Zahl $\alpha - \lambda\beta$ zu finden, die eine kleinere Norm als β hat. Zunächst bestimme man eine gebrochene Zahl $\lambda' = a' + b'i$, so daß $\alpha - \lambda'\beta = 0$ ist; sodann ersetze man a' und b' durch die nächstliegenden ganzen Zahlen a und b und setze $\lambda = a + bi$, $\lambda' - \lambda = \varepsilon$. Dann folgt:

$$\begin{aligned} &\alpha - \lambda\beta = \alpha - \lambda'\beta + \varepsilon\beta = \varepsilon\beta, \\ &N(\alpha - \lambda\beta) = N(\varepsilon)N(\beta), \\ &N(\varepsilon) = N(\lambda' - \lambda) = (a' - a)^2 + (b' - b)^2 \leqq (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 < 1, \\ &N(\alpha - \lambda\beta) < N(\beta). \end{aligned}$$

Damit ist ein „Divisionsalgorithmus" gefunden und der Ring als euklidisch erkannt.

Literatur. Über die Frage, ob der euklidische Algorithmus oder eine Verallgemeinerung desselben in beliebigen Hauptidealringen existiert, siehe H. Hasse: J. reine u. angew. Math. Bd. 159 (1928), S. 3—12. In welchen algebraischen Zahlringen der euklidische Algorithmus gilt, haben O. Perron (Math. Ann. Bd. 107, S. 489), A. Oppenheim (Math. Ann. Bd. 109, S. 349), E. Berg (Kgl. Fysiogr. Sällskapets Lund Förhandl. Bd. 5, N 5), N. Hofreiter (Mh. Math. Physik Bd. 42, S. 397), H. Behrbohm und L. Redei (J. reine u. angew. Math. Bd. 174, S. 198) untersucht.

§ 18. Faktorzerlegung

Wir betrachten in diesem Paragraphen nur Integritätsbereiche mit Einselement. Zunächst wollen wir untersuchen, was wir in diesen Bereichen zweckmäßig unter Primelementen oder unzerlegbaren Elementen zu verstehen haben. Dabei betrachten wir, auch wenn es nicht immer ausdrücklich gesagt wird, nur die von Null verschiedenen Ringelemente.

Eine gewöhnliche Primzahl im Ring der ganzen Zahlen läßt sich immer in Faktoren zerlegen, sogar auf zwei Weisen:

$$p = p \cdot 1 = (-p) \cdot (-1).$$

Aber einer dieser Faktoren ist immer eine „Einheit", d. h. eine solche Zahl ε, deren Inverse ε^{-1} auch im Ring liegt. $+1$ und -1 sind Einheiten.

Ist allgemein ein Integritätsbereich mit Einselement gegeben, so verstehen wir unter einer *Einheit*[1] ein solches Element ε, das im Bereich ein Inverses ε^{-1} besitzt. Offensichtlich ist dann auch ε^{-1} eine Einheit.

Jedes Element a läßt, wenn ε eine Einheit ist, eine Zerlegung

$$a = a\varepsilon^{-1} \cdot \varepsilon$$

zu. Solche Zerlegungen, bei denen ein Faktor eine Einheit ist, kann man „triviale Zerlegungen" nennen.

Ein Element $p \neq 0$, das nur triviale Zerlegungen zuläßt, so daß also aus $p = ab$ folgt, daß a oder b Einheit ist, heißt ein *unzerlegbares*

[1] Das Wort „Einheit" wird oft als Synonym für „Einselement" gebraucht. In Untersuchungen über Faktorzerlegung aber sind die beiden Begriffe streng zu trennen, da z. B. -1 auch eine Einheit ist.

Element oder ein *Primelement*. (Speziell bei ganzen Zahlen auch: *Primzahl*; bei Polynomen auch: *irreduzibles Polynom*.)

Man nennt bisweilen zwei Größen wie a und $b = a\varepsilon^{-1}$, die sich nur um eine Einheit als Faktor unterscheiden, „assoziierte Größen". Jede ist Teiler der anderen, und für die zugehörigen Hauptideale gilt:

$$(a) \subseteqq (b), \quad (b) \subseteqq (a), \quad \text{also} \quad (b) = (a);$$

mithin erzeugen zwei assoziierte Größen dasselbe Hauptideal.

Wenn umgekehrt von den beiden Größen a und b jede ein Teiler der anderen ist:

$$a = bc, \quad b = ad,$$

so folgt

$$b = bcd, \quad \text{also} \quad 1 = cd, \quad c = d^{-1},$$

mithin sind c und d Einheiten und es ist a zu b assoziiert.

Ist c ein Teiler von a, aber nicht assoziiert zu a, also $a = cd$ und d keine Einheit, so heißt c ein *echter Teiler* von a. In diesem Fall ist a nicht zugleich Teiler von c, und das Ideal (c) ist ein echter Teiler des Ideals (a). Wäre nämlich a ein Teiler von c, etwa $c = ab$, so wäre

$$\begin{aligned} a &= cd = abd \\ 1 &= bd \end{aligned}$$

und d wäre doch eine Einheit.

Ein Primelement kann jetzt auch definiert werden als ein von Null verschiedenes Element, das keine echten Teiler außer Einheiten besitzt.

Ist in einem euklidischen Ring b ein echter Teiler von a, so ist $g(b) < g(a)$.

