$\{\mathfrak{A}_1^{[\mathfrak{p}_1]}, \mathfrak{A}_2^{[\mathfrak{p}_2]}, \ldots\} \cdot \{\mathfrak{B}_1^{[\mathfrak{p}_1]}, \mathfrak{B}_2^{[\mathfrak{p}_2]}, \ldots\} = \{\mathfrak{A}_1^{[\mathfrak{p}_1]} \cdot \mathfrak{B}_1^{[\mathfrak{p}_1]}, \mathfrak{A}_2^{[\mathfrak{p}_2]} \cdot \mathfrak{B}_2^{[\mathfrak{p}_2]}, \ldots\}$$

Beweis: Es ist

$$\sum_1^m{}_r \mathfrak{A}_r^{[\mathfrak{p}_r]} \pm \sum_1^m{}_r \mathfrak{B}_r^{[\mathfrak{p}_r]} = \sum_1^m{}_r (\mathfrak{A}_r^{[\mathfrak{p}_r]} \pm \mathfrak{B}_r^{[\mathfrak{p}_r]})$$

$$\sum_1^m{}_r \mathfrak{A}_r^{[\mathfrak{p}_r]} \cdot \sum_1^m{}_r \mathfrak{B}_r^{[\mathfrak{p}_r]} = \sum_1^m{}_r \left(\sum_1^m{}_s \mathfrak{A}_r^{[\mathfrak{p}_r]} \mathfrak{B}_s^{[\mathfrak{p}_s]} \right) = \sum_1^m{}_r \mathfrak{A}_r^{[\mathfrak{p}_r]} \cdot \mathfrak{B}_r^{[\mathfrak{p}_r]}$$

(das letztere wegen Satz 36.). Hieraus folgt aber

$$\lim_{m \to \infty} \sum_1^m{}_r (\mathfrak{A}_r^{[\mathfrak{p}_r]} \pm \mathfrak{B}_r^{[\mathfrak{p}_r]}) = \lim_{m \to \infty} \sum_1^m{}_r \mathfrak{A}_r^{[\mathfrak{p}_r]} \pm \lim_{m \to \infty} \sum_1^m{}_r \mathfrak{B}_r^{[\mathfrak{p}_r]}$$

$$\lim_{m \to \infty} \sum_1^m{}_r \mathfrak{A}_r^{[\mathfrak{p}_r]} \cdot \mathfrak{B}_r^{[\mathfrak{p}_r]} = \lim_{m \to \infty} \sum_1^m{}_r \mathfrak{A}_r^{[\mathfrak{p}_r]} \cdot \lim_{m \to \infty} \sum_1^m{}_r \mathfrak{B}_r^{[\mathfrak{p}_r]}$$

und damit (nach Definition 19.) die Behauptung.

Satz 38. Es gelten die Gleichungen:

$$(\mathfrak{A} \pm \mathfrak{B})_\mathfrak{p} = (\mathfrak{A})_\mathfrak{p} \pm (\mathfrak{B})_\mathfrak{p}, \quad (\mathfrak{A} \cdot \mathfrak{B})_\mathfrak{p} = (\mathfrak{A})_\mathfrak{p} \cdot (\mathfrak{B})_\mathfrak{p} .$$

Beweis: Folgt aus Satz 37.

Satz 39. Wenn $\mathfrak{A}^{[p]}$, $\mathfrak{p} = \mathfrak{p}_m$, eine p-adische Zahl ist, so ist

$$\mathfrak{A}^{[p]} = \{0, 0, \ldots, 0, \mathfrak{A}^{[p]}, 0, \ldots\}$$

($\mathfrak{A}^{[p]}$ steht an der m-ten Stelle.

Beweis: Für $r \geqq m$ ist offenbar

$$0 + 0 + \ldots + 0 + \mathfrak{A}^{[p]} + 0 + \ldots + 0 = \mathfrak{A}^{[p]}$$

(insgesamt r Glieder), folglich ist der Limes der linken Seite für $r \to \infty$ gleich $\mathfrak{A}^{[p]}$, und hieraus folgt die Behauptung.

Satz 40. $\mathfrak{A}$ ist dann und nur dann ganz, wenn es alle $(\mathfrak{A})_\mathfrak{p}$ sind.

Beweis: Wenn die $(\mathfrak{A})_\mathfrak{p}$ ganz sind, so ist es auch jedes $\sum_1^m{}_r (\mathfrak{A})_{\mathfrak{p}_r}$, und infolge dessen auch

$$\mathfrak{A} = \sum_1^\infty{}_r (\mathfrak{A})_{\mathfrak{p}_r} = \lim_{m \to \infty} \sum_1^m{}_r (\mathfrak{A})_{\mathfrak{p}_r}$$

Ist umgekehrt $\mathfrak{A}$ ganz, so ist es auch jedes $(\mathfrak{A})_\mathfrak{p}$ aus folgendem Grunde: Für $\mathfrak{q} \neq \mathfrak{p}$ hat $(\mathfrak{A})_\mathfrak{p} - 0 = (\mathfrak{A})_\mathfrak{p}$ den Faktor $\mathfrak{q}^m$ (wegen der $\mathfrak{p}$-adizität); und wenn ein ganzes α so gewählt wird, dass $\mathfrak{A} - \alpha$ den Faktor $\mathfrak{p}^m$ enthalte, so enthält auch $(\mathfrak{A})_\mathfrak{p} - \alpha = (\mathfrak{A} - \alpha) - (\mathfrak{A} - (\mathfrak{A})_\mathfrak{p})$ diesen Faktor, weil $\mathfrak{A} - (\mathfrak{A})_\mathfrak{p}$ ihn enthält. Nach Satz 24. ist also $(\mathfrak{A})_\mathfrak{p}$ ganz.

Satz 41. Es gelten die Gleichungen:

$$\mathfrak{A} = \sum_1^\infty r\,(\mathfrak{A})_{\overline{\mathfrak{p}_r}} = \prod_1^\infty \left(1 + (\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}\right)$$

Beweis: Die erste ist trivial. Die zweite verifizieren wir so:

$$\prod_1^s \left(1 + (\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}\right) = \prod_1^s \left(1 + \{0, 0, \ldots, 0, (\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}, 0, \ldots\}\right) =$$

$$= \prod_1^s \left(\{(1)_{\overline{\mathfrak{p}_1}}, (1)_{\overline{\mathfrak{p}_2}}, \ldots\} + \{0, 0, \ldots, 0, (\mathfrak{A})_{\overline{\mathfrak{p}_r}} - (1)_{\overline{\mathfrak{p}_r}}, 0, \ldots\}\right) =$$

$$= \prod_1^s \{(1)_{\overline{\mathfrak{p}_1}}, (1)_{\overline{\mathfrak{p}_2}}, \ldots, (1)_{\overline{\mathfrak{p}_{r-1}}}, (\mathfrak{A})_{\overline{\mathfrak{p}_r}}, (1)_{\overline{\mathfrak{p}_{r+1}}}, \ldots\} =$$

$$= \{(\mathfrak{A})_{\overline{\mathfrak{p}_1}}, (\mathfrak{A})_{\overline{\mathfrak{p}_2}}, \ldots, (\mathfrak{A})_{\overline{\mathfrak{p}_s}}, (1)_{\overline{\mathfrak{p}_{s+1}}}, (1)_{\overline{\mathfrak{p}_{s+2}}}, \ldots\} =$$

$$= \{(1)_{\overline{\mathfrak{p}_1}}, (1)_{\overline{\mathfrak{p}_2}}, \ldots\} + \sum_1^s r\,\{0, 0, \ldots, 0, (\mathfrak{A})_{\overline{\mathfrak{p}_r}} - (1)_{\overline{\mathfrak{p}_r}}, 0, \ldots\} =$$

$$= 1 + \sum_1^s r\,\{0, 0, \ldots, 0, (\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}, 0, \ldots\} = 1 + \sum_1^s r\,(\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}.$$

Hieraus folgt aber:

$$\prod_1^\infty \left(1 + (\mathfrak{A} - 1)_{\overline{\mathfrak{p}}}\right) = \lim_{s \to \infty} \prod_1^s \left(1 + (\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}\right) = \lim_{s \to \infty} \left(1 + \sum_1^s r\,(\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}}\right) =$$

$$= \lim_{s \to \infty} 1 + \lim_{s \to \infty} \sum_1^s r\,(\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}} = 1 + \sum_1^\infty r\,(\mathfrak{A} - 1)_{\overline{\mathfrak{p}_r}} = 1 + (\mathfrak{A} - 1) = \mathfrak{A}.$$

X. Die Faktor-Zerlegung der idealen Zahlen.

Satz 42. $\mathfrak{A}, \mathfrak{B}$ seien zwei ideale Zahlen. Wenn zu jedem Primideal $\mathfrak{p}$ ein m angegeben werden kann, sodass $\mathfrak{B}$ den Faktor $\mathfrak{p}^m$ enthält, aber $\mathfrak{A}$ den Faktor $^{m+1}$ nicht; so ist $\mathfrak{A} \mid \mathfrak{B}$.

