XLIX.

Über die Theorie der ganzen algebraischen Zahlen.

[Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, 3. Aufl., S. 515—530 (1879).]

Inhalt.

§ 170.

Während unsere bisherigen Untersuchungen über Ideale wesentlich nur in einer Anwendung der Lehre von der Teilbarkeit der Moduln bestanden, gehen wir jetzt zu einer neuen Idealbildung, nämlich zur Multiplikation der Ideale über, welche den eigentlichen Kern der Idealtheorie bildet.

Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, und bedeutet α jede Zahl in $\mathfrak{a}$, ebenso β jede Zahl in $\mathfrak{b}$, so verstehen wir unter dem Produkte $\mathfrak{a}\,\mathfrak{b}$ der Faktoren $\mathfrak{a}$, $\mathfrak{b}$ den Inbegriff aller Zahlen, welche als ein Produkt $\alpha\beta$ oder als Summe von mehreren solchen Produkten $\alpha\beta$ darstellbar sind. Alle diese Zahlen sind wieder in $\mathfrak{o}$ enthalten, und sie verschwinden nicht sämtlich; sie reproduzieren sich durch Addition und Subtraktion, sowie durch Multiplikation mit beliebigen Zahlen ω des Gebietes $\mathfrak{o}$, weil jedes Produkt $\beta\omega$ wieder in $\mathfrak{b}$ enthalten ist. Mithin ist das Produkt $\mathfrak{a}\,\mathfrak{b}$ wieder ein Ideal.

Es leuchtet ohne weiteres ein, daß $\mathfrak{a}\,\mathfrak{o} = \mathfrak{a}$, $\mathfrak{a}(\mathfrak{o}\eta) = \mathfrak{a}\eta$, $\mathfrak{a}\,\mathfrak{b} = \mathfrak{b}\,\mathfrak{a}$ und $(\mathfrak{a}\,\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\,\mathfrak{c})$ ist; wir bezeichnen dieses letztere Produkt kurz mit $\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}$, und aus der schon öfter angewendeten Schlußweise (§§ 2, 147) geht hervor, daß das mit $\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}\,\mathfrak{d}\ldots$ zu bezeichnende Produkt aus m beliebigen Idealen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}\ldots$ eine vollständig bestimmte, von der Anordnung der sukzessiven Multiplikationen gänzlich

unabhängige Bedeutung hat*). Sind alle diese m Faktoren identisch mit dem Ideal $\mathfrak{a}$, so bezeichnen wir ihr Produkt mit $\mathfrak{a}^m$ und nennen es die m^{te} Potenz von $\mathfrak{a}$; m heißt der Exponent dieser Potenz, und wir dehnen diesen Begriff auch auf die beiden Fälle $m = 0$ und $m = 1$ aus, indem wir $\mathfrak{a}^0 = \mathfrak{o}$ und $\mathfrak{a}^1 = \mathfrak{a}$ setzen; dann gelten allgemein die Sätze $\mathfrak{a}^r \mathfrak{a}^s = \mathfrak{a}^{r+s}$ und $(\mathfrak{a}^r)^s = \mathfrak{a}^{rs}$.

Es wird nun unsere Hauptaufgabe sein, den Zusammenhang zwischen diesem Begriffe der Multiplikation und demjenigen der Teilbarkeit der Ideale vollständig zu ergründen; diese Untersuchung bietet erhebliche Schwierigkeiten dar, und wir begnügen uns für jetzt, die folgenden, äußerst einfachen Sätze zu beweisen.

1. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{a}'$, und $\mathfrak{b}$ teilbar durch $\mathfrak{b}'$, so ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}'\mathfrak{b}'$.

Denn da jede Zahl α des Ideals $\mathfrak{a}$ auch in $\mathfrak{a}'$, und jede Zahl β des Ideals $\mathfrak{b}$ auch in $\mathfrak{b}'$ enthalten ist, so ist jedes Produkt $\alpha\beta$, und folglich auch jede Summe solcher Produkte $\alpha\beta$ in $\mathfrak{a}'\mathfrak{b}'$ enthalten.

2. Das Produkt $\mathfrak{a}\mathfrak{b}$ ist ein gemeinschaftliches Vielfaches der beiden Faktoren $\mathfrak{a}$ und $\mathfrak{b}$.

Denn $\mathfrak{a}$ ist durch $\mathfrak{a}$, und $\mathfrak{b}$ ist durch $\mathfrak{o}$ teilbar, woraus (nach 1.) folgt, daß $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{a}\mathfrak{o}$, d. h. durch $\mathfrak{a}$ teilbar ist.

3. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache, und $\mathfrak{d}$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, so ist $\mathfrak{m}\mathfrak{d}$ durch $\mathfrak{a}\mathfrak{b}$ teilbar**).

Denn jede Zahl δ des Ideals $\mathfrak{d}$ ist von der Form $\alpha + \beta$, wo α in $\mathfrak{a}$, und β in $\mathfrak{b}$ enthalten ist, und jede Zahl μ des Ideals $\mathfrak{m}$ ist sowohl in $\mathfrak{b}$ als auch in $\mathfrak{a}$ enthalten, woraus folgt, daß die beiden Produkte $\alpha\mu$ und $\mu\beta$ dem Ideal $\mathfrak{a}\mathfrak{b}$ angehören; dasselbe gilt mithin auch von ihrer Summe $\mu\delta$, also auch von jeder Zahl des Ideals $\mathfrak{m}\mathfrak{d}$.

§ 171.

Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen relative Primideale, und jedes von ihnen heißt relatives Primideal zu dem anderen, wenn ihr größter gemeinschaftlicher Teiler $= \mathfrak{o}$ ist; da nun die Zahl 1 in $\mathfrak{o}$ enthalten

*) Es ist der Inbegriff aller Zahlen von der Form $\Sigma\alpha\beta\gamma\delta\ldots$, wo $\alpha, \beta, \gamma, \delta\ldots$ beliebige Zahlen bzw. der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}\ldots$ bedeuten; dies könnte auch von vornherein als Definition eines Produktes von beliebig vielen Idealen gelten.

**) Daß $\mathfrak{m}\mathfrak{d} = \mathfrak{a}\mathfrak{b}$ ist, werden wir erst später (§ 173, 9.) beweisen können.

ist, so gibt es eine Zahl α in $\mathfrak{a}$ und eine Zahl β in $\mathfrak{b}$, welche der Bedingung

$$\alpha + \beta = 1$$

genügen, und umgekehrt folgt aus der Existenz eines solchen Zahlenpaares α, β, daß $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind, weil (nach § 168, 1.) $\mathfrak{o}$ das einzige Ideal ist, welches in 1 aufgeht. Dasselbe Kriterium kann man offenbar auch so ausdrücken, daß in $\mathfrak{b}$ eine Zahl β existiert, welche der Kongruenz

$$\beta \equiv 1 \pmod{\mathfrak{a}}$$

genügt. Wir bemerken ferner ein für allemal, daß, wenn wir mehr als zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ... relative Primideale nennen, hierunter immer zu verstehen ist, daß jedes dieser Ideale relatives Primideal zu jedem der übrigen ist. Aus dieser Definition ergeben sich zunächst die folgenden Sätze.

1. Ist $\mathfrak{a}$ relatives Primideal zu $\mathfrak{b}$ und zu $\mathfrak{c}$, so ist $\mathfrak{a}$ auch relatives Primideal zu dem Produkte $\mathfrak{b}\mathfrak{c}$.

Denn es gibt in $\mathfrak{b}$, $\mathfrak{c}$ Zahlen β, γ, welche den Bedingungen $\beta \equiv 1$, $\gamma \equiv 1 \pmod{\mathfrak{a}}$ genügen, und hieraus folgt, daß die in $\mathfrak{b}\mathfrak{c}$ enthaltene Zahl $\beta\gamma \equiv 1 \pmod{\mathfrak{a}}$ ist.

2. Ist jedes der Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ ... relatives Primideal zu jedem der Ideale $\mathfrak{b}_1$, $\mathfrak{b}_2$ ..., so sind die Produkte $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$ ... und $\mathfrak{b}_1\mathfrak{b}_2$ ... relative Primideale.

Der Beweis ergibt sich durch wiederholte Anwendung des vorhergehenden Satzes (vgl. § 5, 3.).

3. Sind $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale, so ist $\mathfrak{a}\mathfrak{b}$ ihr kleinstes gemeinschaftliches Vielfaches, und $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Denn bedeutet $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$, so ist $\mathfrak{m}\mathfrak{o}$, also $\mathfrak{m}$ selbst teilbar durch $\mathfrak{a}\mathfrak{b}$ (nach § 170, 3.); da aber $\mathfrak{a}\mathfrak{b}$ (nach § 170, 2.) ein gemeinschaftliches Vielfaches von $\mathfrak{a}$, $\mathfrak{b}$, also durch $\mathfrak{m}$ teilbar ist, so ist $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$; und hieraus folgt (nach § 169, 3.) der Satz über die Normen*).

4. Sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ... relative Primideale, so ist ihr Produkt $\mathfrak{a}\mathfrak{b}\mathfrak{c}$... auch ihr kleinstes gemeinschaftliches Vielfaches, und zugleich ist $N(\mathfrak{a}\mathfrak{b}\mathfrak{c}\ldots) = N(\mathfrak{a})N(\mathfrak{b})N(\mathfrak{c})\ldots$.

*) Daß der letztere allgemein für je zwei beliebige Ideale $\mathfrak{a}$, $\mathfrak{b}$ gilt, kann erst später bewiesen werden (§ 173, 7.).

Der Beweis ergibt sich durch wiederholte Anwendung der vorhergehenden Sätze (vgl. § 7).

5. Sind $\mathfrak{a}, \mathfrak{b}$ relative Primideale, und ist $\mathfrak{b}\mathfrak{c}$ teilbar durch $\mathfrak{a}$, so geht $\mathfrak{a}$ in $\mathfrak{c}$ auf.

Denn es gibt in $\mathfrak{b}$ eine Zahl $\beta \equiv 1 \pmod{\mathfrak{a}}$; ist nun γ eine beliebige Zahl in $\mathfrak{c}$, so ist $\beta\gamma$ in $\mathfrak{b}\mathfrak{c}$, also auch in $\mathfrak{a}$ enthalten, woraus $\gamma \equiv \beta\gamma \equiv 0 \pmod{\mathfrak{a}}$ folgt, was zu beweisen war. —

Die bisher von uns entwickelten Sätze der Idealtheorie bieten eine augenscheinliche Analogie dar mit den Sätzen über die Teilbarkeit der ganzen rationalen Zahlen, und dies findet seinen natürlichen Grund darin, daß, wenn der Körper Ω vom Grade $n = 1$ ist, das Gebiet $\mathfrak{o} = [1]$ und jedes Ideal $\mathfrak{m}$ dieses Gebietes ein Modul $[m]$ ist, wo m irgendeine positive ganze rationale Zahl bedeutet (§ 165). Es liegt nun nahe, in die Theorie der Ideale auch einen Begriff einzuführen, welcher dem Begriffe der rationalen Primzahl entspricht. Das Ideal $\mathfrak{o}$ besitzt offenbar nur einen einzigen Teiler, nämlich $\mathfrak{o}$ selbst; jedes von $\mathfrak{o}$ verschiedene Ideal besitzt aber mindestens zwei verschiedene Teiler, da es außer durch $\mathfrak{o}$ auch noch durch sich selbst teilbar ist. Wir wollen nun ein Ideal $\mathfrak{p}$ ein Primideal nennen, wenn es von $\mathfrak{o}$ verschieden ist und keinen anderen Teiler als $\mathfrak{o}$ und $\mathfrak{p}$ besitzt; dagegen soll $\mathfrak{a}$ ein zusammengesetztes Ideal heißen, wenn es mindestens einen von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedenen Teiler besitzt. Hieraus fließen die folgenden Sätze.

6. Ist $\mathfrak{a}$ von $\mathfrak{o}$ verschieden, so gibt es mindestens ein in $\mathfrak{a}$ aufgehendes Primideal.

Denn wählt man unter den von $\mathfrak{o}$ verschiedenen Teilern von $\mathfrak{a}$ ein solches Ideal $\mathfrak{p}$ aus, dessen Norm den möglich kleinsten Wert hat, so kann $\mathfrak{p}$ (nach § 169, 5.) keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Teiler haben, und folglich ist $\mathfrak{p}$ ein in $\mathfrak{a}$ aufgehendes Primideal.

7. Zwei Ideale sind entweder relative Primideale, oder es gibt ein in beiden aufgehendes Primideal.

Denn ihr größter gemeinschaftlicher Teiler ist entweder $= \mathfrak{o}$, oder er ist (nach 6.) durch ein Primideal teilbar.

8. Ist $\mathfrak{p}$ ein Primideal, $\mathfrak{a}$ ein beliebiges Ideal, so findet einer und nur einer der folgenden beiden Fälle statt: entweder geht $\mathfrak{p}$ in $\mathfrak{a}$ auf, oder $\mathfrak{a}$ und $\mathfrak{p}$ sind relative Primideale.

Denn der größte gemeinschaftliche Teiler von $\mathfrak{a}, \mathfrak{p}$ ist ein Teiler von $\mathfrak{p}$, also entweder $= \mathfrak{p}$, oder $= \mathfrak{o}$.

9. Wenn ein Produkt von Idealen oder Zahlen durch das Primideal $\mathfrak{p}$ teilbar ist, so geht $\mathfrak{p}$ in mindestens einem der Faktoren auf.

Denn wenn $\mathfrak{p}$ in keinem der Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... aufgeht, so ist $\mathfrak{p}$ (nach 8.) relatives Primideal zu jedem derselben, also auch zu ihrem Produkte (nach 2.), welches folglich (nach 8.) nicht durch $\mathfrak{p}$ teilbar ist; und handelt es sich um ein Produkt aus Zahlen η, η', ..., so ergibt sich dasselbe, wenn man die entsprechenden Hauptideale $\mathfrak{o}\eta$, $\mathfrak{o}\eta'$, ... betrachtet.

10. Ist $\mathfrak{p}$ ein Primideal, so gibt es im Körper der rationalen Zahlen eine und nur eine positive Primzahl p, welche durch $\mathfrak{p}$ teilbar ist; zugleich ist $N(\mathfrak{p}) = p^f$, und der Exponent f soll der Grad des Primideals $\mathfrak{p}$ heißen.

Denn die durch $\mathfrak{p}$ teilbaren ganzen rationalen Zahlen, zu denen (nach § 169, 1.) auch $N(\mathfrak{p})$ gehört, bilden offenbar einen Modul, und wenn p die kleinste positive dieser Zahlen bedeutet, so ist dieser Modul $= [p]$ [nach § 165, (8)]; nun kann p nicht $= 1$ sein, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre (nach § 168, 1.), und p kann auch nicht ein Produkt aus zwei kleineren rationalen Zahlen sein, weil sonst eine von beiden (nach 9.) durch $\mathfrak{p}$ teilbar sein müßte, was gegen die Definition von p verstoßen würde; mithin ist p eine Primzahl im Körper der rationalen Zahlen, und es kann keine andere solche Primzahl durch $\mathfrak{p}$ teilbar sein, weil $[p]$ der Inbegriff aller durch $\mathfrak{p}$ teilbaren rationalen Zahlen ist. Da nun $\mathfrak{o}p$ durch $\mathfrak{p}$, und folglich $N(\mathfrak{o}p)$, d. h. p^n durch $N(\mathfrak{p})$ teilbar ist (§ 169, 5.), so folgt, daß $N(\mathfrak{p})$ selbst eine Potenz von p ist.

11. Ist $\mathfrak{a}$ ein zusammengesetztes Ideal, so gibt es zwei durch $\mathfrak{a}$ nicht teilbare Zahlen η, η', deren Produkt durch $\mathfrak{a}$ teilbar ist.

Denn $\mathfrak{a}$ besitzt einen von $\mathfrak{o}$ und $\mathfrak{a}$ verschiedenen Teiler $\mathfrak{e}$, und da derselbe nicht durch $\mathfrak{a}$ teilbar ist, so gibt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η; der größte gemeinschaftliche Teiler $\mathfrak{d}$ der beiden Ideale $\mathfrak{a}$ und $\mathfrak{o}\eta$ ist teilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, und folglich ist $N(\mathfrak{d}) > 1$ (nach § 169, 2.). Nun sei $\mathfrak{a}'\eta$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\eta$, so ist $\mathfrak{a}'$ ein Teiler von $\mathfrak{a}$, und zugleich ist (nach § 169, 4.) $N(\mathfrak{a}) = N(\mathfrak{a}')N(\mathfrak{d}) > N(\mathfrak{a}')$; mithin ist $\mathfrak{a}'$ ein echter Teiler von $\mathfrak{a}$, und es gibt folglich in $\mathfrak{a}'$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η'; dann ist das Produkt $\eta\eta'$ in $\eta\mathfrak{a}'$ und folglich auch in $\mathfrak{a}$ enthalten, was zu beweisen war.

12. Ist $\mathfrak{a}$ teilbar durch das Primideal $\mathfrak{p}$, so kann man die Zahl ν so wählen, daß $\mathfrak{p}^\nu$ das kleinste gemeinschaftliche Vielfache der beiden Ideale $\mathfrak{a}$ und $\mathfrak{o}\nu$ wird.

