Jarník's Notes of the Lecture Course Allgemeine Idealtheorie by B. L. van der Waerden (Göttingen 1927/1928)

Van der Waerden's Allgemeine Idealtheorie

In: Jindřich Bečvář (author); Martina Bečvářová (author): Jarník's Notes of the Lecture Course Allgemeine Idealtheorie by B. L. van der Waerden (Göttingen 1927/1928). (German). Praha: Matfyzpress, 2020. pp. 111–184.

Persistent URL: http://dml.cz/dmlcz/404382

Van der Waerden

Allgemeine Idealtheorie

Göttingen, Wintersem. 1927–28

$\frac{4}{\text{XI}}$

§ 1. Einleitung

Man ist auf verschiedenen Wegen zu dem Idealbegriff bekommen. Erstens hat es sich gezeigt, dass in algebraischen Zahlkörpern[1] die Zerlegung in unzerlegbare Faktoren nicht immer eindeutig ist. Z.B. im Körper $P(\sqrt{-5})$; hier sind die ganzen Zahlen die Zahlen $a + b\sqrt{-5}$, a, b ganz rational.[2] Es ist

$$9 = 3 \cdot 3 = \big(2 - \sqrt{-5}\big)\big(2 + \sqrt{-5}\big);$$

und doch sind 3, $2 - \sqrt{-5}$, $2 + \sqrt{-5}$ unzerlegbar. Denn eine ganze Zahl α dieses Körpers $\alpha = a + b\sqrt{-5}$ hat ihre Norm

$$N\alpha = |\alpha|^2 = a^2 + 5b^2; \tag{1}$$

wäre nun 3 zerlegbar, $3 = \alpha\beta$, so müsste $9 = N3 = N\alpha\, N\beta$ sein, also entweder $N\alpha = 3$, $N\beta = 3$, was aber nach (1) unmöglich ist, oder $N\alpha = 1$, $N\beta = 9$; dann wäre aber notwendig $\alpha = \pm 1$, was keine eigentliche Zerlegung ist. Aus demselben Grunde ist auch $2 \pm \sqrt{-5}$ unzerlegbar.

Um die Eindeutigkeit hier wiederherzustellen, hat Kummer sog. ideale Teiler eingeführt; aber erst Dedekind hat diesen Begriff präzisiert und für allgemeine Zahlkörper die Theorie durchgeführt.

Seine Definition des Ideals lautet: Eine Menge $\mathfrak{m}$ von ganzen Zahlen eines algebraischen Zahlkörpers heisst Ideal, wenn zugleich mit a und b auch $a \pm b$ und la zu $\mathfrak{m}$ gehören, wo l eine beliebige Zahl des Körpers ist.

Jeder Zahl c ist die Gesamtheit von allen ihren Vielfachen zugeordnet, das ist das sog. Hauptideal (c).

Unter $\big(3,\, 2 - \sqrt{-5}\,\big)$ verstehen wir nun die Menge aller Zahlen

$$t \cdot 3 + s \cdot \big(2 - \sqrt{-5}\big),$$

---

[1] The notion of *algebraischer Zahlkörper* is vague here, it means a number system.

[2] See MA-II, p. 85.

For an analogous example see MA-I, p. 66: $4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$.

References to the two volumes monographs *Moderne Algebra* from 1930, resp. 1931, will be referred to MA-I, resp. MA-II.

wo t, s alle ganzen Zahlen des Körpers $P(\sqrt{-5})$ durchläuft; das ist ein Ideal; und ähnlich in anderen Fällen.

Nun brauchen wir noch eine Teilbarkeits- und Produktdefinition.

Eine Zahl des Ideals $\mathfrak{a}$ heisst durch das Ideal $\mathfrak{a}$ teilbar; ein Ideal $\mathfrak{a}$ heisst durch ein Ideal $\mathfrak{b}$ teilbar, $\mathfrak{a} \equiv 0\ (\mathfrak{b})$, wenn alle durch $\mathfrak{a}$ teilbaren Zahlen auch durch $\mathfrak{b}$ teilbar sind.