Beweis. Die Division von b durch a geht nicht auf, ergibt also

$$b = aq + r, \quad g(r) < g(a).$$

Daraus folgt, wenn $a = bc$ gesetzt wird,

$$\begin{aligned} r &= b - aq = b(1 - cq) \\ g(r) &\geqq g(b), \quad \text{also} \quad g(b) \leqq g(r) < g(a). \end{aligned}$$

In einem euklidischen Ring ist jedes von Null verschiedene Element a ein Produkt von Primelementen:

$$a = p_1 p_2 \dots p_r.$$

Bemerkung. Man kann den Satz allgemeiner für Hauptidealringe beweisen: dabei muß man allerdings das Auswahlpostulat (§ 69) verwenden. In diesem elementaren Teil des Buches soll das Auswahlpostulat noch nicht zur Sprache kommen; daher möge der Beweis nur für euklidische Ringe geführt werden.

Beweis. Wir wenden vollständige Induktion nach $g(a)$ an: Die Behauptung sei richtig für alle Elemente b mit $g(b) < n$ und es sei $g(a) = n$. Ist nun a prim: $a = p$, so ist nichts mehr zu beweisen. Ist aber a zerlegbar: $a = bc$, wobei b und c echte Teiler von a sind, so ist

$$g(b) < g(a), \quad g(c) < g(a).$$

Nach der Induktionsvoraussetzung sind nun b und c Produkte von Primelementen. Also ist $a = bc$ auch ein Produkt von Primelementen.

Wir wollen nun untersuchen, wie es mit der Eindeutigkeit der Primfaktorzerlegung $a = p_1 p_2 \dots p_r$ steht und betrachten dabei nicht nur die euklidischen Ringe, sondern allgemein beliebige Hauptidealringe.

In einem Hauptidealring erzeugt ein unzerlegbares Element, das keine Einheit ist, ein teilerloses Primideal (dessen Restklassenring also ein Körper ist).

Beweis. Ist p unzerlegbar, so hat p keine echten Teiler außer Einheiten, also (da jedes Ideal Hauptideal ist) das Ideal (p) keine echten Idealteiler außer dem Einheitsideal.

Bemerkung. Man kann natürlich die Lösbarkeit der Gleichung $ax = b$ im Restklassenring oder der Kongruenz $ax \equiv b\,(p)$ im gegebenen Ring auch direkt aus der Tatsache erschließen, daß für $a \not\equiv 0\,(p)$ notwendig $(a, p) = 1$ sein muß, also

$$1 = ar + ps,$$
$$b = arb + psb,$$
$$b \equiv arb\,(p)$$

ist.

Eine unmittelbare Folgerung ist:

Ist ein Produkt durch das Primelement p teilbar, so muß ein Faktor es sein; denn der Restklassenring hat keine Nullteiler.

Aufgaben. 1. Man löse die Kongruenz

$$6x \equiv 7\,(19)$$

mit Hilfe des euklidischen Algorithmus.

2. Wenn in einem Hauptidealring ein Produkt ab durch c teilbar und a zu c teilerfremd ist, dann ist b durch c teilbar.

Nunmehr sind wir imstande, den *Satz von der Eindeutigkeit der Primfaktorzerlegung in Hauptidealringen* zu beweisen. Es seien

$$(1) \qquad a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

zwei Zerlegungen derselben Zahl a in einem Hauptidealring. Den trivialen Fall, daß a eine Einheit ist und folglich alle p_i und q_j Einheiten sind, schließen wir aus. Dann können wir annehmen, daß p_1 und q_1 keine Einheiten sind und daß alle eventuellen Einheiten unter

den Faktoren p_i und q_j mit dem Faktor p_1 bzw. q_1 vereinigt sind. Die p_i und q_j seien also keine Einheiten. Nun wird behauptet: *Es ist $r = s$ und die p_i stimmen mit den q_j bis auf die Reihenfolge und bis auf Einheitsfaktoren überein.*

Für $r = 1$ ist die Behauptung klar; denn wegen der Unzerlegbarkeit von $a = p_1$ kann das Produkt $q_1 \dots q_s$ auch nur einen Faktor $q_1 = p_1$ enthalten. Wir können also Induktion nach r vornehmen. Da p_1 in dem Produkt $q_1 \dots q_s$ aufgeht, so muß p_1 in einem der Faktoren q_i aufgehen. Durch Umordnung der q erreichen wir, daß p_1 in q_1 aufgeht:

$$(2) \qquad q_1 = \varepsilon_1 p_1.$$

Hierin muß ε_1 Einheit sein, da sonst q_1 nicht prim wäre. Setzt man (2) in (1) ein und kürzt durch p_1, so kommt

$$(3) \qquad p_2 \dots p_r = (\varepsilon_1 q_2) q_3 \dots q_s.$$

Nach der Induktionsvoraussetzung müssen die Faktoren in (3) links und rechts bis auf Einheiten übereinstimmen. Da auch p_1 mit q_1 bis auf die Einheit ε_1 übereinstimmt, ist alles bewiesen.

Aus den bewiesenen Sätzen folgt: *Die Elemente eines euklidischen Ringes sind bis auf Einheiten und bis auf die Reihenfolge der Faktoren eindeutig als Produkte von Primelementen darstellbar.* Insbesondere gilt das für die ganzen Zahlen, für die Polynome einer Veränderlichen mit Koeffizienten aus einem Körper, sowie für die ganzen Gaußschen Zahlen.

Aufgaben. 3. Die ganzzahligen Polynome $f(x)$ sind modulo jeder Primzahl p eindeutig in modulo p unzerlegbare Faktoren zerlegbar.

4. Was sind die Einheiten im Ring der ganzen Gaußschen Zahlen? Man zerlege die Zahlen 2, 3, 5 in diesem Ring in Primfaktoren.

5. Im Ring der Zahlen $a + b\sqrt{-3}$ bestehen für die Zahl 4 die beiden wesentlich verschiedenen Zerlegungen in unzerlegbare Faktoren:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

6. In einem Hauptidealring bilden diejenigen Restklassen modulo a, die aus zu a teilerfremden Elementen bestehen, bei der Multiplikation eine Gruppe.