Der Beweis dieses einfachen, aber für unsere Theorie äußerst wichtigen Satzes*) ist mit einigen Schwierigkeiten verknüpft, die sich jedoch durch die folgende Kette von Schlüssen überwinden lassen. Zunächst leuchtet die Richtigkeit des Satzes ein, wenn $(\mathfrak{p}, \mathfrak{a}) = 1$, also $\mathfrak{a} = \mathfrak{p}$ ist, weil in diesem Falle die Zahl $\nu = 1$ die verlangte Eigenschaft besitzt. Es sei nun m irgendeine ganze rationale Zahl > 1, und wir wollen annehmen, der Satz sei schon für alle die Fälle bewiesen, in welchen $(\mathfrak{p}, \mathfrak{a}) < m$ ist, so brauchen wir offenbar nur noch zu zeigen, daß hieraus immer seine Richtigkeit auch für den Fall $(\mathfrak{p}, \mathfrak{a}) = m$ folgt. Zu diesem Zweck wollen wir wieder, wenn η eine von Null verschiedene Zahl ist, mit $\mathfrak{b}$ den größten gemeinschaftlichen Teiler, mit $\mathfrak{a}'\eta$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{a}, \mathfrak{o}\eta$ bezeichnen; dann ist $\mathfrak{a}'$ ein Teiler von $\mathfrak{a}$, und zugleich ist $N(\mathfrak{a}) = N(\mathfrak{a}')N(\mathfrak{b})$. Ist nun $(\mathfrak{p}, \mathfrak{a}) = m > 1$, also $\mathfrak{p}$ ein echter Teiler von $\mathfrak{a}$, so wollen wir zunächst zeigen, daß man durch geeignete Wahl der Zahl η ein zugehöriges Ideal $\mathfrak{a}'$ erhalten kann, welches erstens durch $\mathfrak{p}$ teilbar und zweitens ein echter Teiler von $\mathfrak{a}$ ist; die letztere Forderung kommt offenbar darauf hinaus, daß $\mathfrak{b}$ von $\mathfrak{o}$ verschieden, also $N(\mathfrak{b}) > 1$, $N(\mathfrak{a}') < N(\mathfrak{a})$ werde. Um diesen Existenzbeweis zu führen, müssen wir zwei Fälle unterscheiden:

a) Wenn $\mathfrak{p}$ das einzige in $\mathfrak{a}$ aufgehende Primideal ist, so wähle man für η eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{a}$ teilbare Zahl, was stets möglich ist, weil $\mathfrak{p}$ ein echter Teiler von $\mathfrak{a}$, also nicht durch $\mathfrak{a}$ teilbar ist. Da nun $\mathfrak{o}\eta$, und folglich auch $\mathfrak{b}$ durch $\mathfrak{p}$ teilbar ist, so ist $N(\mathfrak{b}) > 1$, also $\mathfrak{a}'$ ein echter Teiler von $\mathfrak{a}$. Da ferner $\mathfrak{o}\eta$ nicht durch $\mathfrak{a}$ teilbar ist, so kann $\mathfrak{a}'$ nicht $= \mathfrak{o}$ sein, und folglich gibt es (nach 6.) ein in $\mathfrak{a}'$ aufgehendes Primideal $\mathfrak{q}$; da aber $\mathfrak{a}'$ ein Teiler von $\mathfrak{a}$ ist, so geht $\mathfrak{q}$ auch in $\mathfrak{a}$ auf und ist folglich $= \mathfrak{p}$; mithin ist $\mathfrak{a}'$ teilbar durch $\mathfrak{p}$, was zu zeigen war.

*) Derselbe läßt sich, ohne an Inhalt wesentlich zu gewinnen oder zu verlieren, in sehr verschiedenen Formen ausdrücken; so z. B. ergibt sich aus ihm ohne Zuziehung neuer Beweismittel der folgende Satz: Wenn $\mathfrak{a}$, $\mathfrak{b}$ nicht relative Primideale sind, so gibt es ein durch $\mathfrak{a}$ nicht teilbares Ideal $\mathfrak{c}$ von der Art, daß $\mathfrak{bc}$ durch $\mathfrak{a}$ teilbar wird (vgl. § 171, 5.). Umgekehrt folgt der obige Satz ebenso leicht aus diesem letzteren, der aber, trotz seiner scheinbaren Evidenz, schwerlich einen einfacheren direkten Beweis gestattet.

b) Wenn $\mathfrak{a}$ durch ein von $\mathfrak{p}$ verschiedenes Primideal $\mathfrak{q}$ teilbar ist, so wähle man für η eine durch $\mathfrak{q}$, aber nicht durch $\mathfrak{p}$ teilbare Zahl, was stets möglich ist, weil $\mathfrak{q}$ nicht durch $\mathfrak{p}$ teilbar ist. Da nun $\mathfrak{o}\eta$, und folglich auch $\mathfrak{b}$ durch $\mathfrak{q}$ teilbar ist, so ist $N(\mathfrak{b}) > 1$, also $\mathfrak{a}'$ ein echter Teiler von $\mathfrak{a}$. Da ferner $\mathfrak{a}'\eta$ durch $\mathfrak{a}$ und folglich auch durch $\mathfrak{p}$ teilbar ist, während $\mathfrak{p}$ in dem Faktor η nicht aufgeht, so ist (nach 9.) das Ideal $\mathfrak{a}'$ teilbar durch $\mathfrak{p}$, was zu zeigen war.

Hiermit ist die Existenz einer solchen Zahl η in allen Fällen nachgewiesen. Da nun das zugehörige Ideal $\mathfrak{a}'$ durch $\mathfrak{p}$ teilbar und zugleich ein echter Teiler von $\mathfrak{a}$ ist, so ist $m = (\mathfrak{p}, \mathfrak{a}) = (\mathfrak{p}, \mathfrak{a}')(\mathfrak{a}', \mathfrak{a})$, und $(\mathfrak{a}', \mathfrak{a}) > 1$, also $(\mathfrak{p}, \mathfrak{a}') < m$; mithin gibt es nach unserer obigen Annahme eine Zahl η' von der Art, daß $\mathfrak{p}\eta'$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{a}', \mathfrak{o}\eta'$ ist, und da $\mathfrak{a}'\eta$ dasjenige der Ideale $\mathfrak{a}, \mathfrak{o}\eta$ ist, so folgt (nach § 168, 4.), daß $\mathfrak{p}\eta\eta'$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{a}$ und $\mathfrak{o}\eta\eta'$ ist; mithin hat die Zahl $\nu = \eta\eta'$ die in unserem Satze verlangte Eigenschaft.

§ 172.

Man würde nun unsere bisherige Untersuchung auch ohne Zuziehung neuer Hilfsmittel noch einige Schritte weiterführen und z. B. den folgenden Satz beweisen können, in welchem unter einem einartigen Ideal ein solches verstanden wird, welches durch ein und nur durch ein einziges Primideal teilbar ist*):

13. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist entweder einartiges Ideal, oder es läßt sich, und zwar nur auf eine einzige Weise, als ein Produkt von lauter einartigen Idealen darstellen, die zugleich relative Primideale sind.

Es sei $\mathfrak{p}$ ein in $\mathfrak{a}$ aufgehendes Primideal, und $\mathfrak{p}'$ das kleinste gemeinschaftliche Vielfache aller in $\mathfrak{a}$ aufgehenden, durch $\mathfrak{p}$ teilbaren einartigen Ideale $\mathfrak{e}$, zu denen auch $\mathfrak{p}$ gehört, so ist $\mathfrak{p}'$ offenbar selbst eins der Ideale $\mathfrak{e}$; denn $\mathfrak{p}'$ geht in $\mathfrak{a}$ auf, weil $\mathfrak{a}$ ein gemeinschaftliches Vielfaches dieser Ideale $\mathfrak{e}$ ist, und $\mathfrak{p}'$ ist nur durch das einzige Primideal $\mathfrak{p}$ teilbar, weil selbst das durch $\mathfrak{p}'$ teilbare Produkt aller Ideale $\mathfrak{e}$ (nach 9.) durch kein von $\mathfrak{p}$ verschiedenes Primideal teilbar sein kann. Es sei ferner $\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache aller der-

*) [Im Nachlaß fand sich das Manuskript der dritten Auflage, wobei die beiden Seiten mit dem Beweis dieses Satzes die Überschrift trugen: „Für die dritte Auflage kassiert, doch wichtig.“ Der Beweis soll hier eingeschaltet werden, als erstes explizites Beispiel eines Zerlegungssatzes der allgemeinen Idealtheorie. E. N.]