Das Produkt $\mathfrak{a} \times \mathfrak{b}$ ist die Menge aller endlichen Summen $\sum a_i b_i$, wo a_i aus $\mathfrak{a}$, b_i aus $\mathfrak{b}$ ist.[3] Das ist ein Ideal. Daraus folgt, dass man Ideale multipliziert, wenn man ihre Basiselemente multipliziert. Z.B.

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1,\ a_1 b_2,\ a_2 b_1,\ a_2 b_2).$$

Nun lässt sich schon die Teilbarkeitstheorie durchführen; z.B. ist in $P(\sqrt{-5})$ das Ideal (3) zerlegbar, und zwar

$$(3) = (3,\ 2 - \sqrt{-5})(3,\ 2 + \sqrt{-5}),$$

und beide Faktoren rechts sind unzerlegbar.[4]

Von einer anderen Seite hier ist der Idealbegriff in Polynombereichen aufgetaucht. Kronecker hat den Begriff eines Modulsystems eingeführt: Es seien $f_1, \ldots, f_s$ Polynome in $x_1, x_2, \ldots, x_n$; ein Modulsystem $(f_1, f_2, \ldots, f_s)$ ist die Gesamtheit aller Polynome $r_1 f_1 + r_2 f_2 + \cdots + r_s f_s$, wo $r_1, r_2, \ldots, r_s$ wieder Polynome sind; dies erinnert vollständig an die Dedekindsche Idealdefinition.

(Hilbert hat umgekehrt gezeigt, dass sich jedes Ideal in Polynombereichen so schreiben lässt.)

Der Zweck war hier aber in anderer; in Polynombereichen gilt schon die eindeutige Zerlegung; im Gegenteil, eben bei den Idealen wird dies falsch. Hier handelte sich um etwas anderes: um die Präzision des Begriffes der Dimension einer algebraischen Mannigfaltigkeit, die durch $f_1 = 0$, $f_2 = 0$, $\ldots$, $f_s = 0$ definiert wird, und um ihre Zerlegung in irreduzible Faktoren. So wurde von Kronecker und König die Eliminationstheorie entwickelt.

Hilbert hat Modulsysteme für Invariantentheorie verwendet.

Max Noether betrachtete die Frage, wann sich ein Polynom in der Form $f_1 g_1 + f_2 g_2$ darstellen lässt, wenn $f_1(x, y) = 0$, $f_2(x, y) = 0$ zwei algebr. Kurven sind. Es handelt sich also wieder um Modulsysteme. Die Frage ist auch von Lasker behandelt worden.

Der Begriff des Ideals lässt sich aber auch auf algebraische Funktionen einer Veränderlichen anwenden: es sei $P(x)$ der Körper der rationalen Funktionen

[3] In the following text, the symbol $\times$ for product of ideals is not used.

[4] See MA-II, p. 86.

von x über P, $P[x]$ der zugehörige Polynombereich; $P(x, y_1, y_2, \ldots, y_r)$ sei ein Erweiterungskörper, in welchem $y_1, \ldots, y_r$ algebraische Funktionen sind.

Man definiert ganze algebraische Funktionen und Ideale und findet eine eindeutige Zerlegbarkeit von Idealen in Primideale.

Die Primideale entsprechen dann eineindeutig den Punkten der Riemannschen Fläche.

Ein Primideal wird in der allgemeiner Theorie statt durch Unzerlegbarkeit durch folgende Eigenschaft charakterisiert: Wenn $\mathfrak{ab}$ durch das Primideal $\mathfrak{c}$ teilbar is, so ist entweder $\mathfrak{a}$ oder $\mathfrak{b}$ durch $\mathfrak{c}$ teilbar.

Einen vierten Ausgangspunkt bildete die Theorie der hyperkomplexen Zahlen

$$\alpha = a_1 i_1 + a_2 i_2 + \cdots + a_r i_r,$$

wo a_k Zahlen eines reellen Körpers sind. (Frobenius, E. Noether).