Beweis: Diejenigen Zahlen m, die zu den Primidealen $\overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2}, \ldots$ im Sinne der Prämisse gehören, seien $m_1, m_2, \ldots$ Es sei $\mathfrak{A} \sim [\alpha_1, \alpha_2, \ldots]$, $\mathfrak{B} \sim [\beta_1, \beta_2, \ldots]$.

Da für fast alle r die Differenz $\alpha_r - \alpha_{r+1}$ den Faktor $\mathfrak{p}_1^{m_1 + s}$ enthält, und auch den Faktor $\mathfrak{p}_2^{m_2 + s}$ für fast alle r enthält, ...,

und auch den Faktor $\mathfrak{p}_s^{m_s+s}$ für fast alle r enthält; so gelten ebenfalls für fast alle r alle diese s Bedingungen zugleich. Wir wählen $u = u(s)$ so dass die Differenz $\alpha_r - \alpha_{r+1}$ für $r \geqq u(s)$ alle diese Faktoren enthalte. Dann wird offenbar für $r \geqq u(s)$, $t \geqq u(s)$ auch $\alpha_r - \alpha_t$ alle diese Faktoren enthalten. Da $\mathfrak{A}$ den Faktor $\mathfrak{p}_s^{m_s+1}$ nicht enthält, werden nicht fast alle α_r diesen Faktor enthalten. Also gibt es ein $r \geqq u(s)$ für welches α_r ihn nicht enthält. Folglich enthält ihn kein α_t mit $t \geqq u(s)$.

Ebenso können wir Zahlen $v = v(s)$ konstruieren, für die so oft $r \geqq v(s)$, $t \geqq v(s)$ ist, $\beta_r - \beta_t$ alle Faktoren $\mathfrak{p}_1^{m_1+s}$, $\mathfrak{p}_2^{m_2+s}, \ldots,$ $\mathfrak{p}_s^{m_s+s}$ enthält. Da $\mathfrak{B}$ den Faktor $\mathfrak{p}_s^{m_s}$ enthält, so enthalten ihn fast alle β_r, also auch eines mit $r \geqq v(s)$. Folglich enthalten ihn alle β_t mit $t \geqq v(s)$.

Wir stellen nun eine monoton wachsende Folge $w(1), w(2), \ldots$ auf, sodass allgemein $w(s) \geqq u(s)$, $w(s) \geqq v(s)$ ist. Dann ist:

$$\mathfrak{A} \sim [\alpha_{w(1)}, \alpha_{w(2)}, \ldots], \quad \mathfrak{B} \sim [\beta_{w(1)}, \beta_{w(2)}, \ldots].$$

Jetzt werde eine Folge ganzer Zahlen $\xi_1, \xi_2, \ldots$ derart gewählt, dass ξ_r allgemein den folgenden Bedingungen genügt:

$$\begin{aligned}
&\alpha_{w(1)}\,\xi_r - \beta_{w(1)} \text{ enthält den Faktor } \mathfrak{p}_1^{m_1+r}\\
&\alpha_{w(2)}\,\xi_r - \beta_{w(2)} \text{ enthält den Faktor } \mathfrak{p}_2^{m_2+r}\\
&\quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\alpha_{w(r)}\,\xi_r - \beta_{w(r)} \text{ enthält den Faktor } \mathfrak{p}_r^{m_r+r}
\end{aligned}$$

Nach Satz 29. ist jedes solche System von Bedingungen durch ein ganzzahliges ξ_r lösbar: denn wenn $\alpha_{w(s)}$ den Faktor $\mathfrak{p}_s^m$ enthält, so ist $m < m_s + 1$, $m \leqq m_s$, sodass auch $\beta_{w(s)}$ diesen Faktor enthält.

Wir behaupten nun: die Folge $[\xi_1, \xi_2, \ldots]$ ist fundamental, und für die zu ihr gehörige ideale Zahl $\mathfrak{C}$ ist $\mathfrak{A} \cdot \mathfrak{C} = \mathfrak{B}$. Da alle ξ_r ganz sind, ist es dann auch $\mathfrak{C}$, sodass wirklich $\mathfrak{A} \mid \mathfrak{B}$ ist.

Es sei also $\mathfrak{p} = \mathfrak{p}_n$, und m beliebig gegeben.

Für $r \geqq \text{Max.}(m, n)$ haben die Ausdrücke

$$\alpha_{w(r)}\,\xi_r - \beta_{w(r)} \text{ und } \alpha_{w(r+1)}\,\xi_{r+1} - \beta_{w(r+1)}$$

den Faktor $\mathfrak{p}_m^{m_n+r}$, also auch den Faktor $\mathfrak{p}_m^{m_n+m}$. Ferner haben

$$\alpha_{w(r)} - \alpha_{w(r+1)} \text{ und } \beta_{w(r)} - \beta_{w(r+1)}$$

ebenfalls den Faktor $\mathfrak{p}_n^{m_n+r}$, also auch $\mathfrak{p}_n^{m_n+m}$. Da aber ξ_{r+1} ganz ist, folgt hieraus, dass

$$\begin{aligned}
&\{\alpha_{w(r+1)}\,\xi_{r+1} - \beta_{w(r+1)}\} - \{\alpha_{w(r)}\,\xi_r - \beta_{w(r)}\} +\\
&+ \xi_{r+1}\{\alpha_{w(r)} - \alpha_{w(r+1)}\} - \{\beta_{w(r)} - \beta_{w(r+1)}\} = -\alpha_{w(r)}\{\xi_r - \xi_{r+1}\}
\end{aligned}$$

diesen Faktor ebenfalls hat. Und weil $\alpha_{w(r)}$ den Faktor $\mathfrak{p}_n^{m_n+1}$ nicht hat, so muss $\xi_r - \xi_{r+1}$ den Faktor $\mathfrak{p}_n^{m}$ haben. Damit ist die Fundamentalität von $[\xi_1, \xi_2, \ldots]$ bewiesen.

Weiter ist

$$\mathfrak{A} \cdot \mathfrak{C} \sim [\alpha_{w(1)} \cdot \xi_1, \alpha_{w(2)} \cdot \xi_2, \ldots], \quad \mathfrak{B} \sim [\beta_{w(1)}, \beta_{w(2)}, \ldots]$$

und für beliebiges $\mathfrak{p} = \mathfrak{p}_n$ und m folgt aus $r \geqq \text{Max.}\,(m - m_n, n)$, dass $\alpha_{w(r)}\,\xi_r - \beta_{w(r)}$ den Faktor $\mathfrak{p}_n^{(m_n - n) + m_n}$, d. h. $\mathfrak{p}_n^{m}$ enthält. Folglich ist $[\alpha_{w(1)} \cdot \xi_1, \alpha_{w(2)} \cdot \xi_2, \ldots] \sim [\beta_{w(1)}, \beta_{w(2)}, \ldots]$, d. h. $\mathfrak{A} \cdot \mathfrak{C} = \mathfrak{B}$.

Definition. 20. Wir nennen zwei ideale Zahlen $\mathfrak{A}, \mathfrak{B}$ *assoziiert,* wenn $\mathfrak{A} \mid \mathfrak{B}$ und $\mathfrak{B} \mid \mathfrak{A}$ ist.

Satz 43. Es ist stets $\mathfrak{A}$ mit $\mathfrak{A}$ assoziiert.

Wenn $\mathfrak{A}$ mit $\mathfrak{B}$ assoziiert ist, so ist es auch $\mathfrak{B}$ mit $\mathfrak{A}$.

Wenn $\mathfrak{A}$ mit $\mathfrak{B}$ und $\mathfrak{B}$ mit $\mathfrak{C}$ assoziiert ist, so ist es auch $\mathfrak{A}$ mit $\mathfrak{C}$.