jenigen in $\mathfrak{a}$ aufgehenden Ideale $\mathfrak{q}$, welche, wie z. B. $\mathfrak{o}$, nicht durch $\mathfrak{p}$ teilbar sind, so ergibt sich auf dieselbe Weise, daß $\mathfrak{b}$ selbst eins dieser Ideale $\mathfrak{q}$ ist. Offenbar sind $\mathfrak{p}'$ und $\mathfrak{b}$ relative Primideale. Wir wollen uns nun begnügen, zu beweisen, daß $\mathfrak{a} = \mathfrak{p}'\mathfrak{b}$ ist, weil der Leser hieraus alles Übrige mit Hilfe der früheren Sätze leicht ableiten wird. Man wähle nach Belieben eine durch $\mathfrak{b}$, aber nicht durch $\mathfrak{p}$ teilbare Zahl η (was möglich ist, weil $\mathfrak{b}$ nicht durch $\mathfrak{p}$ teilbar ist), so wird $\mathfrak{b}$ immer der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{o}\eta$ sein; denn jeder gemeinschaftliche Teiler dieser Ideale ist offenbar eins der Ideale $\mathfrak{q}$, mithin ein Teiler von $\mathfrak{b}$, und außerdem ist $\mathfrak{b}$ selbst ein solcher gemeinschaftlicher Teiler. Es sei nun $\mathfrak{r}\eta$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\eta$, so ist $\mathfrak{r}$ ein Teiler von $\mathfrak{a}$ und (nach § 169, 4.)

$$N(\mathfrak{a}) = N(\mathfrak{r}) \cdot N(\mathfrak{b}).$$

Die Zahl η^2 ist ebenfalls, wie η, durch $\mathfrak{b}$, aber nicht durch $\mathfrak{p}$ teilbar, mithin haben die beiden Ideale $\mathfrak{a}$, $\mathfrak{o}\eta^2$ denselben größten gemeinschaftlichen Teiler $\mathfrak{b}$ wie die Ideale $\mathfrak{a}$, $\mathfrak{o}\eta$; hieraus folgt (nach § 168, 4.), daß $\mathfrak{r}\eta^2$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{o}\eta^2$, mithin $\mathfrak{r}\eta$ dasjenige der Ideale $\mathfrak{r}$, $\mathfrak{o}\eta$ ist; bedeutet aber $\mathfrak{b}'$ den größten gemeinschaftlichen Teiler dieser beiden Ideale, so ist (nach § 169, 4.) $N(\mathfrak{r}) = N(\mathfrak{r})N(\mathfrak{b}')$, also $N(\mathfrak{b}') = 1$, $\mathfrak{b}' = \mathfrak{o}$. Es ist daher $\mathfrak{r}$ relatives Primideal zu dem Hauptideal $\mathfrak{o}\eta$ und folglich auch zu dessen Teiler $\mathfrak{b}$; mithin ist $\mathfrak{r}\mathfrak{b}$ (nach 3.) das kleinste gemeinschaftliche Vielfache von $\mathfrak{r}$ und $\mathfrak{b}$, und $N(\mathfrak{r}\mathfrak{b}) = N(\mathfrak{r}) \cdot N(\mathfrak{b})$, also $N(\mathfrak{r}\mathfrak{b}) = N(\mathfrak{a})$; da aber $\mathfrak{a}$ ein gemeinschaftliches Vielfaches von $\mathfrak{r}$ und $\mathfrak{b}$, mithin durch $\mathfrak{r}\mathfrak{b}$ teilbar ist, so folgt aus der Gleichheit der Normen (nach § 169, 5.), daß

$$\mathfrak{a} = \mathfrak{r}\mathfrak{b}$$

ist. Wir haben nun noch zu zeigen, daß $\mathfrak{r} = \mathfrak{p}'$ ist; zunächst leuchtet ein, daß das Ideal $\mathfrak{p}'$, weil es in $\mathfrak{r}\mathfrak{b}$ aufgeht, zugleich aber relatives Primideal zu $\mathfrak{b}$ ist, in $\mathfrak{r}$ aufgehen muß; wäre ferner $\mathfrak{r}$ durch ein von $\mathfrak{p}$ verschiedenes Primideal teilbar, so müßte letzteres auch in $\mathfrak{a}$ aufgehen, es wäre folglich eins der Ideale $\mathfrak{q}$ und ginge folglich in $\mathfrak{b}$ auf, was nicht möglich ist, weil $\mathfrak{r}$ und $\mathfrak{b}$ relative Primideale sind; hieraus folgt offenbar, daß $\mathfrak{r}$ eins der Ideale $\mathfrak{e}$ ist und daher in $\mathfrak{p}'$ aufgeht. Also ist $\mathfrak{r} = \mathfrak{p}'$, was wir zeigen wollten.

Indessen ist dieser Satz, den wir später (§ 173, 4.) doch durch einen noch schärferen zu ersetzen haben werden, für unsere Zwecke nicht erforderlich, und wir haben ihn nur erwähnt, um zu zeigen,

wie weit man mit den bisherigen Beweismitteln gelangen kann. Bei einer sorgfältigen Prüfung der letzteren und der durch sie gewonnenen Resultate ergibt sich nun folgendes.

So augenfällig auch die Analogie zwischen den vorhergehenden Sätzen und denjenigen über die Teilbarkeit der ganzen rationalen Zahlen ist, so kann dieselbe bis jetzt doch keineswegs eine vollständige genannt werden. Man darf nicht vergessen, daß die Teilbarkeit eines Ideals $\mathfrak{c}$ durch ein Ideal $\mathfrak{a}$ nach unserer Definition (§§ 165, 168) lediglich darin besteht, daß alle Zahlen des Ideals $\mathfrak{c}$ auch in $\mathfrak{a}$ enthalten sind; nun ergab sich zwar sehr leicht (§ 170, 2.), daß jedes Produkt aus $\mathfrak{a}$ und einem beliebigen Ideal $\mathfrak{b}$ stets durch $\mathfrak{a}$ teilbar ist, aber es ist keineswegs leicht zu beweisen, daß umgekehrt jedes durch $\mathfrak{a}$ teilbare Ideal $\mathfrak{c}$ auch ein Produkt aus $\mathfrak{a}$ und einem Ideal $\mathfrak{b}$ ist. Diese Schwierigkeit läßt sich auch mit den bisher von uns gebrauchten Beweismitteln allein durchaus nicht überwinden, und wir müssen den Grund dieser Tatsache hier etwas näher erörtern, weil dieselbe mit einer sehr wichtigen Verallgemeinerung der Theorie zusammenhängt. Bei einer genauen Prüfung der bisher entwickelten Theorie wird man sich leicht davon überzeugen, daß alle Definitionen einen bestimmten Sinn und die Beweise aller Sätze ihre volle Kraft behalten, auch wenn nicht vorausgesetzt wird, daß das mit $\mathfrak{o}$ bezeichnete Gebiet alle ganzen Zahlen des Körpers Ω umfaßt. Die wirklich benutzten Eigenschaften des Systems $\mathfrak{o}$ kommen vielmehr auf die folgenden zurück:

a) Das System $\mathfrak{o}$ ist ein endlicher Modul $[\omega_1, \omega_2, \ldots, \omega_n]$, dessen Basis zugleich eine Basis des Körpers Ω bildet (§ 162).

b) Jedes Produkt aus zwei Zahlen des Systems $\mathfrak{o}$ gehört demselben System $\mathfrak{o}$ an.

c) Die Zahl 1 ist in $\mathfrak{o}$ enthalten.