Wenn eine Menge $\mathcal{M}$ so beschaffen ist, dass mit α, β auch $\alpha \pm \beta$, $\alpha\beta$ zu $\mathcal{M}$ gehören, heisst $\mathcal{M}$ ein Ring; freilich kann z.B. bei den hyperkomplexen Zahlen die kommutativität der Multiplikation fehlen.

Ein System von hyperk. Zahlen heisst ein Ideal, wenn mit α, β auch $\alpha \pm \beta$, $\gamma\alpha$, $\alpha\gamma$ (γ beliebig) zu ihm gehören – freilich braucht est nicht kommutativ zu sein.

Wir werden uns jedoch hauptsächlich mit der kommutativen Theorie beschäftigen. Die allgemeine Idealtheorie soll nun alle diese Standpunkte umfassen.

Litteratur

1.) Algebraische Zahlkörper:

Dedekind, XI Supplement in Dirichlet's Vorlesungen über Zahlentheorie.[5]

Hilbert, Zahlbegriff.[6] Landau,[7] Hecke.[8]

[5] P.G. Lejeune Dirichlet: *Vorlesungen über Zahlentheorie, herausgegeben von R. Dedekind*, Vieweg, Braunschweig, 1863, xiii + 414 pages, 2nd ed. 1871, xviii + 497 pages, 3rd ed. 1879, 1881, xvi + 627 pages, 4th ed. 1894, xvii + 657 pages.

[6] D. Hilbert: *Ueber den Zahlbegriff*, Jahresbericht der Deutschen Mathematiker Vereinigung 8(1900), pp. 180–184.

[7] E. Landau: *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Teubner, Leipzig, 1918, vii + 143 pages, 2nd ed. 1927, vii + 147 pages, reprint: Chelsea, New York, 1949.
E. Landau: *Vorlesungen über Zahlentheorie. I. Aus der elementaren und additiven Zahlentheorie. II. Aus der analytischen und geometrischen Zahlentheorie. III. Aus der algebraischen Zahlentheorie und über die Fermatsche Vermutung*, Hirzel, Leipzig, 1927, xii + 360, viii + 308, viii + 342 pages.

[8] E. Hecke: *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Ver-

2.) Modulsysteme:

F.S. Macaulay, Modular Systems, Cambr. Tracts 19.[9] V. d. Waerden, Nullstellentheorie …, Math. Ann. 96.[10]

3.) Funktionenkörper:

Dedekind – Weber, Algebr. Funkt. einer Veränderlichen, Crelle's J. 92.[11]

4.) Allgemeine Theorie:

E. Noether, Idealtheorie in Ringbereichen, Math. Ann. 83.[12]

Abstrakter Aufbau …, Math. Ann. 96.[13]

7
XI

§ 2. Gruppen

Eine Gruppe ist eine Menge, worin zu jedem geordneten Paar von Elementen a, b wieder ein Element ab der Menge als ihr „Produkt" definiert ist, wobei folgendes gilt:

1.) $(ab)c = a(bc)$ (assoziatives Gesetz),

---

lagsgesellschaft, Leipzig, 1923, viii + 265 pages, 2nd ed. (herausgegeb. von Wilhelm Maak), Geest & Portig K.-G., 1954, viii + 264 pages. Reprint: Chelsea, New York, 1948, viii + 266 pages, 2nd ed. Chelsea, Bronx, New York, 1970, viii + 274 pages. English translation (George U. Brauer and Jay R. Goldman with the assistance of R. Kotzen): *Lectures on the Theory of Algebraic Numbers*, Graduate texts in Mathematics 77, Springer, New York, Heidelberg, Berlin, 1981, xii + 239 pages.
Erich Hecke (1887–1947) studied in Breslau (Wrocław) and Berlin, graduated in Göttingen under the supervision of David Hilbert in 1910. Hecke became a professor in Basel (1915), Göttingen (1918) and Hamburg (1919). He was interested in algebraic numbers, functional equations for the zeta function, the theory of modular forms, the general theory of cusp form, L-functions and ideal class characters. Wilhelm Maak (1912–1992) was his student.