Beweis: Klar.

Satz 44. Zwei assoziierte Zahlen sind entweder beide ganz, oder keine ist es.

Beweis: Klar.

Satz 45. Wenn $\mathfrak{A}'$ zu $\mathfrak{A}''$ und $\mathfrak{B}'$ zu $\mathfrak{B}''$ assoziiert ist, so ist es auch $\mathfrak{A}' \cdot \mathfrak{B}'$ zu $\mathfrak{A}'' \cdot \mathfrak{B}''$.

Beweis: Klar.

Definition 21. $\mathfrak{A}$ ist eine *Einheit,* wenn es zu 1 assoziiert ist.

Satz 46. Jede Einheit ist ganz.

± 1 sind Einheiten.

Wenn $\mathfrak{E}$ und $\mathfrak{F}$ beide Einheiten sind, so ist es auch $\mathfrak{E} \cdot \mathfrak{F}$.

Wenn $\mathfrak{E}$ eine Einheit ist, und $\mathfrak{F}$ ganz und $\mathfrak{F} \mid \mathfrak{E}$ ist, so ist $\mathfrak{F}$ auch eine Einheit.

Beweis: Klar.

Definition 22. Zu jedem Primideal $\mathfrak{p}_m$ werde irgendeine Zahl $\overline{\zeta}_m$ zugeordnet, die zu $\overline{\mathfrak{p}}_m$ gehört, aber zu $\overline{\mathfrak{p}}_m^2$ nicht.

Definition 23. Die ideale Zahl $1 + (\zeta_m - 1)_{\overline{\mathfrak{p}}_m}$ bezeichnen wir mit $\overline{\mathfrak{P}}_m$.

Die Zahl $1 + (\zeta_m^s - 1)_{\overline{\mathfrak{p}}_m}$ bezeichnen wir mit $\overline{\mathfrak{P}}_m^s$ $(s = 0, \pm 1, \pm 2, \ldots)$, die Zahl $1 - (1)_{\overline{\mathfrak{p}}_m}$ mit $\mathfrak{P}_m^{\pm\infty}$.

Satz 47. Es ist $\overline{\mathfrak{P}}_m^0 = 1$, $\overline{\mathfrak{P}}_m^1 = \overline{\mathfrak{P}}_m$.

Ferner ist stets (auch für s oder $t = +\infty$) $\overline{\mathfrak{P}}_m^{s+t} = \overline{\mathfrak{P}}_m^s \cdot \overline{\mathfrak{P}}_m^t$.

Schliesslich ist $\lim_{s\to\infty} \overline{\mathfrak{P}}_m^s = \overline{\mathfrak{P}}_m^{+\infty}$.

Beweis: Die zwei ersten Behauptungen folgen aus der Definition von $\overline{\mathfrak{P}}_m^s$ sofort, wenn man beim Multiplizieren den Satz 38. benützt. Die dritte Bahauptung beweisen wir so:

Es ist $\lim_{s\to\infty} \overline{\mathfrak{P}}_m^s = \overline{\mathfrak{P}}_m^{+\infty}$, wenn für jedes $\mathfrak{p}$ und jedes n die Differenz $\overline{\mathfrak{P}}_m^{+\infty} - \overline{\mathfrak{P}}_m^s$ für fast alle s den Faktor $\mathfrak{p}^n$ enthält.

Nun ist

$$\overline{\mathfrak{P}}_m^{+\infty} - \overline{\mathfrak{P}}_m^s = (1-(1)_{\overline{\mathfrak{p}}_m}) - (1+(\overline{\zeta}_m^s - 1)_{\overline{\mathfrak{p}}_m}) =$$
$$= -(\overline{\zeta}_m^s - 1)_{\overline{\mathfrak{p}}_m} - (1)_{\overline{\mathfrak{p}}_m} = (\overline{\zeta}_m^s)_{\overline{\mathfrak{p}}_m}.$$

Wenn $\mathfrak{p} \neq \overline{\mathfrak{p}}_m$ ist, so hat $(\overline{\zeta}_m^s)_{\overline{\mathfrak{p}}_m}$ für alle s den Faktor $\overline{\mathfrak{p}}^n$, weil es $\overline{\mathfrak{p}}_m$-adisch ist. Wenn dagegen $\mathfrak{p} = \overline{\mathfrak{p}}$ ist, hat $(\overline{\zeta}_m^s) - (\overline{\zeta}_m^s)_{\overline{\mathfrak{p}}_m}$ stets den Faktor $\overline{\mathfrak{p}}_m^n$, also müssen wir nur feststellen, wann $\overline{\zeta}_m^s$ den Faktor $\overline{\mathfrak{p}}_m^n$ hat Das ist aber wegen $\overline{\mathfrak{p}}_m \mid \zeta_m$ sicher der Fall, sobald $s \geq$ Max. $(0, n)$ ist.

Satz 48. Jedes Produkt $\prod_1^\infty \overline{\mathfrak{P}}_r^{m_r}$ ist konvergent, dabei können die $m_r = 0, \pm 1, \pm 2, \ldots$ oder $+\infty$ sein.

Beweis: Es sei $\mathfrak{A} = \{(\overline{\zeta}_1^{m_1}), (\overline{\zeta}_2^{m_2}), \ldots\}$. Dann ist

$$(\mathfrak{A}-1)_{\overline{\mathfrak{p}}_r} = (\mathfrak{A})_{\overline{\mathfrak{p}}_r} - (1)_{\overline{\mathfrak{p}}_r} = (\overline{\zeta}_r^{m_r})_{\overline{\mathfrak{p}}_r} - (1)_{\overline{\mathfrak{p}}_r} = (\overline{\zeta}_r^{m_r} - 1)_{\overline{\mathfrak{p}}_r},$$
$$1 + (\mathfrak{A}-1)_{\overline{\mathfrak{p}}_r} = 1 + (\overline{\zeta}_r^{m_r} - 1)_{\overline{\mathfrak{p}}_r} = \overline{\mathfrak{P}}_r^{m_r}.$$

(Für $m_r = +\infty$ haben wir $\overline{\zeta}_r^{m_r}$ durch 0 zu ersetzen.) Nun ist $\prod_1^\infty (1 + (\mathfrak{A}-1)_{\overline{\mathfrak{p}}_r})$ nach Satz 41. sicher konvergent, u. zw. gleich $\mathfrak{A}$, also gilt dasselbe von $\prod_1^\infty \overline{\mathfrak{P}}_r^{m_r}$.

Satz 49. *(Hauptsatz I.)* Jede ideale Zahl $\mathfrak{A}$ kann auf die Form

$$\mathfrak{A} = \mathfrak{E} \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{m_r}$$

gebracht werden, wobei $\mathfrak{E}$ eine Einheit ist und die $m_r = 0, \pm 1, \pm 2, \ldots$ oder $+\infty$ sind.

Beweis: Es ist zunächst

$$\mathfrak{A} = \prod_1^\infty (1 + (\mathfrak{A}-1)_{\overline{\mathfrak{p}}_r}).$$

Die Zahl $1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}$ ihrerseits hat, wie wir beim Beweise des Satzes 41. zeigten, die Form

$$\{(1)_{\bar{\mathfrak{p}}_1}, (1)_{\bar{\mathfrak{p}}_2}, \ldots, (1)_{\bar{\mathfrak{p}}_{r-1}}, (\mathfrak{A})_{\bar{\mathfrak{p}}_r}, (1)_{\bar{\mathfrak{p}}_{r+1}}, \ldots\}$$

Nun sind zwei Fälle denkbar: entweder enthält $(\mathfrak{A})_{\bar{\mathfrak{p}}_r}$ den Faktor $\mathfrak{p}_r^m$ für alle m, oder nicht.