Ein Gebiet $\mathfrak{o}$, welches diese drei Eigenschaften besitzt, wollen wir eine Ordnung nennen. Aus der Verbindung von a) und b) folgt unmittelbar, daß eine Ordnung $\mathfrak{o}$ nur aus ganzen Zahlen des Körpers Ω besteht, und zufolge c) sind auch alle ganzen rationalen Zahlen in $\mathfrak{o}$ enthalten; aber hieraus folgt noch nicht (ausgenommen im Fall $n = 1$), daß $\mathfrak{o}$ alle ganzen Zahlen des Körpers Ω enthält. Nennt man nun eine Zahl α der Ordnung $\mathfrak{o}$ nur dann teilbar durch eine zweite solche Zahl μ, wenn $\alpha = \mu\nu$ ist, wo ν ebenfalls eine Zahl

in $\mathfrak{o}$ bedeutet (vgl. § 167), und modifiziert man in derselben Weise den Begriff der Kongruenz der Zahlen innerhalb des Gebietes $\mathfrak{o}$, so leuchtet unmittelbar ein, daß die Anzahl $(\mathfrak{o}, \mathfrak{o}\mu)$ der in bezug auf μ inkongruenten Zahlen der Ordnung $\mathfrak{o}$ auch jetzt $= \pm N(\mu)$ ist [§ 167, (9)], und ebenso leicht wird man erkennen, daß alle später entwickelten Begriffe und Sätze ihren Sinn und ihre Geltung behalten, wenn unter einer Zahl stets eine Zahl dieser Ordnung $\mathfrak{o}$ verstanden wird. In jeder Ordnung $\mathfrak{o}$ des Körpers Ω existiert daher eine besondere Theorie der Ideale, und diese Theorie ist für alle Ordnungen eine gemeinsame, soweit sie im vorhergehenden entwickelt ist. Aber während die Theorie der Ideale in derjenigen Ordnung $\mathfrak{o}$, welche aus allen ganzen Zahlen des Körpers Ω besteht, schließlich (§ 173) zu allgemeinen Gesetzen führen wird, welche keine Ausnahme erleiden und vollständig mit den Gesetzen der Teilbarkeit der rationalen Zahlen übereinstimmen, so ist die Theorie der Ideale jeder anderen Ordnung nicht von gleicher Einfachheit, insofern eine (immer endliche) Anzahl von Primidealen existiert, aus welchen sich die zugehörigen einartigen Ideale nicht alle durch Potenzierung bilden lassen. Diese allgemeinste Theorie der Ideale jeder Ordnung, deren Entwicklung für die Ziele der Zahlentheorie ebenfalls unerläßlich ist, und welche für den Fall $n = 2$ mit der Theorie der verschiedenen Ordnungen der binären quadratischen Formen zusammenfällt (§ 61), soll aber im folgenden von unserer Betrachtung gänzlich ausgeschlossen bleiben*), und wir wollen uns begnügen, an einem Beispiel auf den Charakter der oben erwähnten Ausnahmen aufmerksam zu machen.

Das Gebiet $\mathfrak{o}$ aller ganzen Zahlen desjenigen quadratischen Körpers, dessen Grundzahl $= -3$, ist $= [1, \theta]$, wo θ eine Wurzel der Gleichung $\theta^2 + \theta + 1 = 0$ bedeutet (§ 166). Das System $\mathfrak{o}' = [1, 2\theta] = [1, \sqrt{-3}]$ ist eine Ordnung, welche nicht alle ganzen Zahlen des Körpers enthält, weil $(\mathfrak{o}, \mathfrak{o}') = 2$ ist (§ 165); die durch $\mathfrak{o}'$ teilbaren Moduln $\mathfrak{p}' = [2, 2\theta] = \mathfrak{o}(2)$ und $\mathfrak{o}'(2) = [2, 4\theta]$ sind Ideale dieser Ordnung $\mathfrak{o}'$ (insofern sie die Eigenschaften I. und II. besitzen); aber obgleich $\mathfrak{o}'(2)$ durch $\mathfrak{p}'$ teilbar ist, so existiert in $\mathfrak{o}'$ doch kein Ideal $\mathfrak{q}'$ von der Art, daß $\mathfrak{p}'\mathfrak{q}' = \mathfrak{o}'(2)$ würde. —

*) In einem gewissen Umfange ist diese Theorie behandelt in des Herausgebers Abhandlung: Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877).

Um nun die Theorie der Ideale in derjenigen Ordnung $\mathfrak{o}$, welche alle ganzen Zahlen des Körpers Ω umfaßt, zum vollständigen Abschlusse zu bringen, bedürfen wir der folgenden Hilfssätze:

1. Ist μ eine von Null verschiedene ganze, und φ eine gebrochene, d. h. nicht ganze Zahl des Körpers Ω*), so sind alle Glieder der geometrischen Reihe

$$\mu,\ \mu\varphi,\ \mu\varphi^2,\ \ldots,\ \mu\varphi^e,\ \mu\varphi^{e+1},\ \ldots$$

bis zu einem in endlicher Entfernung liegenden Gliede $\mu\varphi^e$ ganze Zahlen, und alle folgenden Glieder sind gebrochene Zahlen.

Zum Beweise bemerken wir zunächst, daß alle Glieder der Reihe in Ω enthalten sind, und daß das Anfangsglied eine ganze Zahl ist. Bedeutet nun m den absoluten Wert von $N(\mu)$, so können höchstens m Glieder ganze Zahlen, also in $\mathfrak{o}$ enthalten sein; wären nämlich mindestens $(m+1)$ Glieder ganze Zahlen, so müßten unter ihnen [nach § 167, (9)] mindestens zwei verschiedene einander kongruent sein nach dem Modul μ; bezeichnet man dieselben mit $\mu\varphi^s$ und $\mu\varphi^r$, wo $r > s$, so wäre $\mu\varphi^r \equiv \mu\varphi^s \pmod{\mu}$, und folglich würde die gebrochene Zahl φ einer Gleichung r^{ten} Grades von der Form

$$\varphi^r - \varphi^s - \omega = 0$$

genügen, wo ω eine ganze Zahl, was (nach § 160, 2.) unmöglich ist. Von einer bestimmten Stelle ab werden daher alle Glieder der Reihe gewiß gebrochene Zahlen sein; ist nun

$$\mu\varphi^e = \varkappa$$

die letzte in der Reihe auftretende ganze Zahl, so ist e ein endlicher Exponent $\geqq 0$; ist $e > 0$, so sind alle vorhergehenden Glieder ebenfalls ganze Zahlen; denn wenn $r < e$, so ist

$$(\mu\varphi^r)^e = \mu^{e-r}\varkappa^r$$

eine ganze Zahl, und hieraus folgt (nach § 160, 2.), daß auch $\mu\varphi^r$ eine ganze Zahl ist, was zu beweisen war.

2. Sind μ, ν zwei von Null verschiedene Zahlen in $\mathfrak{o}$, und ist ν nicht teilbar durch μ, so gibt es in $\mathfrak{o}$ immer zwei von Null verschiedene Zahlen $\varkappa, \lambda$ von der Art, daß $\varkappa\mu = \lambda\nu$, und daß $\varkappa^2$ nicht durch λ teilbar ist.

*) Da, wenn μ, φ irgendwelche algebraische Zahlen sind, sich immer leicht die Existenz eines endlichen Körpers Ω nachweisen läßt, welchem beide Zahlen angehören, so gilt der obige Satz allgemein, und ebenso der folgende Satz.

Dies folgt unmittelbar aus dem vorhergehenden Satze; denn wenn man $\nu = \mu\varphi$ setzt, so ist φ eine gebrochene Zahl des Körpers Ω, und von den Gliedern der Reihe

$$\mu,\ \mu\varphi,\ \mu\varphi^2,\ \ldots$$

sind die beiden ersten in $\mathfrak{o}$ enthalten; bezeichnet man nun (wie in 1.) die beiden letzten Glieder der Reihe, welche ganze Zahlen, also in $\mathfrak{o}$ enthalten sind, mit

$$\lambda = \mu\varphi^{e-1},\quad \varkappa = \mu\varphi^e,$$

so ist offenbar $\varkappa\mu = \lambda\nu$, und da das nächstfolgende Glied

$$\mu\varphi^{e+1} = \frac{\varkappa^2}{\lambda}$$

eine gebrochene Zahl ist, so kann $\varkappa^2$ nicht durch λ teilbar sein, was zu beweisen war.

§ 173.

Mit Hilfe dieser Sätze ist es leicht, die Theorie der Ideale unseres Gebietes $\mathfrak{o}$ zu dem gewünschten Abschluß zu bringen; dies geschieht durch die folgende Reihe von Sätzen.

1. Ist $\mathfrak{p}$ ein Primideal, so gibt es eine durch $\mathfrak{p}$ teilbare Zahl λ und eine durch $\mathfrak{p}$ nicht teilbare Zahl $\varkappa$ von der Art, daß $\mathfrak{p}\varkappa$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{o}\lambda$ und $\mathfrak{o}\varkappa$ ist.

Denn es sei μ eine beliebige, aber von Null verschiedene Zahl in $\mathfrak{p}$, so gibt es, weil $\mathfrak{o}\mu$ durch $\mathfrak{p}$ teilbar ist, eine Zahl ν von der Art, daß $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$ wird (§ 171, 12.); diese Zahl ν kann nicht durch μ teilbar sein, weil sonst $\mathfrak{o}\nu$, und nicht $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$ wäre. Man kann daher (nach § 172, 2.) die beiden Zahlen $\varkappa, \lambda$ so wählen, daß $\varkappa\mu = \lambda\nu$, und $\varkappa^2$ nicht durch λ teilbar wird; dann ist (nach § 165) $\mathfrak{p}\nu\varkappa$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\mu\varkappa$ und $\mathfrak{o}\nu\varkappa$, und da das erste dieser beiden Ideale $= \mathfrak{o}\lambda\nu$ ist, so folgt durch Division mit ν (nach § 165), daß $\mathfrak{p}\varkappa$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\lambda$ und $\mathfrak{o}\varkappa$ ist; mithin ist $\mathfrak{p}$ ein Teiler von $\mathfrak{o}\lambda$ (nach § 168, 4.), d. h. λ ist teilbar durch $\mathfrak{p}$; aber $\varkappa$ ist nicht teilbar durch $\mathfrak{p}$, weil sonst $\varkappa^2$ durch $\mathfrak{p}\varkappa$, also auch durch λ teilbar wäre, was nicht der Fall ist.