[9] F.S. Macaulay: *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics 19, Cambridge University Press, Cambridge, 1916, xiv + 112 pages. Reprint: *With a new introduction by Paul Roberts*, Cambridge Mathematical Library, Cambridge University Press, 1994, xxxi + 112 pages.
Francis Sowerby Macaulay (1862–1937) studied in Cambridge (1879–1882). From 1883 until 1885, he taught mathematics at Kingswood School in Bath, from 1885 until 1911, he worked as Mathematics Master at the St. Paul's School in London. He dealt with algebra, algebraic geometry and number theory.

[10] B.L. van der Waerden: *Zur Nullstellentheorie der Polynomideale*, Mathematische Annalen 96(1926), pp. 183–208.

[11] R. Dedekind, H. Weber: *Theorie der algebraischen Functionen einer Veränderlichen*, Journal für die reine und angewandte Mathematik 92(1882), pp. 181–291.

[12] E. Noether: *Idealtheorie in Ringbereichen*, Mathematische Annalen 83(1921), pp. 24–66.

[13] E. Noether: *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkörpern*, Mathematische Annalen 96(1926), pp. 26–61.

2.) zu jedem a und jedem b aus $\mathcal{M}$ gibt es wenigstens ein x aus $\mathcal{M}$ mit $ax = b$ und wenigstens ein y aus $\mathcal{M}$ mit $ya = b$.

Wenn auch $ab = ba$ (kommutatives Gesetz), so heisst die Gruppe Abelsch.

Z.B. Alle rationalen Zahlen ausser 0 bilden eine Gruppe gegenüber der gewöhnlichen Multiplikation.

Alle rationalen, oder alle ganzen Zahlen bilden eine Gruppe gegenüber der gewöhnlichen Addition. Wir werden oft solche „additive Gruppen“ betrachten.[14]

Alle linearen Transformationen mit n Veränderlichen mit nicht verschwindender Determinante bilden eine (nicht Abelsche) Gruppe, wenn wir die Multiplikation der Transformationen

$$x_i' = \sum_k a_{ik} x_k, \qquad x_i'' = \sum_k b_{ik} x_k'$$

durch ihre Zusammensetzung definieren:

$$x_i'' = \sum_k c_{ik} x_k, \qquad \text{wo} \qquad c_{ik} = \sum_r b_{ir} a_{rk}.$$

Wir deuten diese lineare Transformationen oft durch ihre Matrizen A, B, C an und schreiben dann[15]

$$C = AB.$$

Die Permutationen[16] einer Menge $\mathcal{M}$, d.h. die eineindeutigen Abbildungen der Menge $\mathcal{M}$ auf sich selbst mittels einer Funktion σ:

$$\overline{a} = \sigma(a),$$

bilden eine Gruppe, wenn die Multiplikation durch

$$(\sigma\tau)(a) = \sigma(\tau(a))$$

definiert ist.

---

[14] See MA-I, pp. 15–16.
In MA-I, p. 15, van der Waerden introduced a group as a set with an associative binary operation satisfying an axiom of left identity and an axiom of left inverses. In turn, he proved that these two axioms can be replaced by the equivalent axiom of solvability of the equations $ax = b$ and $ya = b$, in the case of finite sets by the axiom of uniqueness of a solution of these equations. In these lectures, he proceeded the other way around. From the axiom of solvability of the equations $ax = b$ and $ya = b$, he proved the existence of (leftside and doubleside) identity and (leftside and doubleside) inverses. In turn he showed that the existence and uniqueness of a solution of the above equations follows from these two axioms. In the definition of a group it is necessary to assume a non-empty set $\mathcal{M}$, which in MA-I, p. 15, is not necessary.

[15] In the contemporary approach it should be $C = BA$. See MA-II, pp. 111–112.

[16] See MA-I, pp. 16–17.