In erstem Falle ist nach Satz 20. $(\mathfrak{A})_{\bar{\mathfrak{p}}_r}=0$, denn es enthält jeden Faktor $\mathfrak{p}^m$ (wenn $\mathfrak{p}\neq\bar{\mathfrak{p}}_r$ ist, zufolge der $\bar{\mathfrak{p}}_r$-adizität, und wenn $\mathfrak{p}=\bar{\mathfrak{p}}_r$ ist, nach der Annahme). Folglich ist

$$1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}=\{(1)_{\bar{\mathfrak{p}}_1}, (1)_{\bar{\mathfrak{p}}_2}, \ldots, (1)_{\bar{\mathfrak{p}}_{r-1}}, 0, (1)_{\bar{\mathfrak{p}}_{r+1}}, \ldots\}=$$
$$=1-(1)_{\bar{\mathfrak{p}}_r}=\bar{\mathfrak{P}}_r^{+\infty}$$

Im zweiten Falle stellen wir zuerst fest, dass es unbedingt ein m gibt, für welches $(\mathfrak{A})_{\bar{\mathfrak{p}}_r}$ den Faktor $\bar{\mathfrak{p}}_r^m$ enthält: das wurde bereits beim Beweise von Satz 22. bemerkt. Da es aber auch ein solches m gibt, für welches das nicht der Fall ist, so können wir ein $m=m_r$ finden, sodass $(\mathfrak{A})_{\bar{\mathfrak{p}}_r}$ den Faktor $\mathfrak{p}_r^{m_r}$ hat, den Faktor $\bar{\mathfrak{p}}_r^{m_r+1}$ aber nicht.

Betrachten wir nun die $\mathfrak{p}_s$-adische Komponente von $1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}$ und diejenige von $\bar{\mathfrak{P}}_r^{m_r}$. Sie sind beide $=(1)_{\bar{\mathfrak{p}}_s}$, wenn $s\neq r$ ist, und $=(\mathfrak{A})_{\bar{\mathfrak{p}}_r}$, bzw. $(\bar{\zeta}_r^{m_r})_{\bar{\mathfrak{p}}_r}$, wenn $s=r$ ist. $1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}$ enthält den Faktor $\mathfrak{p}_s^m$ sicher, wenn ihn seine $\bar{\mathfrak{p}}_s$-adische Komponente enthält, d. h. $(1)_{\bar{\mathfrak{p}}_s}$ bzw. $(\mathfrak{A})_{\bar{\mathfrak{p}}_r}$. Die erstere enthält nun $\bar{\mathfrak{p}}_s^0$ (weil sie ganz ist), die letztere $\bar{\mathfrak{r}}_r^{m_r}$.

Andererseits enthält $\bar{\mathfrak{P}}_r^{m_r}$ den Faktor $\mathfrak{p}_s^m$ nur dann, wenn ihn seine $\bar{\mathfrak{p}}_s$-adische Komponente enthält, d. h. $(1)_{\bar{\mathfrak{p}}_s}$ bzw. $(\bar{\zeta}_r^{m_r})_{\bar{\mathfrak{p}}_r}$. Diese enthält den Faktor aber nur dann, wenn ihn 1 bzw. $\bar{\zeta}_r^{m_r}$ enthält. Die erstere enthält aber $\bar{\mathfrak{p}}_s^1$ nicht, die letztere $\bar{\mathfrak{p}}_r^{m_r+1}$ nicht.

Damit sind die Prämissen von Satz 42. erfüllt: es muss $\bar{\mathfrak{P}}_r^{m_r} \mid 1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}$ sein. Also ist

$$1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}=\mathfrak{C}_r\,.\,\bar{\mathfrak{P}}_r^{m_r}\ (\mathfrak{C}_r \text{ ganz})$$
$$(\mathfrak{A})_{\bar{\mathfrak{p}}_r}=(1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r})_{\bar{\mathfrak{p}}_r}=(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}\,.\,(\bar{\mathfrak{P}}_r^{m_r})_{\bar{\mathfrak{p}}_r}=(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}\,.\,(\bar{\zeta}_r^{m_r})_{\bar{\mathfrak{p}}_r}.$$

Also ist

$$1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}=\{(1)_{\bar{\mathfrak{p}}_1},(1)_{\bar{\mathfrak{p}}_2},\ldots,(1)_{\bar{\mathfrak{p}}_{r-1}},(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}\cdot(\bar{\zeta}_r^{m_r})_{\bar{\mathfrak{p}}_r},(1)_{\bar{\mathfrak{p}}_{r+1}},\ldots\}=$$
$$=\{(1)_{\bar{\mathfrak{p}}_1},(1)_{\bar{\mathfrak{p}}_2},\ldots,(1)_{\bar{\mathfrak{p}}_{r-1}},(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r},(1)_{\bar{\mathfrak{p}}_{r+1}},\ldots\}\cdot\bar{\mathfrak{P}}_r^{m_r}.$$

Dabei hat $(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}$ den Faktor $\mathfrak{p}_r^1$ nicht: denn dann hätte

$$(\mathfrak{A})_{\bar{\mathfrak{p}}_r}=(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}\cdot(\bar{\zeta}_r^{m_r})_{\bar{\mathfrak{p}}_r}$$

den Faktor $\bar{\mathfrak{p}}_r^{m_r+1}$, entgegen unserer Annahme. $(\bar{\zeta}_r^{m_r})_{\mathfrak{p}_r}$ hat nämlich den Faktor $\bar{\mathfrak{p}}_r^{m_r}$, weil $\bar{\zeta}_r^{m_r}$ ihn hat: denn da $\bar{\zeta}_r$ zu $\mathfrak{p}_r$ aber nicht zu $\mathfrak{p}_r^2$ gehört, ist

$$\bar{\zeta}_r=\mathfrak{p}_r\cdot\mathfrak{q}_1^{s_1}\cdot\mathfrak{q}_2^{s_2}\ldots\mathfrak{q}_n^{s_n}$$

($\mathfrak{q}_1,\mathfrak{q}_2,\ldots\mathfrak{q}_n$ von $\mathfrak{p}_r$ und voneinander verschiedene Primideale)

$$\bar{\zeta}_r^{m_r}=\mathfrak{p}_r^{m_r}\cdot\mathfrak{q}_1^{m_r s_1}\cdot\mathfrak{q}_2^{m_r s_2}\ldots\mathfrak{q}_u^{m_r s_u}.$$

Also können wir beide Fälle so zusammenfassen:

Es ist

$$1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r}=\{(1)_{\bar{\mathfrak{p}}_1},\ldots,(1)_{\bar{\mathfrak{p}}_{r-1}},(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r},(1)_{\bar{\mathfrak{p}}_{r+1}},\ldots\}\cdot\bar{\mathfrak{P}}_r^{m_r}$$

wobei $(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}$ ganz ist und den Faktor $\bar{\mathfrak{p}}_r^1$ nicht enthält; und $m_r=0,\pm1,\pm2,\ldots,+\infty$ ist.

Also ist

$$\{(\mathfrak{C}_1)_{\bar{\mathfrak{p}}_1},(\mathfrak{C})_{\bar{\mathfrak{p}}_r},\ldots\}\cdot\prod_1^{\infty}{}^{r}\bar{\mathfrak{P}}_r^{m_r}=\prod_1^{\infty}{}^{r}\{(1)_{\bar{\mathfrak{p}}_1},\ldots,(1)_{\bar{\mathfrak{p}}_{r-1}},(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r},(1)_{\bar{\mathfrak{p}}_{r+1}},\ldots\}\cdot$$
$$\cdot\prod_1^{\infty}{}^{r}\bar{\mathfrak{P}}_r^{m_r}=\prod_1^{\infty}{}^{r}\{(1)_{\bar{\mathfrak{p}}_{r_1}},(1)_{\bar{\mathfrak{p}}_{r_2}},\ldots,(1)_{\bar{\mathfrak{p}}_{r-1}},(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r},(1)_{\bar{\mathfrak{p}}_{r+1}},\ldots\}\cdot\mathfrak{P}_r^{m_r}=$$
$$=\prod_1^{\infty}{}^{r}(1+(\mathfrak{A}-1)_{\bar{\mathfrak{p}}_r})=\mathfrak{A}.$$

Wir sind also am Ziele, wenn wir noch beweisen, dass

$$\mathfrak{E}=\{(\mathfrak{C}_1)_{\bar{\mathfrak{p}}_1},(\mathfrak{C}_2)_{\bar{\mathfrak{p}}_2},\ldots\}$$

eine Einheit ist.