2. Jedes Primideal $\mathfrak{p}$ kann durch Multiplikation mit einem geeignet gewählten Ideal $\mathfrak{b}$ in ein Hauptideal $\mathfrak{o}\lambda = \mathfrak{p}\mathfrak{b}$ verwandelt werden.

Denn behalten $\varkappa$, λ dieselbe Bedeutung wie im vorhergehenden Satze, und bezeichnet man mit $\mathfrak{d}$ den größten gemeinschaftlichen Teiler von $\mathfrak{o}\lambda$, $\mathfrak{o}\varkappa$, so ist (nach § 170, 3.) das Produkt $\mathfrak{p}\varkappa\mathfrak{d}$ durch das Produkt $\mathfrak{o}\lambda\varkappa$, und folglich $\mathfrak{p}\mathfrak{d}$ durch $\mathfrak{o}\lambda$ teilbar (§ 165). Da aber $\varkappa$ nicht durch $\mathfrak{p}$ teilbar ist, so ist $\mathfrak{p}$ (nach § 171, 8.) relatives Primideal zu dem Ideal $\mathfrak{o}\varkappa$ und folglich auch zu dessen Teiler $\mathfrak{d}$, mithin ist (nach § 171, 3.) $\mathfrak{p}\mathfrak{d}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{p}$ und $\mathfrak{d}$, und da λ durch diese beiden Ideale teilbar ist, so muß $\mathfrak{o}\lambda$ auch durch $\mathfrak{p}\mathfrak{d}$ teilbar sein. Mithin ist $\mathfrak{p}\mathfrak{d} = \mathfrak{o}\lambda$, was zu beweisen war.

3. Ist das Ideal $\mathfrak{a}$ teilbar durch das Primideal $\mathfrak{p}$, so gibt es ein und nur ein Ideal $\mathfrak{q}$ von der Art, daß $\mathfrak{p}\mathfrak{q} = \mathfrak{a}$ wird; dieses Ideal $\mathfrak{q}$ ist ein echter Teiler von $\mathfrak{a}$, und folglich ist $N(\mathfrak{q}) < N(\mathfrak{a})$.

Denn wählt man (nach 2.) ein Ideal $\mathfrak{b}$ so, daß $\mathfrak{p}\mathfrak{b} = \mathfrak{o}\lambda$ wird, so muß $\mathfrak{a}\mathfrak{b}$ (nach § 170, 1.) durch $\mathfrak{p}\mathfrak{b}$, also durch λ teilbar sein, weil $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar ist, und folglich ist $\mathfrak{a}\mathfrak{b} = \lambda\mathfrak{q}$, wo $\mathfrak{q}$ ein bestimmtes Ideal bedeutet (§ 168). Multipliziert man diese Gleichung mit $\mathfrak{p}$, so ergibt sich $\lambda\mathfrak{a} = \lambda\mathfrak{p}\mathfrak{q}$, also $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$. Genügt nun das Ideal $\mathfrak{r}$ ebenfalls der Bedingung $\mathfrak{p}\mathfrak{r} = \mathfrak{a}$, so ist $\mathfrak{p}\mathfrak{r} = \mathfrak{p}\mathfrak{q}$; durch Multiplikation mit $\mathfrak{b}$ folgt hieraus $\lambda\mathfrak{r} = \lambda\mathfrak{q}$, also ist $\mathfrak{r} = \mathfrak{q}$ (§ 165). Man kann ferner (nach § 171, 12.) die Zahl ν so wählen, daß $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\nu$ wird; da nun $\mathfrak{p}\nu$ durch $\mathfrak{a}$, also durch $\mathfrak{p}\mathfrak{q}$ teilbar ist, so ergibt sich (nach § 170, 1.) durch Multiplikation mit $\mathfrak{b}$, daß $\lambda\nu$ durch $\lambda\mathfrak{q}$, also die Zahl ν durch $\mathfrak{q}$ teilbar ist; aber ν ist gewiß nicht teilbar durch $\mathfrak{a}$, weil sonst $\mathfrak{o}\nu$, und nicht $\mathfrak{p}\nu$, das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\nu$ wäre. Da also ν teilbar durch $\mathfrak{q}$, aber nicht teilbar durch $\mathfrak{a}$ ist, so ist das Ideal $\mathfrak{q}$, welches offenbar in $\mathfrak{a}$ aufgeht, verschieden von $\mathfrak{a}$, also ein echter Teiler von $\mathfrak{a}$, was zu beweisen war.

4. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist entweder ein Primideal, oder es läßt sich, und zwar nur auf eine einzige Weise, als Produkt von lauter Primidealen darstellen.

Da $\mathfrak{a}$ von $\mathfrak{o}$ verschieden ist, so gibt es (nach § 171, 6.) ein in $\mathfrak{a}$ aufgehendes Primideal $\mathfrak{p}_1$, und folglich kann man (nach 3.) $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$ setzen, wo $N(\mathfrak{a}_1) < N(\mathfrak{a})$ ist. Wenn $N(\mathfrak{a}_1) = 1$, also $\mathfrak{a}_1 = \mathfrak{o}$ ist, so ergibt sich $\mathfrak{a} = \mathfrak{p}_1$; ist aber $N(\mathfrak{a}_1) > 1$, also $\mathfrak{a}_1$ von $\mathfrak{o}$ verschieden, so kann man wieder $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$ setzen, wo $\mathfrak{p}_2$ ein Primideal und $N(\mathfrak{a}_2) < N(\mathfrak{a}_1)$ ist. Wenn $N(\mathfrak{a}_2) > 1$ ist, so kann man in derselben

Weise fortfahren, bis unter den Idealen $a_1, a_2, \ldots$ das Ideal $o = a_r$ auftritt, was nach einer endlichen Anzahl von Zerlegungen geschehen muß, weil die Normen dieser Ideale immer kleiner werden. Auf diese Weise erhält man

$$a = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r,$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ sämtlich Primideale sind. Ist nun zugleich

$$a = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_s,$$

wo $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_s$ ebenfalls Primideale bedeuten, so geht $\mathfrak{q}_1$ in a, also in dem Produkte der r Ideale $\mathfrak{p}$, und folglich (nach § 171, 9.) auch in einem der Faktoren $\mathfrak{p}$, z. B. in $\mathfrak{p}_1$ auf; da aber $\mathfrak{p}_1$ als Primideal keinen anderen Teiler als o und $\mathfrak{p}_1$ besitzt, so muß $\mathfrak{q}_1 = \mathfrak{p}_1$ sein. Es ist daher

$$\mathfrak{p}_1 (\mathfrak{p}_2 \ldots \mathfrak{p}_r) = \mathfrak{p}_1 (\mathfrak{q}_2 \ldots \mathfrak{q}_s),$$

und hieraus folgt (nach 3.)

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r = \mathfrak{q}_2 \ldots \mathfrak{q}_s.$$

Offenbar kann man in derselben Weise fortfahren (vgl. § 8), und man gelangt so zu dem Resultat, daß jedes Primideal, welches in dem einen Produkte einmal oder öfter als Faktor auftritt, genau ebenso oft in dem anderen Produkte als Faktor auftreten muß.

5. Jedes Ideal a kann durch Multiplikation mit einem passend gewählten Ideal m in ein Hauptideal $am = o\mu$ verwandelt werden.

Denn man setze a (nach 4.) in die Form $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r$, so lassen sich die Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ (nach 2.) durch Multiplikation in Hauptideale $\mathfrak{p}_1 \mathfrak{b}_1 = o\lambda_1, \mathfrak{p}_2 \mathfrak{b}_2 = o\lambda_2 \ldots \mathfrak{p}_r \mathfrak{b}_r = o\lambda_r$ verwandeln; setzt man nun $\mathfrak{b}_1 \mathfrak{b}_2 \ldots \mathfrak{b}_r = m$, $\lambda_1 \lambda_2 \ldots \lambda_r = \mu$, so wird $am = o\mu$, was zu beweisen war.