Einige Folgerungen aus der Definition:[17]

I. Aus 1.) allein (ohne Benutzung von 2.)) folgt: In einem zusammengesetzten Produkt wie $\big((ab)(cd)\big)e$ kommt es nicht darauf an, wie die Klammern angeordnet sind; insbesondere ist also z.B.

$$\big((ab)(cd)\big)e = \big(((ab)c)d\big)e \qquad (\underline{\text{Normalform}}).$$

Beweis. Durch Induktion. Es sei dies für k Faktoren bewiesen (für $k = 3$ stimmt es nach 1.)); es sei nun ein Produkt von $k+1$ Elementen in der Form $(\dots\dots)(\dots)$ gegeben; wenn in der zweiten Klammer nur 1 Element steht, so führe ich die erste Klammer von k Elementen auf die Normalform, wodurch schon der ganze Produkt die Normalform hat. Sonst bringe ich die zweite Klammer in der Normalform

$$(\quad)(\,(\quad)f\,);$$

das ist nach 1.) gleich

$$\underbrace{(\,(\quad)(\quad)\,)}\,f$$

und diese Klammer von k Elementen bringe ich auf die Normalform, womit alles bewiesen ist.

Daher lassen wir im folgenden Klammern überhaupt weg, wenn es uns angenehm sein wird.

In den Abelschen Gruppen kann man auch die Reihenfolge eines zusammengesetzten Produktes beliebig ändern; denn z.B.

$$a_1a_2a_3a_4\cdots = a_1(a_2a_3)a_4\cdots = a_1(a_3a_2)a_4\cdots = a_1a_3a_2a_4\dots,$$

und durch solche Vertauschungen von je zwei benachbarten Faktoren kann ich jede Anordnung erreichen.

Ich definiere in nun Potenzen durch Induktion: $a^1 = a,\ \ a^{n+1} = a^n \cdot a.$

Es ist $a^{m+n} = a^m a^n \quad (m, n > 0$ ganz).

Denn für $n = 1$ ist es die Definition von a^{m+1}, für $n > 1$ machen wir den Beweis durch Induktion; er sei also für ein n richtig:

$$a^m \cdot a^{n+1} = a^m(a^n \cdot a^1) = (a^m a^n) \cdot a^1 = a^{m+n} \cdot a^1 = a^{(m+n)+1} = a^{m+n+1}.$$

Ebenso beweist man $(a^m)^n = a^{mn}$.

Falls die Gruppe Abelsch ist, so gilt offenbar noch weiter

$$(ab)^n = a^n b^n.$$

[17] See MA-I, pp. 20–23.

II. Wir benutzen jetzt auch 2.).

Ich behaupte: es gibt ein e, so dass $ea = a$ für alle a gilt.

Beweis. Ich wähle ein b und löse die Gleichung $xb = b$; die Lösung nenne ich e, also $eb = b$. Es sei nun a beliebig; es gibt ein c mit $bc = a$; also $eb = b$, $(eb)c = bc$, $e(bc) = bc$, $ea = a$ w.z.b.w.

Ebenso beweist man die Existenz eines e', so dass

$$ae' = a \qquad \text{für alle} \quad a.$$

Dann ist

$$e' = ee' = e\,;$$

es ist also jedes solche e jedem solchen e' gleich. Es gibt also nur eine linksseitige Einheit (d.h. Element mit $ea = a$) und nur eine rechtsseitige Einheit (d.h. e' mit $ae' = a$) und sie sind einander gleich. Dieses Element heisst Einheit der Gruppe.

Weiter gibt es zu jedem a ein linksseitiges inverses Element a^{-1}, d.h. ein a^{-1} mit $a^{-1}a = e$, wo e die Einheit bedeutet; das folgt aus 2.).

Wir können nun 2.) ersetzen durch die Forderung der Existenz einer linksseitigen Einheit und eines linksseitigen inversen Elementes.

Denn: wir bilden

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

Wir multiplizieren mit $(a^{-1})^{-1}$:

$$a \cdot a^{-1} = (a^{-1})^{-1}a^{-1} = e$$

Es ist also das linksseitige inverse zugleich das rechtsseitige inverse Element. Dann ist $ae = a \cdot a^{-1}a = ea = a$, also e ist zugleich eine rechtsseitige Einheit. Und $ax = b$, $ya = b$ sind also immer lösbar, nämlich durch $x = a^{-1}b$, $y = ba^{-1}$.