Da alle $(\mathfrak{E})_{\bar{\mathfrak{p}}_r}=(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}$ ganz sind, ist auch $\mathfrak{E}$ ganz, d. h. $1\mid\mathfrak{E}$. Da $(\mathfrak{E})_{\bar{\mathfrak{p}}_r}=(\mathfrak{C}_r)_{\bar{\mathfrak{p}}_r}$ den Faktor $\bar{\mathfrak{p}}_r^1$ nicht enthält, enthält ihn auch $\mathfrak{E}$ nicht. Hingegen enthält 1 den Faktor $\bar{\mathfrak{p}}_r$ (weil 1 ganz ist), also können wir wieder den Satz 42. anwenden: es ist $\mathfrak{E}\mid1$. D. h.: $\mathfrak{E}$ und 1 sind assoziiert, $\mathfrak{E}$ ist eine Einheit.

XI. Die Eindeutigkeit der Exponentenfolge.

Definition 23. Wenn

$$\mathfrak{A} = \mathfrak{E} \cdot \prod_1^\infty{}_{(r)} \mathfrak{P}_r^{m_r}, \quad \mathfrak{E} \text{ Einheit}, \quad m_r = 0, \pm 1, \pm 2, \ldots, +\infty$$

ist, so nennen wir $m_1, m_2, \ldots$ eine *Exponentenfolge von* $\mathfrak{A}$.

Satz 50. $m_1, m_2, \ldots$ sei eine Exponentenfolge von $\mathfrak{A}$.

$\mathfrak{A}$ enthält den Faktor $\overline{\mathfrak{p}}_r^m$ dann und nur dann, wenn $m \leqq m_r$ ist.

Beweis: Wir müssen zeigen, dass $\mathfrak{A}$ den Faktor $\overline{\mathfrak{p}}_r^{m_r}$ enthält, und den Faktor $\overline{\mathfrak{p}}_r^{m_r+1}$ nicht, falls m_r endlich ist; und für $m = +\infty$, dass es alle Faktoren $\overline{\mathfrak{p}}_r^m$ enthält.

Da $\mathfrak{A}$ mit $\prod_1^\infty{}_{(r)} \overline{\mathfrak{P}}_r^{m_r}$ assoziiert ist, können wir an seiner Stelle dieses Produkt betrachten. Wenn wir $(\overline{\zeta}_r^{m_r})_{\overline{\mathfrak{p}}_r}$ bzw. 0 (je nach dem m_r endlich oder $+\infty$ ist), kurz mit $\mathfrak{C}_r^{[\mathfrak{p}_r]}$ bezeichnen, so ist

$$\prod_1^\infty{}_{(r)} \mathfrak{P}_r^{m_r} = \prod_1^\infty{}_{(r)} \{(1)_{\overline{\mathfrak{p}}_1}, \ldots, (1)_{\overline{\mathfrak{p}}_{r-1}}, \mathfrak{C}_r^{[\mathfrak{p}_r]}, (1)_{\overline{\mathfrak{p}}_{r+1}}, \ldots\} = \{\mathfrak{C}_1^{[\overline{\mathfrak{p}}_1]}, \mathfrak{C}_2^{[\overline{\mathfrak{p}}_2]}, \ldots\}$$

Statt $\prod_1^\infty{}_{(r)} \mathfrak{P}_r^{m_r}$ können wir natürlich seine $\overline{\mathfrak{p}}_r$-adische Komponente, $\mathfrak{C}_r^{[\overline{\mathfrak{p}}_r]}$, untersuchen.

Wenn m_r endlich ist, so ist zunächst $\mathfrak{C}_r^{[\overline{\mathfrak{p}}_r]} = (\overline{\zeta}_r^{m_r})_{\overline{\mathfrak{p}}_r}$, und wenn wir statt $(\overline{\zeta}_r^{m_r})_{\overline{\mathfrak{p}}_r}$ das hier völlig gleichwertige $\overline{\zeta}_r^{m_r}$ betrachten, so sehen wir:

$$\overline{\zeta}_r^{m_r} = \mathfrak{p}_r^{m_r} \cdot \mathfrak{q}_1^{m_r s_1} \cdot \mathfrak{q}_2^{m_r s_2} \cdot \ldots \cdot \mathfrak{q}_n^{m_r s_n}$$

(Vgl. Beweis von Satz 42.) und dieser Ausdruck enthält den Faktor $\mathfrak{p}_r^{m_r}$, aber nicht den Faktor $\mathfrak{p}_r^{m_r+1}$.

Wenn $m_r = +\infty$ ist, so ist $\mathfrak{C}_r^{[\overline{\mathfrak{p}}_r]} = 0$, es enthält also alle Faktoren $\mathfrak{p}_r^m$.

Satz 51. *(Hauptsatz II.)* Jede ideale Zahl $\mathfrak{A}$ hat eine und nur eine Exponentenfolge.

Beweis: Dass es mindestens eine gibt, wissen wir aus Satz 48. Sind nun $m_1, m_2, \ldots$ und $n_1, n_2, \ldots$ zwei Exponentenfolgen von $\mathfrak{A}$, so ist nach Satz 50. $m \leqq m_r$ mit $m \leqq n_r$ (m endlich, m_r, n_r eventuell $+\infty$) gleichbedeutend. Also muss allgemein $m_r = n_r$ sein.

Satz 52. Jede Folge $m_1, m_2, \ldots$ ($m_r = 0, \pm 1, \pm 2, \ldots, +\infty$) ist Exponentenfolge einer geeigneten idealen Zahl.

Beweis: Z. B. von $1 \cdot \prod_1^\infty{}_{(r)} \overline{\mathfrak{P}}_r^{m_r}$.

XII. Eigenschaften der Exponentenfolge.

Satz 53. 1 hat die Exponentenfolge $0, 0, \ldots$; 0 hat die Exponentenfolge $+\infty, +\infty, \ldots$

Beweis: Da für jedes $\mathfrak{p}_r$ der Faktor $\mathfrak{p}_r^m$ in der Zahl 0 enthalten ist, sind für 0 alle m_r gleich $+\infty$.

Bei der 1 hingegen ist:

$$1 \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^0 = 1 \cdot \prod_1^\infty 1 = 1 \cdot \lim_{s \to \infty} \prod_1^s 1 = 1 \cdot \lim_{s \to \infty} 1 = 1 \cdot 1 = 1.$$

Satz 54. Die ideale Zahl $\mathfrak{A}$ besitze die Exponentenfolge $m_1, m_2, \ldots$, die ideale Zahl $\mathfrak{B}$ die Exponentenfolge $n_1, n_2, \ldots$. Dann hat $\mathfrak{A} \cdot \mathfrak{B}$ die Exponentenfolge $m_1 + n_1,\ m_2 + n_2, \ldots$

Beweis: Es ist

$$\mathfrak{A} = \mathfrak{E} \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{m_r}, \quad \mathfrak{B} = \mathfrak{F} \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{n_r}$$

wobei $\mathfrak{E}, \mathfrak{F}$ Einheiten sind; also ist

$$\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{E} \cdot \mathfrak{F} \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{m_r} \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{n_r} = (\mathfrak{E} \cdot \mathfrak{F}) \cdot \prod_1^\infty (\overline{\mathfrak{P}}_r^{m_r} \cdot \overline{\mathfrak{P}}_r^{n_r}) =$$

$$= (\mathfrak{E} \cdot \mathfrak{F}) \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{n_r + n_r}$$

und auch $\mathfrak{E} \cdot \mathfrak{F}$ ist eine Einheit.

Satz 55. $\mathfrak{A} \mid \mathfrak{B}$ ist mit $m_r \leqq n_r$ (für alle r) gleichbedeutend.

Beweis: Wenn $\mathfrak{A} \mid \mathfrak{B}$ ist, so ist jeder in $\mathfrak{A}$ enthaltene Faktor $\mathfrak{p}_r^m$ auch in $\mathfrak{B}$ enthalten. Also folgt aus $m \leqq m_r$ auch $m \leqq n_r$ (m endlich, m_r, n_r eventuell $+\infty$). Folglich muss $m_r \leqq n_r$ sein.