Wir werden im übernächsten Kapitel sehen, daß es auch andere als Hauptidealringe gibt, in denen der Satz von der eindeutigen Faktorzerlegung gilt. Für alle solchen Ringe beweisen wir nun den Satz:

Wenn in $\mathfrak{o}$ jedes Element eindeutig in Primelemente zerlegbar ist, so erzeugt jedes unzerlegbare Element p ein Primideal, jedes von Null verschiedene zerlegbare Element ein Nichtprimideal.

Beweis. p sei unzerlegbar. Ist nun $ab \equiv 0\,(p)$, so muß in der Faktorzerlegung von ab der Faktor p vorkommen. Diese Faktorzerlegung erhält man aber durch Zusammensetzung der Faktorzerlegungen von

a und b; also muß schon in a oder b der Faktor p vorkommen, also $a \equiv 0(p)$ oder $(b) \equiv 0(p)$ sein.

Nun sei p zerlegbar: $p = ab$, a und b echte Teiler von p. Dann folgt $ab \equiv 0(p)$, $a \not\equiv 0(p)$, $b \not\equiv 0(p)$. Das Ideal (p) ist also nicht prim.

Aufgaben. 7. Man beweise für alle Ringe mit eindeutiger Faktorzerlegung, daß es für je zwei oder mehrere Elemente einen „größten gemeinsamen Teiler" und ein „kleinstes gemeinsames Vielfaches" gibt, die beide bis auf Einheitsfaktoren bestimmt sind.

Bemerkung. Für Ringe der betrachteten Art ist der G.G.T. im Elementsinn nicht immer derselbe wie der G.G.T. im Idealsinn. So haben z.B. im ganzzahligen Polynombereich einer Veränderlichen x die Elemente 2 und x keine gemeinsamen Teiler außer Einheiten; aber das Ideal $(2, x)$ ist nicht das Einheitsideal. (Daß in diesem Ring die eindeutige Faktorzerlegung besteht, wird im übernächsten Kapitel bewiesen werden.)

Viertes Kapitel

Vektorräume und Tensorräume

§ 19. Vektorräume

Es seien gegeben erstens ein Schiefkörper K, dessen Elemente $a, b, \ldots$ *Koeffizienten* oder *Skalare* heißen mögen, zweitens ein Modul (d. h. eine additive abelsche Gruppe) $\mathfrak{M}$, dessen Elemente $\boldsymbol{x}, \boldsymbol{y}, \ldots$ *Vektoren* heißen, drittens eine Multiplikation $\boldsymbol{x}a$ der Vektoren mit Skalaren, mit folgenden Eigenschaften:

V 1. $\quad \boldsymbol{x}a$ liegt in $\mathfrak{M}$.

V 2. $\quad (\boldsymbol{x} + \boldsymbol{y})a = \boldsymbol{x}a + \boldsymbol{y}a$.

V 3. $\quad \boldsymbol{x}(a + b) = \boldsymbol{x}a + \boldsymbol{x}b$.

V 4. $\quad \boldsymbol{x}(ab) = (\boldsymbol{x}a)b$.

V 5. $\quad \boldsymbol{x}1 = \boldsymbol{x}$.

Sind diese Voraussetzungen erfüllt, so heißt $\mathfrak{M}$ ein *Vektorraum über K*, genauer ein *K-rechts-Vektorraum*, weil die Koeffizienten a rechts von den Vektoren stehen. Der Begriff *K-links-Vektorraum* wird analog definiert; das Assoziativgesetz V 4 lautet für einen Links-Vektorraum

V 4* $\quad (ab)\boldsymbol{x} = a(b\boldsymbol{x})$.

Ist K kommutativ, so kann man statt $\boldsymbol{x}a$ auch $a\boldsymbol{x}$ schreiben. Der Rechts-Vektorraum wird dann zu einem Links-Vektorraum. Ist aber K nicht kommutativ, so muß man zwischen Rechts- und Links-Vektorräumen unterscheiden.

Statt $\boldsymbol{x}(ab)$ oder $(\boldsymbol{x}a)b$ schreiben wir $\boldsymbol{x}ab$. Das Nullelement von $\mathfrak{M}$ wird, wie das von K, einfach mit 0 bezeichnet.

Beispiele von Vektorräumen sind alle Erweiterungskörper eines Körpers K, allgemeiner alle Ringe R, die einen Schiefkörper K umfassen, sofern das Einselement von K auch Einselement von R ist.

Aus V 2 folgt wie gewöhnlich

$$(\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_r)a = \boldsymbol{x}_1 a + \cdots + \boldsymbol{x}_r a,$$
$$(\boldsymbol{x} - \boldsymbol{y})a = \boldsymbol{x}a - \boldsymbol{y}a,$$
$$0 \cdot a = 0.$$

Ebenso folgt aus V 3

$$\boldsymbol{x}(a_1 + \cdots + a_s) = \boldsymbol{x}a_1 + \cdots + \boldsymbol{x}a_s$$
$$\boldsymbol{x}(a - b) = \boldsymbol{x}a - \boldsymbol{x}b,$$
$$\boldsymbol{x} \cdot 0 = 0.$$

Der Vektorraum $\mathfrak{M}$ heißt *endlichdimensional* oder kurz *endlich* über K, wenn es endlich viele Erzeugende $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m$ gibt, durch die jedes Element von $\mathfrak{M}$ sich mit Koeffizienten a^k aus K ausdrücken läßt[1]:

(1) $$\boldsymbol{x} = \sum \boldsymbol{e}_k a^k.$$

Wenn eine der Erzeugenden $\boldsymbol{e}_k$ sich durch die übrigen $\boldsymbol{e}_i$ ausdrücken läßt, so ist dieses $\boldsymbol{e}_k$ als erzeugendes Element von $\mathfrak{M}$ überflüssig. Streicht man es dann aus der Reihe $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m$ und fährt so fort bis kein $\boldsymbol{e}_i$ mehr überflüssig ist, so bleiben schließlich n *Basisvektoren* $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ übrig, von denen keiner sich linear durch die anderen ausdrücken läßt. Man nennt solche Vektoren, von denen keiner sich durch die anderen ausdrücken läßt, *linear unabhängig*.