Satz. Aus $ax = ay$ folgt $x = y$.

Denn $a^{-1}ax = a^{-1}ay$, $\quad ex = ey$, $\quad$ also $\quad x = y$.

Jetzt wollen wir a^0, a^{-n} definieren:[18] und zwar durch

$$a^{n-m} = a^n \cdot (a^{-1})^m \qquad (n, m \ \text{ganz} \ > 0). \tag{2}$$

Die rechte Seite hängt nur von $n - m$ ab; denn wenn $n' - m' = n - m$ und z.B. $n' = n + p$, $m' = m + p$ $(p > 0)$, so ist

$$a^{n+p} \cdot (a^{-1})^{m+p} = a^n \underbrace{aaa\ldots}_{p \text{ mal}} \ \underbrace{a^{-1}a^{-1}a^{-1}\ldots}_{p \text{ mal}} \ (a^{-1})^m = a^n(a^{-1})^m.$$

[18] The next passage is not too smooth. In MA-I, p. 22, the author avoided it.

Also ist (2) in der Tat eine Definition.

Es ist insbesondere $a^0 = a^1(a^{-1})^1 = e,\ a^{-n} = (a^{-1})^n$.

Nun ist es leicht, $a^n a^m = a^{n+m},\ (a^n)^m = a^{nm}$ allgemein (für $n, m \gtreqless 0$) zu zeigen. Denn z.B:

$$a^n = a^N(a^{-1})^{N'},$$
$$a^m = a^M(a^{-1})^{M'} \qquad (N, N', M, M' > 0),$$

dann: $$a^n \cdot a^m = a^N(a^{-1})^{N'}a^M(a^{-1})^{M'}.$$

Alles ist vertauschbar, da $aa^{-1} = a^{-1}a = e$. Also

$$a^n \cdot a^m = a^{N+M}(a^{-1})^{N'+M'} = a^{n+m}.$$

Ebenso bei $(a^n)^m$.

Sehr oft werden wir die Einheit e mit 1 bezeichnen.

Abelsche Gruppen

Diese werden wir oft additiv schreiben; d.h. $a + b$ statt ab; die Einheit nennen wir dann 0, statt a^{-1} schreibt man $-a$, statt a^n schreibt man na. Dann ist

$$na + ma = (n + m)a,$$
$$n(ma) = nma,$$
$$n(a + b) = na + nb.$$

Hier bedeuten n, m ganze rationale Zahlen, a, b Elemente der Gruppe. Die letzte Gleichung gilt freilich im allgemeinen nur für Abelschen Gruppen.[19]

Untergruppen

Eine Untergruppe einer Gruppe $\mathcal{M}$ ist eine Teilmenge von $\mathcal{M}$, die selbst eine Gruppe ist. Dazu genügt es, dass sie mit a und b auch ab und a^{-1} enthält; denn die Einheit e ist in ihr dann wegen $a^{-1}a = e$ auch enthalten und das assoziative Gesetz ist von selbst erfüllt.[20]

Z.B.: die geraden Permutationen, die $\prod_{1 \le i < k \le n}(x_i - x_k)$ unverändert lassen, oder die linearen Substitutionen, die $\sum_{i=1}^{n} x_i^2$ unverändert lassen, bilden eine Gruppe.

---

[19] See MA-I, pp. 22–23.

[20] See MA-I, pp. 23–24.

The subset in question must be non-empty.

Es seien a, b, ... irgendwelche Elemente einer Gruppe $\mathcal{G}$; die „von a, b, ... erzeugte Gruppe“ $\mathcal{H}$ ist die Menge aller Potenzprodukte von a, b, ..., d.h. aller Elemente der Form wie

$$a^{-1}b^2a^4c^{-2}de^3 \dots f^4.$$

Das ist eine Gruppe, denn sowohl ein Produkt von zwei Potenzprodukten wie das Inverse eines Potenzproduktes (in unserem Beispiel $f^{-4} \dots e^{-3}d^{-1}c^2a^{-4}b^{-2}a$) sind auch Potenzprodukte. $\mathcal{H}$ ist auch Durchschnitt aller Untergruppen von $\mathcal{G}$, die die Elemente a, b, ... enthalten.