Nun sei umgekehrt $m_r \leqq n_r$. Da $\mathfrak{E}$ eine Einheit ist, ist $\mathfrak{E} \cdot \mathfrak{G} = 1$, $\mathfrak{G}$ ganz; also ist auch $\mathfrak{G}$, und damit $\mathfrak{H} = \mathfrak{E} \cdot \mathfrak{G}$ eine Einheit. Es ist $\mathfrak{E} \cdot \mathfrak{H} = \mathfrak{F}$. Für

$$\mathfrak{C} = \mathfrak{H} \cdot \prod_1^\infty \overline{\mathfrak{P}}_r^{n_r - m}$$

ist offenbar $\mathfrak{A} \cdot \mathfrak{C} = \mathfrak{B}$. (Der Ausdruck $n_r - m_r$ ist für den Fall $m_r = +\infty$ eigentlich sinnlos; wir nehmen für $m_r = n_r = +\infty$ für $n_r - m_r$ irgendeinen Wert $\geqq 0$ an, einerlei welchen; der Fall n_r endlich und $m_r = +\infty$ ist durch die Voraussetzung $m_r \leqq n_r$ ausgeschlossen.)

Wir müssen nur noch zeigen, dass $\mathfrak{C}$ ganz ist, dann ist alles bewiesen.

$\mathfrak{H}$ ist Einheit, also ganz; es bleibt noch $\prod_1^{\infty}{}_{r} \overline{\mathfrak{P}}_r^{n_r - m_r}$ zu erledigen. $\prod_1^{\infty}{}_{r} \overline{\mathfrak{P}}_r^{n_r - m_r}$ ist nach Satz 40. ganz, wenn es alle seine $\overline{p}_r$-adischen Komponenten sind. Seine $\overline{p}_r$-adische Komponente ist aber für endliches $n_r - m_r$ gleich $(\overline{\zeta}_r^{n_r - m_r})_{\overline{p}_r}$, und für $n_r - m_r = +\infty$ gleich 0. (Vgl. Beweis von Satz 49.) 0 ist jedenfalls ganz; $(\overline{\zeta}_r^{n_r - m_r})_{\overline{p}_r}$ ist es auch, denn $\overline{\zeta}_r^{n_r - m_r}$ ist wegen $n_r - m_r \geqq 0$ ganz.

Satz 56. $\mathfrak{A}$ ist dann und nur dann ganz, wenn alle $m_r \geqq 0$ sind.

$\mathfrak{A}$ und $\mathfrak{B}$ sind dann und nur dann assoziiert, wenn alle $m_r = n_r$ sind.

$\mathfrak{A}$ is dann und nur dann Einheit, wenn alle $m_r = 0$ sind.

Beweis: Folgt aus Satz 55. sowie 53.

Satz 57. *(Hauptsatz III.)* $\mathfrak{a}$ sei ein beliebiges Ideal, es sei $\mathfrak{a} = \overline{\mathfrak{p}}_1^{m_1} \cdot \overline{\mathfrak{p}}_2^{m_2} \cdot \ldots \cdot \overline{\mathfrak{p}}_r^{m_r}$ (natürlich alle $m_1, m_2, \ldots, m_r$ endlich). Wir bilden die ideale Zahl $\mathfrak{A} = \overline{\mathfrak{P}}_1^{m_1} \cdot \overline{\mathfrak{P}}_2^{m_2} \cdot \ldots \cdot \overline{\mathfrak{P}}_r^{m_r}$.

Dann ist für jede reale Zahl α die Relation $\mathfrak{a} \mid \alpha$ mit $\mathfrak{A} \mid \alpha$ gleichbedeutend

Beweis: Schreiben wir die Primideal-Faktorenzerlegung von (α) an: (für $\alpha = 0$ ist ja alles klar)

$$(\alpha) = \mathfrak{p}_1^{n_1} \cdot \mathfrak{p}_2^{n_2} \cdot \ldots \cdot \mathfrak{p}_r^{n_r} \cdot \mathfrak{p}_{r+1}^{n_{r+1}} \cdot \ldots \cdot \mathfrak{p}_s^{n_s}$$

α enthält offenbar die Faktoren $\mathfrak{p}_1^{n_1}, \mathfrak{p}_2^{n_2}, \ldots, \mathfrak{p}_s^{n_s}, \mathfrak{p}_{s+1}^0, \mathfrak{p}_{s+2}^0, \ldots$ und es enthält die Faktoren $\mathfrak{p}_1^{n_1+1}, \mathfrak{p}_2^{n_2+1}, \ldots, \mathfrak{p}_{s+1}^1, \mathfrak{p}_{s+2}^1, \ldots$ nicht. Nach Satz 50. ist also die Exponentenfolge von α gleich $n_1, n_2, \ldots, n_r, n_{r+1}, \ldots, n_s, 0, 0, \ldots$ Die von $\mathfrak{A}$ ist andererseits $m_1, m_2, \ldots, m_r, 0, \ldots, 0, 0, 0, \ldots$ Nach Satz 55. ist also $\mathfrak{A} \mid \alpha$ mit

$$n_1 \geqq m_1, n_2 \geqq m_2, \ldots, n_r \geqq m_r \text{ und } n_{r+1} \geqq 0, \ldots, n_s \geqq 0$$

gleichbedeutend. Dies ist aber auch die notwendig und hinreichende Bedingung dafür, dass $\mathfrak{a} \mid (\alpha)$, d. h. $\mathfrak{a} \mid \alpha$ sei.

XIII. Der grösste gemeinsame Teiler.

Satz 58. $\mathfrak{A}, \mathfrak{B}$ seien zwei ideale Zahlen. Es gibt eine ideale Zahl $\mathfrak{C}$ derart, dass die Gleichungen

$$\mathfrak{A} = \mathfrak{C} \cdot \mathfrak{X}, \quad \mathfrak{B} = \mathfrak{C} \cdot \mathfrak{Y},$$
$$\mathfrak{C} = \mathfrak{A} \cdot \mathfrak{U} + \mathfrak{B} \cdot \mathfrak{V}$$

mit ganzen $\mathfrak{X}, \mathfrak{Y}, \mathfrak{U}, \mathfrak{V}$ bestehen.

Beweis: Wir setzen

$$\mathfrak{A} = \mathfrak{E} \cdot \prod_1^\infty \mathfrak{P}_r^{m_r}, \quad \mathfrak{A} = \mathfrak{F} \cdot \prod_1^\infty \mathfrak{P}_r^{n_r}$$

wobei $\mathfrak{E}, \mathfrak{F}$ Einheiten sind, also für ganze $\mathfrak{G}, \mathfrak{H}$

$$\mathfrak{E} \cdot \mathfrak{G} = 1, \quad \mathfrak{F} \cdot \mathfrak{H} = 1$$

gilt. Es sei nun

$$\mathfrak{C} = \prod_1^\infty \mathfrak{P}_r^{\text{Min. } (m_r, n_r)}$$

$\mathfrak{C}$ erfüllt unsere Bedingungen.

Erstens folgt aus Min. $(m_r, n_r) \leqq m_r$ und $\leqq n_r$ nach Satz 55. dass $\mathfrak{C} \mid \mathfrak{A}$, $\mathfrak{C} \mid \mathfrak{B}$ ist, d. h.

$$\mathfrak{A} = \mathfrak{C} \cdot \mathfrak{X}, \quad \mathfrak{B} = \mathfrak{C} \cdot \mathfrak{Y}.$$

Zweitens zerlegen wir die Folge $1, 2, \ldots$ in zwei Teilmengen $u_1, u_2, \ldots$ und $v_1, v_2, \ldots$ derart, dass jedes $r = 1, 2, \ldots$ entweder ein u_s oder ein v_s ist, und dass im ersten Falle stets Min. $(m_r, n_r) = m_r$ ist, im zweiten aber stets $= n_r$.

Wir bestimmen die Zahl $\mathfrak{U}'$ und $\mathfrak{V}'$ so, dass

$$(\mathfrak{U}')_{\mathfrak{p}_r} = (1)_{\mathfrak{p}_r} \text{ für } r = u_s, \text{ und } = 0 \quad \text{für } r = v_s$$

$$(\mathfrak{V}')_{\mathfrak{p}_r} = 0 \quad \text{für } r = u_s, \text{ und } = (1)_{\mathfrak{p}_r} \text{ für } r = v_s$$

ist. Man sieht sofort, dass $\mathfrak{U}'$ und $\mathfrak{V}'$ ganz sind, und dass

$$\mathfrak{U}' \cdot \prod_1^\infty \mathfrak{P}_r^{m_r} + \mathfrak{V}' \cdot \prod_1^\infty \mathfrak{P}_r^{n_r} = \prod_1^\infty \mathfrak{P}_r^{\text{Min. } (m_r, n_r)}$$

ist Also ist für $\mathfrak{U} = \mathfrak{G} \cdot \mathfrak{U}'$, $\mathfrak{B} = \mathfrak{H} \cdot \mathfrak{V}'$ wirklich

$$\mathfrak{C} = \mathfrak{A} \cdot \mathfrak{U} + \mathfrak{B} \cdot \mathfrak{V}.$$

Definition 24. $\mathfrak{C}$ ist *ein grösster gemeinsamer Teiler von* $\mathfrak{A}$ *und* $\mathfrak{B}$, wenn $\mathfrak{d} \mid \mathfrak{C}$ damit gleichbedeutend ist, dass $\mathfrak{d} \mid \mathfrak{A}$ und $\mathfrak{d} \mid \mathfrak{B}$ ist.