Wenn $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ linear unabhängig sind, so folgt aus

(2) $$\boldsymbol{p}_1 a^1 + \cdots + \boldsymbol{p}_n a^n = 0$$

notwendig

$$a^1 = 0, \ldots, a^n = 0.$$

Wäre nämlich ein $a^i \neq 0$, so könnte man aus (2) ein $\boldsymbol{p}_i$ auflösen und durch die anderen ausdrücken.

Wenn $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ eine linear unabhängige Basis für den Vektorraum $\mathfrak{M}$ bilden, so läßt sich jeder Vektor $\boldsymbol{x}$ *eindeutig* durch die Basis-

[1] Bei der Kennzeichnung der Koeffizienten a^k durch obere Indices folgen wir einer Konvention von Einstein, die in der Vektor- und Tensorrechnung sehr zweckmäßig ist. Summationen erstrecken sich nach dieser Konvention immer auf die Indices, die einmal unten und einmal oben vorkommen.

Reihe n-ter Ordnung wird demnach durch die Formel

$$b_x = f(x)$$
$$= b_0 + (\Delta b_0)x + \frac{\Delta^2 b_0}{2}x(x-1) + \cdots + \frac{\Delta^n b_0}{n!}x(x-1)\ldots(x-n+1)$$

gegeben.

Das Differenzenschema (8) findet praktisch Anwendung bei der Interpolation und Integration von Funktionen, die durch numerische (etwa empirisch gewonnene) Tabellen gegeben sind. Sind $b_0, b_1, b_2, \ldots$ die Werte einer Funktion $\varphi(x)$ für äquidistante Argumentwerte α_0, $\alpha_0 + h$, $\alpha_0 + 2h, \ldots$, so zeigt die Praxis, daß bei regelmäßig verlaufenden Funktionen und bei nicht allzu großer Intervallänge h die zweiten, dritten, vierten oder schlimmstenfalls die fünften Differenzen praktisch Null werden, also die Funktion sich in einigen unmittelbar aufeinanderfolgenden Intervallen fast genau wie ein Polynom von höchstens viertem Grad verhält. Für die Zwecke der numerischen Interpolation oder Integration kann man daher die Funktion durch ein Polynom ersetzen, welches an 2 bis 5 aufeinanderfolgenden Stellen die durch die Tabellen gegebenen Werte annimmt. Die Interpolation geschieht mittels der Formel (2); dabei kommt man fast immer mit den ersten und zweiten Differenzen, also mit linearen oder quadratischen Polynomen aus. Bei der Umrechnung von Differenzen $\Delta^k a_\nu$ in Differenzenquotienten treten außer den Faktoren $k!$ noch Potenzen der Intervallänge h auf; an Stelle von (9) hat man demnach die Formel

$$\lambda_k = \frac{\Delta^k a_0}{k!\, h^k}$$

zu benutzen.

Sind die Argumentwerte $\alpha_0, a_1, \ldots$ nicht mehr äquidistant, so hat man statt der Differenzen $\Delta^k a_\nu$ von vornherein die Differenzenquotienten (7) zu bilden. Für weitere Einzelheiten der Rechnung sowie für Fehlerabschätzungen usw. verweisen wir auf die einschlägige Lehrbuchliteratur[1].

Aufgaben. 1. Die Teilsummen $s_m = \sum_{\nu=0}^{m-1} a_\nu$ einer arithmetischen Reihe n-ter Ordnung (wobei $s_0 = 0$ gesetzt wird) bilden eine arithmetische Reihe $(n+1)$-ter Ordnung. Daraus ist die Summenformel

$$s_m = m a_0 + \binom{m}{2}\Delta a_0 + \cdots + \binom{m}{n+1}\Delta^n a_0$$

herzuleiten.

2. Man gebe Formeln für die Summen $\sum_{\nu=0}^{m-1}\nu$, $\sum_{\nu=0}^{m-1}\nu^2$, $\sum_{\nu=0}^{m-1}\nu^3$.

[1] Siehe etwa G. Kowalewski: Interpolation und genäherte Quadratur. Leipzig 1930.

§ 30. Faktorzerlegung

Wir haben in § 18 schon gesehen, daß für den Polynombereich $K[x]$, wo K ein kommutativer *Körper* ist, der Satz von der eindeutigen Zerlegung in Primfaktoren gilt. Wir werden jetzt den folgenden allgemeineren *Hauptsatz* beweisen:

Ist $\mathfrak{S}$ ein Integritätsbereich mit Einselement und gilt in $\mathfrak{S}$ der Satz von der eindeutigen Primfaktorzerlegung, so gilt dieser Satz auch im Polynombereich $\mathfrak{S}[x]$.

Der hier darzustellende Beweis geht auf Gauss zurück.

Es sei $f(x) = \sum_0^n a_i x^i$ ein von Null verschiedenes Polynom aus $\mathfrak{S}[x]$.

Der größte gemeinsame Teiler d von $a_0, \ldots, a_n$ in $\mathfrak{S}$ (vgl. § 18, Aufgabe 7) heißt der *Inhalt* von $f(x)$. Klammert man d aus, so kommt

$$f(x) = d \cdot g(x),$$

wo $g(x)$ den Inhalt 1 hat. $g(x)$ und d sind bis auf Einheitsfaktoren eindeutig bestimmt. Polynome vom Inhalt 1 heißen *Einheitsformen* oder *primitive Polynome* (in bezug auf $\mathfrak{S}$).