Eine von einem einzigen Element a erzeugte Gruppe heisst zyklische Gruppe; ihre Elemente sind a^m; sie ist offenbar Abelsch; denn $a^m a^n = a^{m+n} = a^n a^m$.

Zwei Gruppen $\mathcal{G}$, $\overline{\mathcal{G}}$ sind isomorph oder vom selben Typus (Zeichen: $\mathcal{G} \cong \overline{\mathcal{G}}$), wenn ihre Elemente so eineindeutig zugeordnet werden können, dass dem Produkt zweier Elemente aus $\mathcal{G}$ wieder der Produkt der zugeordneten Elemente aus $\overline{\mathcal{G}}$ zugeordnet wird.[21]

Struktur zyklischer Gruppen

Hier sind zwei Fälle möglich:[22]

1.) Entweder ist stets $a^m \neq a^n$ für $m \neq n$. Die Zusammensetzung ist durch $a^n a^m = a^{n+m}$ vollständig bestimmt, der Typus ist bestimmt, die Gruppe ist isomorph mit der additiven Gruppe der ganzen rationalen Zahlen.

2.) Oder es ist $a^m = a^n$ für irgendein m und n mit $m \neq n$, z.B. mit $m > n$; dann ist $a^{m-n} = e$. Es sei q die kleinste positive Zahl mit $a^q = e$; dann sind 1, a, a^2, ..., a^{q-1} untereinander (1 dasselbe wie e) verschieden und die Zusammensetzung ist auch durch $a^n \cdot a^m = a^{n+m}$ vollständig bestimmt mit dem Zusatz, dass auf der rechten Seite $n+m$ durch den Rest von $n+m$ modulo q ersetzt werden soll. Also sind auch alle zyklische Gruppen der Ordnung q isomorph. (Ordnung der Gruppe ist die Anzahl ihrer Elemente, wenn die Gruppe endlich ist, oder ihre Mächtigkeit, wenn sie unendlich ist.)

---

[21] See MA-I, pp. 29–30.
In MA-I, p. 29, a more general notion of an isomorphism of sets with some stucture is given: *... so daß die Relationen, die zwischen irgend welchen Elementen $a, b, \dots$ von $\mathfrak{M}$ bestehen, auch zwischen den zugeordneten Elementen $\overline{a}, \overline{b}, \dots$ bestehen und umgekehrt, so nennt man die beiden Mengen isomorph (bezüglich der fraglichen Relationen) ...*
Neither in MA-I nor in MA-II the term *vom selben Typus* appears, in the lecture van der Waerden occasionally used it, see for example the beginning of Section 5 of the second chapter.

[22] See MA-I, pp. 25–26.

11
XI

Bei einer additiven Abelschen Gruppe schreiben wir $a - b$ oder $-b + a$ für die Lösung von $b + x = a$.[23]

Untergruppen von additiven Abelschen Gruppen heissen Moduln. Damit eine Teilmenge einer Abelschen additiven Gruppe ein Modul sei, ist es notwendig und hinreichend, dass sie mit a, b auch $a - b$ enthält; denn dann enthält sie auch $a - a = 0$, $0 - a = -a$, $a - (-b) = a + b$.[24]

§ 3. Ringe

Zahlenringe hat zuerst Hilbert betrachtet; abstrakt bei E. Noether, Math. Ann. 83.[25] Einfacher bei Hasse, Höhere Algebra I.[26]

Ein Ring ist eine Menge von Elementen, in welcher zu a, b aus der Menge $a + b$ und ab definiert sind, die folgenden Voraussetzungen genügen:

I 1.) $(a + b) + c = a + (b + c)$

2.) $a + b = b + a$

3.) bei jedem a, b ist $a + x = b$ lösbar

II 1.) $a(bc) = (ab)c$

2.) $ab = ba$

III 1.) $a(b + c) = ab + ac$

2.) $(b + c)a = ba + ca$

Es werden auch Ringe betrachtet, wo II 2.) nicht gilt (nichtkommutative Ringe). Wir beschränken uns aber auf kommutative Ringe, wo freilich III 2.) dann überflüssig ist.