Satz 57. Zwei Zahlen $\mathfrak{A}, \mathfrak{B}$ haben stets grösste gemeinsame Teiler, diese bilden eine Klasse assoziierter Zahlen.

Beweis: Betrachten wir das $\mathfrak{C}$ des Satzes 56. Aus $\mathfrak{d} \mid \mathfrak{C}$ folgt wegen $\mathfrak{C} \mid \mathfrak{A}$, $\mathfrak{C} \mid \mathfrak{B}$ hier $\mathfrak{d} \mid \mathfrak{A}$, $\mathfrak{d} \mid \mathfrak{B}$. Aus $\mathfrak{d} \mid \mathfrak{A}$, $\mathfrak{d} \mid \mathfrak{B}$ aber folgt $\mathfrak{d} \mid \mathfrak{A} \cdot \mathfrak{U}$, $\mathfrak{d} \mid \mathfrak{B} \cdot \mathfrak{V}$ also $\mathfrak{d} \mid \mathfrak{A} \cdot \mathfrak{U} + \mathfrak{B} \cdot \mathfrak{V}$, d. h. $\mathfrak{d} \mid \mathfrak{C}$. Also ist $\mathfrak{C}$ ein grösster gemeinsamer Teiler von $\mathfrak{A}$ und $\mathfrak{B}$.

Wenn $\mathfrak{C}'$ und $\mathfrak{C}''$ grösste gemeinsame Teiler von $\mathfrak{A}$ und $\mathfrak{B}$ sind, so ist $\mathfrak{d} \mid \mathfrak{C}'$ mit $\mathfrak{d} \mid \mathfrak{C}''$ gleichbedeutend. Wegen $\mathfrak{C}' \mid \mathfrak{C}'$ ist also $\mathfrak{C}' \mid \mathfrak{C}''$, und wegen $\mathfrak{C}'' \mid \mathfrak{C}''$ ist $\mathfrak{C}'' \mid \mathfrak{C}'$: also sind sie assoziiert.

Wenn umgekehrt $\mathfrak{C}'$ grösster gemeinsamer Teiler von $\mathfrak{A}$ und $\mathfrak{B}$ ist, und mit $\mathfrak{C}''$ assoziiert ist, so ist es auch $\mathfrak{C}''$: denn $\mathfrak{H} \mid \mathfrak{C}''$ ist mit $\mathfrak{H} \mid \mathfrak{C}'$ gleichbedeutend.

Satz 58. Jeder grösste gemeinsame Teiler von $\mathfrak{A}$ und $\mathfrak{B}$ hat die Form $\mathfrak{A} \cdot \mathfrak{U} + \mathfrak{B} \cdot \mathfrak{V}$ ($\mathfrak{U}, \mathfrak{V}$ ganz), und die Exponentenreihe Min. (m_1, n_1), Min. $(m_2, n_2), \ldots$

Beweis: Für das $\mathfrak{C}$ des Satzes 56. trifft beides zu, und dieses $\mathfrak{C}$ ist ein grösster gemeinsamer Teiler von $\mathfrak{A}$ und $\mathfrak{B}$. Alle anderen sind aber mit $\mathfrak{C}$ assoziiert, folglich gilt unser Satz auch für sie.

XIV. Die Einteilung der idealen Zahlen.

Definition 25. Wie wir wissen, ist $\mathfrak{A}$ dann und nur dann 0, wenn seine Exponentenfolge aus lauter $+\infty$ besteht.

Wenn die Exponentenfolge auch endliche m_r enthält, aber mindestens ein $+\infty$, so ist $\mathfrak{A}$ ein *Nullteiler*.[11])

Wenn die Exponentenfolge lauter endliche m_r enthält, aber unendlich oft $m_r \neq 0$ ist, so ist $\mathfrak{A}$ *unendlich*.[12])

Wenn die Exponentenfolge lauter endliche m_r enthält, und nur endlich oft $m_r \neq 0$ ist, so ist $\mathfrak{A}$ *endlich*.[12])

Satz 59. In einer Klasse assoziierter idealer Zahlen sind alle Elemente $= 0$, oder alle Nullteiler, oder alle unendlich, oder alle endlich.

Beweis: Folgt aus Satz 56., da es sich um Aussagen über die Exponentenfolge handelt.

Satz 60. $\mathfrak{A}$ ist dann und nur dann endlich, wenn es zwei reale Zahlen α, β gibt, sodass $\mathfrak{A} \mid \alpha, \beta \mid \mathfrak{A}$ ($\alpha \neq 0, \beta \neq 0$) ist.

Beweis: Wenn $\mathfrak{A}$ endlich ist, so ist es offenbar gleich

$$\mathfrak{E} \cdot \mathfrak{P}_1^{m_1} \cdot \mathfrak{P}_2^{m_2} \cdot \ldots \cdot \mathfrak{P}_r^{m_r},$$

$\mathfrak{E}$ eine Einheit, wir können also das zu $\mathfrak{A}$ assoziierte Produkt

$$\mathfrak{A}' = \mathfrak{P}_1^{m_1} \cdot \mathfrak{P}_2^{m_2} \cdot \ldots \cdot \mathfrak{P}_r^{m_r}$$

betrachten. Wenn wir α so wählen, dass es zu $\mathfrak{p}_1^{m_1} \cdot \mathfrak{p}_2^{m_2} \cdot \ldots \cdot \mathfrak{p}_r^{m_r}$ gehört, und dabei $\neq 0$ ist, so ist nach Satz 57.

$$\mathfrak{P}_1^{m_1} \cdot \mathfrak{P}_2^{m_2} \cdot \ldots \cdot \mathfrak{P}_r^{m_r} \mid \alpha, \mathfrak{A}' \mid \alpha, \mathfrak{A} \mid \alpha.$$

---

[11]) Dass unsere „Nullteiler" solche im gewöhnlichen Sinne des Wortes sind, zeigen wir in Satz 62.

[12]) Prüfer deftniert die endlichen idealen Zahlen anders. Dass beide Definitionen gleichbedeutend sind, zeigen wir in Satz 60.

Ebenso können wir ein $\beta \neq 0$ so bestimmen, dass für

$$\mathfrak{B}' = \mathfrak{P}_1^{-m_1} \cdot \mathfrak{P}_2^{-m_2} \cdot \ldots \cdot \mathfrak{P}_r^{-m_r}$$

$\mathfrak{B}' | \beta$, d. h. $\beta = \mathfrak{B}' . \mathfrak{C}$ ($\mathfrak{C}$ ganz) sei. Nun ist offenbar $\mathfrak{A}' . \mathfrak{B}' = 1$,

$$\mathfrak{C} . \frac{1}{\beta} = 1 . \mathfrak{C} . \frac{1}{\beta} = \mathfrak{A}' . \mathfrak{B}' . \mathfrak{C} . \frac{1}{\beta} = \mathfrak{A}' . \beta . \frac{1}{\beta} =$$

$$= \mathfrak{A}' . 1 = \mathfrak{A}', \frac{1}{\beta} | \mathfrak{A}', \frac{1}{\beta} | \mathfrak{A}.$$

Nun sei umgekehrt $\mathfrak{A} | \alpha, \beta | \mathfrak{A}$ ($\alpha \neq 0, \beta \neq 0$). Wenn wir

$$(\alpha) = \overline{\mathfrak{p}}_1^{m_1} \cdot \overline{\mathfrak{p}}_2^{m_2} \cdot \ldots \cdot \overline{\mathfrak{p}}_r^{m_r}, \quad (\beta) = \overline{\mathfrak{p}}_1^{n_1} \cdot \overline{\mathfrak{p}}_2^{n_2} \cdot \ldots \cdot \overline{\mathfrak{p}}_r^{n_r}$$

setzen, so hat offenbar α die Exponentenfolge $m_1, m_2, \ldots, m_r, 0, 0, \ldots$, und β die Exponentenfolge $n_1, n_2, \ldots, n_r, 0, 0, \ldots$ (Alle m_r, n_r sind endlich). Für die Exponentenfolge $p_1, p_2, \ldots$ von $\mathfrak{A}$ gilt folglich:

$$m_1 \leqq p_1 \leqq n_1, m_2 \leqq p_2 \leqq n_2, \ldots, m_r \leqq p_r \leqq n_r, p_{r+1} = 0, p_{r+2} = 0, \ldots$$

Also is $\mathfrak{A}$ endlich.