Hilfssatz 1. *Das Produkt zweier Einheitsformen ist wieder eine Einheitsform.*

Beweis. Es seien

$$f(x) = a_0 + a_1 x + \cdots$$

und

$$g(x) = b_0 + b_1 x + \cdots$$

Einheitsformen. Gesetzt, die Koeffizienten von $f(x) \cdot g(x)$ hätten einen gemeinsamen Teiler d, der keine Einheit wäre. Ist p ein Primfaktor von d, so muß p in allen Koeffizienten von $f(x)\,g(x)$ aufgehen. Es sei a_r der erste nicht durch p teilbare Koeffizient von $f(x)$ und entsprechend b_s der von $g(x)$.

Der Koeffizient von x^{r+s} in $f(x)\,g(x)$ sieht so aus:

$$a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots$$
$$+ a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots.$$

Die Summe soll durch p teilbar sein. Alle Glieder außer dem ersten sind durch p teilbar. Also muß $a_r b_s$ durch p teilbar, also a_r oder b_s durch p teilbar sein, entgegen der Voraussetzung.

Es sei nun Σ der Quotientenkörper von $\mathfrak{S}$ (§ 13). Dann ist in $\Sigma[x]$ jedes Polynom eindeutig zerlegbar (§ 18). Um nun von der Zerlegung in $\Sigma[x]$ zu einer Zerlegung in $\mathfrak{S}[x]$ zu gelangen, benutzen wir folgende Tatsache: Jedes Polynom $\varphi(x)$ von $\Sigma[x]$ kann man in der Gestalt $\frac{F(x)}{b}$ ($F(x)$ in $\mathfrak{S}[x]$, b in $\mathfrak{S}$) schreiben, wo b etwa das Produkt der

Nenner der Koeffizienten von $\varphi(x)$ ist. Sodann kann man $F(x)$ als Produkt „Inhalt mal Einheitsform" schreiben:

$$F(x) = a \cdot f(x),$$

$$\varphi(x) = \frac{a}{b} \cdot f(x). \tag{1}$$

Wir behaupten nun:

Hilfssatz 2. *Die in* (1) *auftretende Einheitsform $f(x)$ ist eindeutig bis auf Einheiten aus $\mathfrak{S}$ durch $\varphi(x)$ bestimmt. Umgekehrt ist $\varphi(x)$ nach* (1) *eindeutig bis auf Einheiten aus $\Sigma[x]$ durch $f(x)$ bestimmt. Läßt man in dieser Weise jedem $\varphi(x)$ aus $\Sigma[x]$ eine Einheitsform $f(x)$ entsprechen, so entspricht dem Produkt zweier Polynome $\varphi(x) \cdot \psi(x)$ bis auf Einheiten das Produkt der zugehörigen Einheitsformen (und umgekehrt). Ist $\varphi(x)$ unzerlegbar in $\Sigma[x]$, so ist $f(x)$ unzerlegbar in $\mathfrak{S}[x]$ (und umgekehrt).*

Beweis: Es seien zwei verschiedene Darstellungen eines $\varphi(x)$ gegeben:

$$\psi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x).$$

Dann folgt:

$$adf(x) = cbg(x). \tag{2}$$

Der Inhalt der linken Seite ist ad, der der rechten Seite cb; also muß

$$ad = \varepsilon cb$$

sein, wo ε eine Einheit aus $\mathfrak{S}$ ist. Setzt man das in (2) ein und kürzt durch cb, so folgt

$$\varepsilon f(x) = g(x).$$

$f(x)$ und $g(x)$ unterscheiden sich also nur um eine Einheit aus $\mathfrak{S}$.

Für das Produkt zweier Polynome

$$\varphi(x) = \frac{a}{b} f(x),$$

$$\psi(x) = \frac{c}{d} g(x)$$

erhält man sofort:

$$\varphi(x) \cdot \psi(x) = \frac{ac}{bd} f(x) g(x),$$

und nach Hilfssatz 1 ist $f(x)\,g(x)$ wieder eine Einheitsform. Dem Produkt $\varphi(x) \cdot \psi(x)$ entspricht also das Produkt $f(x) \cdot g(x)$.

Ist schließlich $\varphi(x)$ unzerlegbar, so ist es auch $f(x)$; denn eine Zerlegung $f(x) = g(x)\,h(x)$ würde sofort eine Zerlegung

$$\varphi(x) = \frac{a}{b} f(x) = \frac{a}{b} g(x) \cdot h(x)$$

nach sich ziehen. Das Umgekehrte folgt ebenso.

Damit ist Hilfssatz 2 bewiesen.

Vermöge des Hilfssatzes 2 überträgt sich nun die eindeutige Faktorzerlegung der Polynome $\varphi(x)$ unmittelbar auf die zugehörigen Einheitsformen. Also: *Einheitsformen lassen sich bis auf Einheiten eindeutig in Primfaktoren, die wieder Einheitsformen sind, zerlegen.*

Nun wenden wir uns der Faktorzerlegung beliebiger Polynome in $\mathfrak{S}[x]$ zu. Unzerlegbare Polynome sind notwendig entweder unzerlegbare Konstanten oder unzerlegbare Einheitsformen; denn jedes andere Polynom ist zerlegbar in Inhalt mal Einheitsform. Um also ein Polynom $f(x)$ zu zerlegen, muß man zuerst $f(x)$ in Inhalt mal Einheitsform aufspalten und dann diese beiden Bestandteile getrennt in Primfaktoren zerlegen. Das erstere ist bis auf Einheiten eindeutig möglich nach der Voraussetzung des Hauptsatzes, das zweite ebenfalls nach dem eben Bewiesenen. Damit ist der Hauptsatz bewiesen.