6. Ist das Ideal c teilbar durch das Ideal a, so gibt es ein und nur ein Ideal b, welches der Bedingung $ab = c$ genügt. — Ist ab teilbar durch ab', so ist b teilbar durch b', und aus $ab = ab'$ folgt $b = b'$.

Denn wenn c durch a teilbar, und m ein beliebiges Ideal ist, so ist (nach § 170, 1.) cm teilbar durch am; wählt man daher (nach 5.) das Ideal m so, daß am ein Hauptideal $o\mu$ wird, so ist (nach § 168) $cm = b\mu$, wo b ein bestimmtes Ideal bedeutet; hieraus folgt, wenn man mit a multipliziert, $c\mu = ab\mu$, also $c = ab$. — Sind ferner a, b, b' beliebige Ideale, und nehmen wir an, es sei ab teilbar durch ab', so folgt durch Multiplikation mit m, daß $b\mu$ durch $b'\mu$, also b durch b' teilbar ist. Und wenn $ab = ab'$ ist, so muß jedes

der Ideale $\mathfrak{b}, \mathfrak{b}'$ durch das andere teilbar, folglich $\mathfrak{b} = \mathfrak{b}'$ sein, was zu beweisen war.

7. Sind $\mathfrak{a}, \mathfrak{b}$ beliebige Ideale, so ist $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$, und folglich $(\mathfrak{a}, \mathfrak{a}\mathfrak{b}) = N(\mathfrak{b})$.

Wir betrachten zunächst ein Produkt $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$, dessen einer Faktor $\mathfrak{p}$ ein Primideal ist. Dann ist der andere Faktor $\mathfrak{q}$ ein echter Teiler von $\mathfrak{a}$, weil sonst $\mathfrak{q} = \mathfrak{a}$, und folglich (nach 6.) $\mathfrak{p} = \mathfrak{o}$ wäre, und es gibt daher in $\mathfrak{q}$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η; bezeichnen wir nun (wie in § 169, 4.) mit $\mathfrak{a}'\eta$ das kleinste gemeinschaftliche Vielfache, mit $\mathfrak{b}$ den größten gemeinschaftlichen Teiler der beiden Ideale $\mathfrak{a}$ und $\mathfrak{o}\eta$, so ist $N(\mathfrak{a}) = N(\mathfrak{a}')N(\mathfrak{b})$, und hieraus folgt

$$N(\mathfrak{p}\mathfrak{q}) = N(\mathfrak{p})N(\mathfrak{q}),$$

weil, wie wir zugleich zeigen wollen, $\mathfrak{a}' = \mathfrak{p}$ und $\mathfrak{b} = \mathfrak{q}$ ist. In der Tat, da η durch $\mathfrak{q}$, also $\mathfrak{p}\eta$ (nach § 170, 1.) durch $\mathfrak{p}\mathfrak{q}$ teilbar ist, so ist $\mathfrak{p}\eta$ ein gemeinschaftliches Vielfaches von $\mathfrak{a}$ und $\mathfrak{o}\eta$, mithin teilbar durch $\mathfrak{a}'\eta$, woraus folgt, daß $\mathfrak{a}'$ in $\mathfrak{p}$ aufgehen, also $= \mathfrak{o}$ oder $= \mathfrak{p}$ sein muß; das erstere ist aber unmöglich, weil $\mathfrak{o}\eta$ nicht durch $\mathfrak{a}$ teilbar ist; also ist $\mathfrak{a}' = \mathfrak{p}$. Da ferner $\mathfrak{q}$ ein gemeinschaftlicher Teiler von $\mathfrak{a}$ und $\mathfrak{o}\eta$ ist und folglich in $\mathfrak{b}$ aufgeht, so kann man (nach 6.) $\mathfrak{b} = \mathfrak{e}\mathfrak{q}$ setzen, und da dieses Ideal $\mathfrak{b}$ in $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$ aufgeht, so muß (nach 6.) das Ideal $\mathfrak{e}$ in $\mathfrak{p}$ aufgehen, also $= \mathfrak{o}$ oder $= \mathfrak{p}$ sein, woraus entsprechend $\mathfrak{b} = \mathfrak{q}$, oder $\mathfrak{b} = \mathfrak{p}\mathfrak{q} = \mathfrak{a}$ folgt; das letztere ist aber unmöglich, weil η nicht durch $\mathfrak{a}$ teilbar ist; also ist $\mathfrak{b} = \mathfrak{q}$, wie behauptet war. Nachdem hiermit unser Satz für den Fall bewiesen ist, daß einer der Faktoren ein Primideal ist, ergibt sich seine Allgemeingültigkeit leicht wie folgt. Da (nach 4.) jedes von $\mathfrak{o}$ verschiedene Ideal

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_r$$

gesetzt werden darf, wo $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ Primideale bedeuten, so folgt aus dem eben Bewiesenen, daß

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_r) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3 \dots \mathfrak{p}_r),$$

also

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3) \dots N(\mathfrak{p}_r)$$

ist. Setzt man nun, wenn $\mathfrak{b}$ ein zweites Ideal ist,

$$\mathfrak{b} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s,$$

so folgt ebenso

$$N(\mathfrak{b}) = N(\mathfrak{q}_1)N(\mathfrak{q}_2) \dots N(\mathfrak{q}_s);$$

zugleich ist aber

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\dots\mathfrak{p}_r\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_s,$$

also

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)\dots N(\mathfrak{p}_r)N(\mathfrak{q}_1)\dots N(\mathfrak{q}_s),$$

mithin wirklich $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$, was zu beweisen war.

8. Ein Ideal $\mathfrak{a}$ (oder eine Zahl α) ist stets und nur dann durch ein Ideal $\mathfrak{b}$ (oder eine Zahl δ) teilbar, wenn alle in $\mathfrak{b}$ (oder δ) aufgehenden Potenzen von Primidealen auch in $\mathfrak{a}$ (oder α) aufgehen.

Denn wenn $\mathfrak{p}$ ein Primideal ist, und $\mathfrak{p}^m$ in einem Ideale $\mathfrak{b}$ aufgeht, so ist (nach 6.) $\mathfrak{b} = \mathfrak{e}\mathfrak{p}^m$, und wenn man das Ideal $\mathfrak{e}$ (nach 4.) in seine Primfaktoren zerlegt, so ist auch $\mathfrak{b}$ als Produkt von lauter Primidealen dargestellt, unter denen folglich der Faktor $\mathfrak{p}$ mindestens $m$mal vorkommt; umgekehrt, wenn in der Zerlegung von $\mathfrak{b}$ in Primfaktoren das Primideal $\mathfrak{p}$ mindestens $m$mal als Faktor auftritt, so ist $\mathfrak{b}$ offenbar durch $\mathfrak{p}^m$ teilbar. Wenn daher gesagt wird, daß alle in $\mathfrak{b}$ aufgehenden Potenzen von Primidealen auch in einem Ideale $\mathfrak{a}$ aufgehen, so heißt dies nichts anderes, als daß alle in der Zerlegung von $\mathfrak{b}$ auftretenden Primfaktoren auch sämtlich mindestens ebensooft in der Zerlegung von $\mathfrak{a}$ als Faktoren auftreten; unter den Faktoren von $\mathfrak{a}$ finden sich daher zunächst alle Faktoren von $\mathfrak{b}$, und wenn man das Produkt der übrigen Faktoren von $\mathfrak{a}$ mit $\mathfrak{r}$ bezeichnet, so ist $\mathfrak{a} = \mathfrak{r}\mathfrak{b}$, und folglich ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$. Daß aber umgekehrt, wenn $\mathfrak{b}$ ein Teiler von $\mathfrak{a}$ ist, alle in $\mathfrak{b}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{a}$ aufgehen, versteht sich von selbst.

Nachdem unser Satz bewiesen ist, bemerken wir noch folgendes. Vereinigt man alle untereinander gleichen Primfaktoren eines Ideals $\mathfrak{a}$ zu einer Potenz, so erhält man

$$\mathfrak{a} = \mathfrak{p}^a\mathfrak{q}^b\mathfrak{r}^c\dots,$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}\dots$ lauter voneinander verschiedene Primideale bedeuten, und nach dem eben bewiesenen Satze sind die sämtlichen Teiler von $\mathfrak{a}$ in der Form

$$\mathfrak{b} = \mathfrak{p}^{a'}\mathfrak{q}^{b'}\mathfrak{r}^{c'}\dots$$

enthalten, wo die Exponenten $a', b', c'\dots$ den Bedingungen

$$0 \leqq a' \leqq a,\ 0 \leqq b' \leqq b,\ 0 \leqq c' \leqq c\dots$$

genügen; da je zwei verschiedenen Kombinationen von Exponenten $a', b', c'\dots$ (nach 4.) zwei verschiedene Ideale $\mathfrak{b}$ entsprechen, so ist die Anzahl aller verschiedenen Teiler

$$= (a+1)(b+1)(c+1)\dots$$

9. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache und $\mathfrak{d}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{a}$, $\mathfrak{b}$, so ist

$$\mathfrak{a} = \mathfrak{d}\mathfrak{a}', \quad \mathfrak{b} = \mathfrak{d}\mathfrak{b}', \quad \mathfrak{m}\mathfrak{d} = \mathfrak{a}\mathfrak{b},$$
$$\mathfrak{m} = \mathfrak{d}\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{a}',$$

wo $\mathfrak{a}'$, $\mathfrak{b}'$ relative Primideale bedeuten. Ist ferner $\mathfrak{b}\mathfrak{c}$ teilbar durch $\mathfrak{a}$, so ist $\mathfrak{c}$ teilbar durch $\mathfrak{a}'$.