Satz 61. Es gibt zu jedem Ideale $\mathfrak{a}$ eine ideale Zahl $\mathfrak{A}$, sodass $\mathfrak{a} | \alpha$ mit $\mathfrak{A} | \alpha$ gleichbedeutend ist.

Zu einer idealen Zahl $\mathfrak{A}$ kann hingegen ein solches Ideal $\mathfrak{a}$ dann und nur dann angegeben werden, wenn $\mathfrak{A}$ endlich ist.

Beweis: Dass zu jedem α ein $\mathfrak{A}$ und zu jedem endlichen $\mathfrak{A}$ ein α existiert wurde bereits durch Satz 57. ausgesagt. Wir müssen noch zeigen, dass für nicht endliche $\mathfrak{A}$ kein α vorhanden ist.

Wenn in der Exponentenfolge von $\mathfrak{A}$ ein $+\infty$ vorkommt, also etwa $m_r = +\infty$ ist, so enthält $\mathfrak{A}$ alle Faktoren $\overline{\mathfrak{p}}_r^m$. Aus $\mathfrak{A} | \alpha$ folgt dann, dass auch α alle Faktoren $\overline{\mathfrak{p}}_r^m$ enthält, d. h. es muss $\alpha = 0$ sein. Ein Ideal, welches nur die 0 enthält, gibt es aber nicht.

Wenn alle m_r endlich sind, so müssen unendlich viele $\neq 0$ sein. (Sonst ist $\mathfrak{A}$ endlich.) Ist für unendlich viele m_r sogar $m_r > 0$, so ist in diesen Fällen $m_r \geqq 1$, d. h. $\mathfrak{A}$ enthält den Faktor $\overline{\mathfrak{p}}_r^1$. Wenn $\mathfrak{A} | \alpha$ ist, so muss also α unendlich viele Faktoren $\overline{\mathfrak{p}}_r^1$ enthalten, woraus wieder $\alpha = 0$ folgt.

Also können wir uns auf den Fall beschränken, dass fast alle $m_r \leqq 0$ und unendlich viele < 0 sind. Die r für die $m_r > 0$ ist, seien etwa $u_1, u_2, \ldots, u_t$, die r für die $m_r < 0$ ist, $v_1, v_2, \ldots$ Dann ist für jedes

$$\alpha_s = \overline{\mathfrak{p}}_{v_s}^{-1} \cdot \overline{\mathfrak{p}}_{u_1}^{m_1} \cdot \overline{\mathfrak{p}}_{u_2}^{m_2} \cdot \ldots \cdot \overline{\mathfrak{p}}_{u_t}^{m_t}$$

offenbar $\mathfrak{A} | \alpha_s$. Aus

$$\overline{\mathfrak{p}}_{v_s}^{-1} \cdot \overline{\mathfrak{p}}_{u_1}^{m_1} \cdot \overline{\mathfrak{p}}_{u_2}^{m_2} \cdot \ldots \cdot \overline{\mathfrak{p}}_{u_t}^{m_t} | \alpha$$

folgt also $\mathfrak{A} \mid \alpha$. Oder wenn wir

$$\bar{\mathfrak{p}}_{u_1}^{m_1} \cdot \bar{\mathfrak{p}}_{u_2}^{m_2} \cdot \ldots \cdot \bar{\mathfrak{p}}_{u_t}^{m_t} = \mathfrak{a}'$$

setzen: aus $\frac{\mathfrak{a}'}{\bar{\mathfrak{p}}_{v_s}} \mid \alpha$ folgt $\mathfrak{A} \mid \alpha$. Wäre nun $\mathfrak{A} \mid \alpha$ mit $\mathfrak{a} \mid \alpha$ gleichbedeutend, so müsste $\mathfrak{a} \mid \frac{\mathfrak{a}'}{\bar{\mathfrak{p}}_{v_s}}$, $\bar{\mathfrak{p}}_{v_s} \mid \frac{\mathfrak{a}'}{\mathfrak{a}}$ sein. D. h. $\frac{\mathfrak{a}'}{\mathfrak{a}}$ hätte unendlich viele Primfaktoren, was unmöglich ist.

XV. Die Division.

Satz 62. Es sei $\mathfrak{A} \,.\, \mathfrak{B} = 0$. Dann ist entweder $\mathfrak{A} = 0$, oder $\mathfrak{B} = 0$, oder aber sind sowohl $\mathfrak{A}$ als $\mathfrak{B}$ Nullteiler.

Beweis: Die Exponentenfolge von $\mathfrak{A}$ und $\mathfrak{B}$ seien $m_1, m_2, \ldots$ bzw. $n_1, n_2, \ldots$ $\mathfrak{A} \,.\, \mathfrak{B} = 0$ bedeutet, dass für alle r $m_r + n_r = +\infty$ ist, d. h. $m_r = +\infty$ oder $n_r = +\infty$ ist. Also sind entweder alle $m_r = +\infty$ oder alle $n_r = +\infty$, oder es gibt sowohl ein m_r als ein n_r, welches $+\infty$ ist. Das ist aber die Behauptung.

Satz 62. $\mathfrak{A}$ sei $\neq 0$ und kein Nullteiler. Die Gleichung $\mathfrak{A} \,.\, \mathfrak{X} = \mathfrak{B}$ hat dann eine und nur eine Lösung.

Beweis: Es sei

$$\mathfrak{A} = \mathfrak{E} \,.\, \prod_1^{\infty}{}_r \bar{\mathfrak{P}}_r^{m_r}, \quad \mathfrak{B} = \mathfrak{F} \,.\, \prod_1^{\infty}{}_r \bar{\mathfrak{P}}_r^{n_r}, \quad \mathfrak{E}, \mathfrak{F} \text{ Einheiten.}$$

Wegen $\mathfrak{E} \mid \mathfrak{F}$ gibt es ein $\mathfrak{G}$, sodass $\mathfrak{E} \,.\, \mathfrak{G} = \mathfrak{F}$ ist.

$$\mathfrak{X} = \mathfrak{G} \,.\, \prod_1^{\infty}{}_r \bar{\mathfrak{P}}_r^{n_r - m_r}$$

(alle m_r sind nach Annahme endlich) genügt dann den Anforderungen.

Aus $\mathfrak{A} \,.\, \mathfrak{X}_1 = \mathfrak{B}$, $\mathfrak{A} \,.\, \mathfrak{X}_2 = \mathfrak{B}$ folgt

$$\mathfrak{A} \,.\, \mathfrak{X}_1 = \mathfrak{A} \,.\, \mathfrak{X}_2, \quad \mathfrak{A} \,.\, \mathfrak{X}_1 - \mathfrak{A} \,.\, \mathfrak{X}_2 = 0, \quad \mathfrak{A} \,.\, (\mathfrak{X}_1 - \mathfrak{X}_2) = 0$$

und weil $\mathfrak{A}$ kein Nullteiler ist, $\mathfrak{X}_1 - \mathfrak{X}_2 = 0$, $\mathfrak{X}_1 = \mathfrak{X}_2$.

Definition 26. Die im Satze 62.. erwähnte ideale Zahl bezeichnen wir mit $\frac{\mathfrak{A}}{\mathfrak{B}}$.

Satz 63. Wenn $\mathfrak{A}, \mathfrak{B}$ die Exponentenfolgen $m_1, m_2, \ldots$ bzw. $n_1, n_2, \ldots$ haben ($\mathfrak{A} \neq 0$ und kein Nullteiler), so hat $\frac{\mathfrak{A}}{\mathfrak{B}}$ die Exponentenfolge $n_1 - m_1$, $n_2 - m_2, \ldots$

Beweis: Dies wurde beim Beweise von Satz 62. festgestellt.