Als wichtiges Nebenresultat des Beweises ergibt sich:

Ist ein Polynom $F(x)$ aus $\mathfrak{S}[x]$ zerlegbar in $\Sigma[x]$, so ist es schon in $\mathfrak{S}[x]$ zerlegbar.

Denn vermöge $F(x) = d \cdot f(x)$ entspricht dem Polynom $F(x)$ eine Einheitsform $f(x)$, und nach Hilfssatz 2 zieht eine Produktzerlegung von $F(x)$ in $\Sigma[x]$ eine solche von $f(x)$ in $\mathfrak{S}[x]$ nach sich; mit $f(x)$ ist aber $F(x)$ zerlegbar.

Beispielsweise ist ein jedes Polynom mit ganzen rationalen Koeffizienten, das sich rationalzahlig zerlegen läßt, schon ganzzahlig zerlegbar. Also: *Wenn ein ganzzahliges Polynom ganzzahlig unzerlegbar ist, so ist es auch rationalzahlig unzerlegbar.*

Durch vollständige Induktion erhält man aus dem Hauptsatz das weitergehende Ergebnis:

Ist $\mathfrak{S}$ ein Integritätsbereich mit Einselement und gilt in $\mathfrak{S}$ der Satz von der eindeutigen Faktorzerlegung, so gilt dieser Satz auch im Polynombereich $\mathfrak{S}[x_1, \ldots, x_n]$.

Daraus folgt unter anderem die eindeutige Faktorzerlegung für die ganzzahligen Polynome (von beliebig vielen Variablen), für die Polynome mit Koeffizienten aus einem Körper usw.

Der Begriff „primitives Polynom", oben in den Gaußschen Hilfssätzen eingeführt, wird insbesondere dann verwendet, wenn es sich um Polynombereiche in mehreren Variablen handelt. Ist K ein Körper, so heißt ein Polynom f aus $\mathsf{K}[x_1, \ldots, x_n]$ *primitiv in bezug auf* $x_1, \ldots, x_{n-1}$, wenn es primitiv in bezug auf den Integritätsbereich $\mathsf{K}[x_1, \ldots, x_{n-1}]$ ist, d. h. keinen nichtkonstanten Teiler hat, der nur von $x_1, \ldots, x_{n-1}$ abhängt.

Aufgaben. 1. Einheiten in $\mathfrak{S}[x]$ sind nur die Einheiten von $\mathfrak{S}$.

2. Man beweise, daß in einer Faktorzerlegung eines homogenen Polynoms nur homogene Faktoren auftreten können.

3. Man beweise, daß die Determinante

$$\Delta = \begin{vmatrix} x_{11} & \dots & x_{1n} \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ x_{n1} & \dots & x_{nn} \end{vmatrix}$$

im Polynombereich $\mathfrak{S}[x_{11}, \dots, x_{nn}]$ unzerlegbar ist. (Man zeichne eine Unbestimmte, etwa x_{11}, aus und zeige, daß Δ primitiv in bezug auf die übrigen ist.)

4. Man gebe eine Regel an, die es erlaubt, von jedem ganzzahligen Polynom zu entscheiden, ob es einen Faktor ersten Grades hat.

5. Man beweise die Unzerlegbarkeit des Polynoms

$$x^4 - x^2 + 1$$

im ganzzahligen Polynombereich der Unbestimmten x. Ist das Polynom im rationalzahligen Polynombereich zerlegbar? Ist es zerlegbar über dem Ring der ganzen Gaußschen Zahlen?

§ 31. Irreduzibilitätskriterien

Es sei $\mathfrak{S}$ ein Integritätsbereich mit Einselement, in dem die eindeutige Zerlegbarkeit gilt, und es sei

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

ein Polynom aus $\mathfrak{S}[x]$. Der folgende Satz gibt in vielen Fällen Auskunft über die Irreduzibilität von $f(x)$.

Eisensteinscher Satz. *Wenn es ein Primelement p in $\mathfrak{S}$ gibt, so daß*

$$\begin{aligned} a_n &\not\equiv 0(p), \\ a_i &\equiv 0(p) \quad \text{für alle } i < n, \\ a_0 &\not\equiv 0(p^2) \end{aligned}$$

ist, so ist $f(x)$ irreduzibel in $\mathfrak{S}[x]$ bis auf konstante Faktoren; mit anderen Worten es ist $f(x)$ irreduzibel in $\Sigma[x]$, wo Σ den Quotientenkörper von $\mathfrak{S}$ bedeutet.

Beweis. Wäre $f(x)$ zerlegbar:

$$\begin{aligned} f(x) &= g(x) \cdot h(x), \\ g(x) &= \sum_0^r b_\nu x^\nu, \\ h(x) &= \sum_0^s c_\nu x^\nu, \\ r > 0, \quad s > 0, \quad r + s &= n, \end{aligned}$$

so hätte man

$$a_0 = b_0 c_0 \quad \text{und} \quad a_0 \equiv 0(p).$$

Daraus folgt, daß entweder $b_0 \equiv 0(p)$ oder $c_0 \equiv 0(p)$ ist. Es sei etwa $b_0 \equiv 0(p)$. Dann ist $c_0 \not\equiv 0(p)$, weil sonst $a_0 = b_0 c_0 \equiv 0(p^2)$ wäre.