Denn weil $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{d}$ teilbar sind, so kann man (nach 6.) $\mathfrak{a} = \mathfrak{d}\mathfrak{a}'$, $\mathfrak{b} = \mathfrak{d}\mathfrak{b}'$ setzen; bedeutet nun $\mathfrak{d}'$ den größten gemeinschaftlichen Teiler der Ideale $\mathfrak{a}'$, $\mathfrak{b}'$, so ist (nach § 170, 1.) das Produkt $\mathfrak{d}\mathfrak{d}'$ ein gemeinschaftlicher Teiler von $\mathfrak{a}$, $\mathfrak{b}$, also auch ein Teiler von $\mathfrak{d}$, woraus (nach 6.) $\mathfrak{d}' = \mathfrak{o}$ folgt; mithin sind $\mathfrak{a}'$, $\mathfrak{b}'$ relative Primideale. Ist nun $\mathfrak{b}\mathfrak{c}$ teilbar durch $\mathfrak{a}$, also $\mathfrak{d}\mathfrak{b}'\mathfrak{c}$ teilbar durch $\mathfrak{d}\mathfrak{a}'$, so muß (nach 6.) $\mathfrak{a}'$ in $\mathfrak{b}'\mathfrak{c}$, mithin (nach § 171, 5.) auch in $\mathfrak{c}$ aufgehen. Hieraus folgen sofort die Behauptungen über $\mathfrak{m}$; da nämlich $\mathfrak{m}$ teilbar durch $\mathfrak{b}$, also (nach 6.) von der Form $\mathfrak{b}\mathfrak{c}$, zugleich aber auch teilbar durch $\mathfrak{a}$ ist, so ist $\mathfrak{c}$ teilbar durch $\mathfrak{a}'$, also $\mathfrak{m}$ teilbar durch $\mathfrak{b}\mathfrak{a}'$ (nach § 170, 1.); da aber umgekehrt dieses letztere Ideal $\mathfrak{b}\mathfrak{a}' = \mathfrak{d}\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}\mathfrak{b}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{a}$, $\mathfrak{b}$ ist, so muß es durch $\mathfrak{m}$ teilbar und folglich $= \mathfrak{m}$ sein, was zu beweisen war.

Erläuterungen zu den vorstehenden Abhandlungen XLVI bis XLIX.

Im vorangehenden ist das „Elfte Supplement“ in den verschiedenen Fassungen gegeben, vollständig in der letzten, während von den früheren nur jeweils das dort nicht Übernommene gebracht wurde. Es zeigt sich, daß die Entwicklungen zur analytischen Zahlentheorie — Dedekindsche ζ-Funktion, transzendente Bestimmung der Klassenzahl — fast unverändert in alle Auflagen übernommen wurden, ebenso die Theorie der Einheiten. Dagegen hat das, was als Dedekinds ureigene Schöpfung zu bezeichnen ist, Körpertheorie und Idealtheorie, von Auflage zu Auflage neue Formen angenommen.

Die erste Begründung der Körpertheorie (in der 2. Auflage, XLVII) ruht vollständig auf hyperkomplexer Grundlage, einer Grundlage, die Dedekind später verlassen hat, weil sie für die hier vorliegenden Zwecke entbehrlich war, wohl auch um das Verständnis zu erleichtern; die hyperkomplexe Theorie war noch sehr kompliziert und formal. Die hyperkomplexe Auffassung, deren Wichtigkeit in neuester Zeit immer mehr hervortritt, steht aber auch hinter den späteren Fassungen; sie findet sich wieder ziemlich stark in Dedekind-Weber (vgl. die Erläuterungen zu XVIII). Die weiteren hyperkomplexen Arbeiten schließen direkt an die ursprüngliche Begründung der Körpertheorie an (vgl. die Erläuterungen zu XX).

Die ausführliche Entwicklung der Galoisschen Theorie in der heutigen Form findet sich erst in der 4. Auflage (XLVI), Andeutungen davon schon in der ersten Begründung der Körpertheorie (vgl. Anm. *) S. 228), weiter ausgeführte in den folgenden Darstellungen. Dedekind geht aus von der Betrachtung der Iso-

morphismen beliebiger Körper und ihrer Zusammensetzung, Betrachtungen, die erst in neuester Zeit wieder aufgenommen wurden; durch Spezialisierung auf Galoissche Körper kommt er zur Automorphismengruppe. Diese Auffassung der Galoisschen Gruppe als Automorphismengruppe ist einer der Ausgangspunkte in der neueren Entwicklung der Algebra geworden; Dedekind hat sie schon in seinen Göttinger Vorlesungen 1857/58 entwickelt (vgl. Anm. *) S. 52). Dabei arbeitet Dedekind bei dem Fortsetzungssatz der Isomorphismen ohne Benutzung eines primitiven Elements, ein Umstand, der ihm die Übertragung auf unendliche Körper ermöglichte (XXXI); auch das ist erst in neuester Zeit allgemein in die Algebra eingedrungen.

Die Entwicklung der Idealtheorie läuft ganz ähnlich wie die der Körpertheorie; die ersten Fassungen sind allgemeiner, aber noch sehr kompliziert. Die erste Begründung der 2. Auflage (XLVII) spaltet den Zerlegungssatz in zwei Teile: das Ideal wird als kl. gem. Vielf. (Durchschnitt) von symbolischen Primidealpotenzen dargestellt; erst dann wird der Produktbegriff eingeführt und zu der üblichen Zerlegungsform übergegangen. Dabei wird aber schon bei der Durchschnittsdarstellung benutzt, daß es sich um die Hauptordnung handelt; die ganze Abgeschlossenheit wird wesentlich herangezogen.

Die 3. Auflage enthält ein Stück allgemeine Idealtheorie, die eindeutige Zerlegung der Ideale einer Ordnung in Primärideale (einartige Ideale). Der ausgeführte Beweis fand sich im Nachlaß mit dem Vermerk „für die dritte Auflage kassiert, doch wichtig“ und ist jetzt an der betreffenden Stelle wieder eingefügt (XLIX). Daß nur in der Hauptordnung die ausnahmslose Darstellung der Primärideale als Potenzen von Primidealen gilt, ist dort (XLIX, § 172) klar ausgesprochen, ebenso, daß nur in der Hauptordnung ausnahmslos aus Teilbarkeit Produktdarstellung folgt; auch auf die Bedeutung der allgemeineren Idealtheorie ist hingewiesen. Bis auf diese Zufügungen ist der Aufbau aus der französischen Darstellung (XLVIII) übernommen, die im übrigen stärker als die übrigen Fassungen durch zahlreich eingefügte Beispiele den Charakter einer elementaren Einführung trägt.

Die 4. Auflage (XLVI) steht auf neuer Grundlage: sie stellt die Gruppeneigenschaft der ganzen und gebrochenen Ideale in den Vordergrund, indem auf Grund der ganzen Abgeschlossenheit — formal eingekleidet in einen allgemeinen Modulsatz — gezeigt wird, daß jedes Ideal ein eigentlicher (umkehrbarer) Modul ist. Diese Auffassung wollte Dedekind in einer nicht mehr zur Ausführung gekommenen 5. Auflage noch unterstreichen, dadurch, daß er von vornherein ganze und gebrochene Ideale seinen Definitionen zugrunde legte. Im übrigen plante er nach den vorgefundenen Notizen keine wesentliche Änderung des 11. Supplements, nur ein noch etwas stärkeres Hervorheben der formalen Modulidentitäten, im Anschluß an XXX.

Über die axiomatische Begründung der Idealtheorie, die überall durch Dedekindsche Gedankengänge beeinflußt ist, ist in den Erläuterungen zu XXV berichtet; die Begriffsbildungen des 11. Supplements durchziehen heute die ganze abstrakte Algebra.

Noether.