Nicht alle Koeffizienten von $g(x)$ sind durch p teilbar; denn sonst wäre das Produkt $f(x) = g(x) \cdot h(x)$ durch p teilbar, also alle Koeffizienten, insbesondere a_n durch p teilbar, entgegen der Voraussetzung. Es sei also b_i der erste Koeffizient von $g(x)$, der nicht durch p teilbar ist ($0 < i \leqq r < n$). Es ist

$$\begin{aligned} a_i &= b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i, \\ a_i &\equiv 0(p), \\ b_{i-1} &\equiv 0(p), \\ &\dots\dots\dots\dots \\ b_0 &\equiv 0(p), \end{aligned}$$

also

$$\begin{aligned} b_i c_0 &\equiv 0(p), \\ c_0 &\not\equiv 0(p), \\ b_i &\equiv 0(p), \end{aligned}$$

entgegen der Voraussetzung.

Also ist $f(x)$ bis auf konstante Faktoren irreduzibel.

Beispiel 1. $x^m - p$ (p prim) ist im ganzzahligen (und somit auch im rationalzahligen) Polynombereich irreduzibel. Also ist $\sqrt[m]{p}$ ($m > 1$, p prim) stets irrational.

Beispiel 2. $f(x) = x^{p-1} + x^{p-2} + \dots + 1$ ist, wenn p Primzahl ist, die linke Seite einer „Kreisteilungsgleichung". Wir fragen wieder nach ganzzahliger (oder, was auf dasselbe hinauskommt, rationalzahliger) Irreduzibilität. Das Eisensteinsche Kriterium ist nicht direkt anwendbar; aber man kann folgendermaßen schließen. Wäre $f(x)$ reduzibel, so wäre $f(x+1)$ es auch. Nun ist

$$\begin{aligned} f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} &= \frac{x^p + \binom{p}{1} x^{p-1} + \dots + \binom{p}{p-1} x}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \dots + \binom{p}{p-1}. \end{aligned}$$

Alle Koeffizienten außer dem von x^{p-1} sind durch p teilbar; denn in der Formel für die Binomialkoeffizienten

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!}$$

ist für $i < p$ der Zähler durch p teilbar, der Nenner aber nicht. Außerdem ist das konstante Glied $\binom{p}{p-1} = p$ nicht durch p^2 teilbar. Also ist $f(x+1)$ irreduzibel, also $f(x)$ irreduzibel.

Beispiel 3. Dieselbe Transformation führt auch für $f(x) = x^2 + 1$ zur Entscheidung, da

$$f(x+1) = x^2 + 2x + 2$$

ist.

Aufgaben. 1. Man zeige die Irrationalität von $\sqrt[m]{p_1 p_2 \dots p_r}$, wo $p_1, \dots, p_r$ verschiedene Primzahlen sind und $m > 1$ ist.

2. Man zeige die Irreduzibilität von

$$x^2 + y^2 - 1$$

in $\mathsf{P}([x, y]$, wo P irgend ein Körper ist, in welchem $+1 \neq -1$ ist.

3. Man zeige die Irreduzibilität der Polynome

$$x^4 + 1; \quad x^6 + x^3 + 1,$$

im ganzzahligen Polynombereich.

Im Grunde beruht der Eisensteinsche Satz darauf, daß man die Gleichung

$$f(x) = g(x) \cdot h(x)$$

in eine Kongruenz nach p^2 verwandelt:

$$f(x) \equiv g(x) \cdot h(x),$$

und diese ad absurdum führt. In sehr vielen anderen Fällen ist es ebenfalls möglich, Irreduzibilitätsbeweise dadurch zu führen, daß man die Gleichungen in Kongruenzen modulo irgendeiner Größe q des Bereichs $\mathfrak{S}$ verwandelt und untersucht, ob das vorgelegte Polynom $f(x)$ modulo q zerfällt. Ist insbesondere $\mathfrak{S}$ der Bereich der ganzen Zahlen $\mathbb{Z}$, so gibt es im Restklassenbereich nach q nur endlichviele Polynome von gegebenem Grad; also hat man modulo q immer nur endlichviele Möglichkeiten der Zerfällung von $f(x)$ zu untersuchen. Stellt es sich heraus, daß $f(x)$ modulo q irreduzibel ist, so war $f(x)$ auch in $\mathbb{Z}[x]$ irreduzibel, und auch im anderen Fall kann man unter Umständen Schlüsse aus der gefundenen Zerlegung mod q ziehen, wobei man sich im Falle q = Primzahl auf den Satz von der eindeutigen Primfaktorzerlegung der Polynome mod q (§ 18, Aufgabe 3) stützen kann.

Beispiel 4. $\mathfrak{S} = \mathbb{Z}$; $f(x) = x^5 - x^2 + 1$. Wenn $f(x)$ mod 2 zerlegbar ist, so muß einer der Faktoren linear oder quadratisch sein. Nun gibt es mod 2 bloß zwei lineare Polynome:

$$x, x + 1,$$

und bloß ein irreduzibles quadratisches Polynom:

$$x^2 + x + 1.$$

Ausführung der Division lehrt, daß $x^5 - x^2 + 1$ durch alle diese Polynome nicht teilbar ist (mod 2). Man sieht das auch direkt aus

$$x^5 - x^2 + 1 = x^2(x^3 - 1) + 1 \equiv x^2(x + 1)(x^2 + x + 1) + 1.$$

Also ist $f(x)$ irreduzibel.

§ 32. Die Durchführung der Faktorzerlegung in endlichvielen Schritten

Wir haben zwar die theoretische Möglichkeit eingesehen, bei gegebenem Körper Σ jedes Polynom aus $\Sigma[x_1, \ldots, x_n]$ in Primfaktoren zu zerlegen, und in einigen Fällen auch die Mittel aufgezeigt, die Zerlegung wirklich anzugeben bzw. die Unmöglichkeit einer Zerlegung darzutun; aber eine allgemeine Methode, die Zerlegung in jedem Fall in endlichvielen Schritten durchzuführen, besitzen wir noch nicht. Eine solche Methode wollen wir wenigstens für den Fall, daß Σ der Körper der rationalen Zahlen ist, angeben.

Man kann nach § 30 jedes rationalzahlige Polynom ganzzahlig voraussetzen und seine Zerlegung im ganzzahligen Polynombereich vornehmen. Im Ring $\mathbb{Z}$ der ganzen Zahlen selbst ist jede Primfaktorzerlegung offenbar durch endliches Ausprobieren durchführbar; außerdem gibt es dort nur endlichviele Einheiten ($+1$ und -1), also nur endlichviele mögliche Zerlegungen. Auch im Polynombereich $\mathbb{Z}[x_1, \ldots, x_n]$ gibt es nur die Einheiten $+1, -1$. Durch vollständige Induktion nach der Variablenzahl n wird nun alles auf das folgende Problem zurückgeführt:

In $\mathfrak{S}$ sei jede Faktorzerlegung in endlichvielen Schritten ausführbar; außerdem gebe es in $\mathfrak{S}$ nur endlichviele Einheiten. Gesucht wird eine Methode, jedes Polynom aus $\mathfrak{S}[x]$ in Primfaktoren zu zerlegen.

Die Lösung ist von KRONECKER gegeben worden.

Es sei $f(x)$ ein Polynom n-ten Grades in $\mathfrak{S}[x]$. Wenn $f(x)$ zerlegbar ist, so hat einer der Faktoren einen Grad $\leqq n/2$; ist also s die größte ganze Zahl $\leqq n/2$, dann haben wir zu untersuchen, ob $f(x)$ einen Faktor $g(x)$ vom Grade $\leqq s$ hat.

Wir bilden die Funktionswerte $f(a_0), f(a_1), \ldots, f(a_s)$ an $s + 1$ beliebig gewählten ganzzahligen Stellen $a_0, a_1, \ldots, a_s$. Soll nun $f(x)$ durch $g(x)$ teilbar sein, so muß $f(a_0)$ durch $g(a_0)$, $f(a_1)$ durch $g(a_1)$ usw. teilbar sein. Da aber jedes $f(a_i)$ in $\mathfrak{S}$ nur endlichviele Teiler besitzt, so kommen für jedes $g(a_i)$ nur endlichviele Möglichkeiten in Betracht, die man nach Voraussetzung alle auffinden imstande ist. Zu jeder möglichen Kombination von Werten $g(a_0)$, $g(a_1), \ldots, g(a_s)$ gibt es nach den Sätzen von § 29 genau ein Polynom $g(x)$, welches man jeweils explizite aufstellen kann. Damit hat man endlichviele Polynome $g(x)$ gefunden, die als Teiler in Betracht kommen. Von jedem dieser Polynome $g(x)$ kann man nun durch den Divisionsalgorithmus feststellen, ob es wirklich ein Teiler von $f(x)$ ist. Ist keines der möglichen $g(x)$, abgesehen von den Einheiten, Teiler von $f(x)$, so ist $f(x)$ unzerlegbar; im anderen Fall hat man eine Zerlegung gefunden und kann auf die beiden Faktoren dasselbe Verfahren anwenden, usw.

Im ganzzahligen Fall ($\mathfrak{S} = \mathbb{Z}$) kann man das Verfahren oft ganz erheblich abkürzen. Zunächst läßt sich durch Zerlegung des gegebenen Polynoms modulo 2 und eventuell noch modulo 3 eine Übersicht darüber gewinnen, welche Gradzahlen die möglichen Faktorpolynome $g(x)$ haben können und welchen Restklassen die Koeffizienten modulo 2 und 3 angehören. Das schränkt die Anzahl der möglichen $g(x)$ schon erheblich ein. Sodann kann man bei Anwendung der Newtonschen Interpolationsformel beachten, daß der letzte Koeffizient λ_s ein Teiler des höchsten Koeffizienten von $f(x)$ sein muß, was wieder eine Einschränkung der Möglichkeiten bedeutet. Schließlich benutzt man oft mit Vorteil mehr als $s + 1$ Stellen a_i. Man verwendet dann zur Bestimmung der möglichen $g(a_i)$ diejenigen $f(a_i)$, welche am wenigsten Primfaktoren enthalten; die übrigen Stellen können nachher benutzt werden um die Anzahl der Möglichkeiten noch weiter einzuschränken, indem man für jedes errechnete $g(x)$ erst prüft, ob es an den noch nicht berücksichtigten Stellen a_i Werte annimmt, die Teiler des jeweiligen $f(a_i)$ sind.

Aufgaben. 1. Man zerlege

$$f(x) = x^5 + x^4 + x^2 + x + 2$$

in $\mathbb{Z}[x]$.

2. Man zerlege

$$f(x, y, z) = -x^3 - y^3 - z^3 + x^2(y + z) + y^2(x + z) + z^2(x + y) - 2xyz$$

in $\mathbb{Z}[x, y, z]$.

§ 33. Symmetrische Funktionen

Es sei $\mathfrak{o}$ ein Ring mit Einselement.

Ein Polynom aus $\mathfrak{o}[x_1, \ldots, x_n]$, das bei jeder beliebigen Permutation der Unbestimmten $x_1, \ldots, x_n$ in sich übergeht, heißt eine (ganze rationale) *symmetrische Funktion* der Variablen $x_1, \ldots, x_n$.

Beispiele: Summe, Produkt, Potenzsumme $s_\varrho = \sum_{\nu=1}^{n} x_\nu^\varrho$.

Setzt man mit einer neuen Unbestimmten z

$$(1) \qquad \begin{cases} f(z) = (z - x_1)(z - x_2) \ldots (z - x_n) \\ \quad = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n, \end{cases}$$