Der Ring bildet also eine Abelsche Gruppe gegenüber Addition; es gibt also eine 0 mit $a + 0 = a$, ein $-a$ zu jedem a mit $a + (-a) = 0$; dann gibt es genau eine Lösung $-b + a = a - b$ von $b + x = a$. Dann ist weiter

$$(n + m)a = na + ma, \quad n(a + b) = na + nb, \quad (nm) \cdot a = n \cdot (ma)$$

[23] See MA-I, p. 19.

[24] See MA-I, p. 26.
The term *Modul* is no longer used for a subgroup of an Abelian group. In MA-I, p. 19, the term *Modul* is used for an additivelly written Abelian group.
In addition, the subset (to be a subgroup) must be non-empty.

[25] E. Noether: *Idealtheorie in Ringbereichen*, Mathematische Annalen 83(1921), pp. 24–66.

[26] H. Hasse: *Höhere Algebra I. Lineare Gleichungen, II. Gleichungen höheren Grades*, Sammlung Göschen 931, 932, W. de Gruyter, Berlin, 1926, 1927, 160 + 160 pages.

(m, n ganze rationale Zahlen); das ist eine direkte Folge unserer Gruppenergebnisse.[27]

Im Produkt darf man ausklammern und beliebig vertauschen, endlich Potenzen mit positiven Exponenten definieren (denn dies folgte im § 2 nur aus dem assoziativen und kommutativen Gesetz):

$$a^1 = a, \quad a^{n+1} = a^n \cdot a; \quad a^n a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad (ab)^n = a^n b^n.$$

Auch für Differenzen gilt freilich das distributive Gesetz[28]

$$a(b - c) = ab - ac;$$

denn es ist $ac + a(b - c) = a\big(c + (b - c)\big) = ab$.

Weiter erweitert man sofort die Gültigkeit des distributiven Gesetzes auch für Summen und Differenzen mit mehreren Summanden:

$$a(b \pm c \pm d \dots) = ab \pm ac \pm ad \dots$$

auch so:

$$(a + b)(c + d) = ac + bc + ad + bd.$$

Kurz: man darf in der üblichen Weise addieren, subtrahieren und multiplizieren.

Alles dies auch dann, wenn dazwischen ganze rationale Zahlen gemischt werden; z.B.

$$a(b + b + \dots) = ab + ab + \dots = n \cdot (ab),$$

also

$$a \cdot (nb) = n \cdot (ab), \qquad (na) \cdot b = n \cdot (ab).$$

Besonders wichtig sind einige Spezialfälle von Ringen:[29]

1.) Ring mit Einheitselement. D.h. es gibt ein e, so dass $ae = a$ für alle a gilt. Es kann nur eine solche Einheit geben; gäbe es noch eine e', so wäre $e' = ee' = e$.

2.) Ring ohne Nullteiler. Es ist $a(b - c) = ab - ac$, speziell für $c = b$: $a \cdot 0 = ab - ab = 0$; also $a \cdot 0 = 0$ für alle a. Wenn umgekehrt gilt: aus $a \neq 0$, $ab = 0$ folgt $b = 0$, so reden wir von einem Ring ohne Nullteiler.

---

[27] In contrast, in MA-I, pp. 36–37, a more general definition is given.
Van der Waerden introduced commutative rings here. It is not clear why he introduced both distributive laws here as axioms. However, he pointed out it in the following remark.

[28] See MA-I, pp. 38–41.

[29] See MA-I, pp. 39–40.

Beispiel eines Ringes mit Nullteiler: die Gesamtheit aller Funktionen, die nur für 2 Werte der Veränderlichen definiert sind und dort ganzzahlige Werte annehmen. Man kann diesen Ring durch Paare (a_1, a_2) darstellen, mit den Regeln

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$
$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Es ist also $(a_1, 0)(0, b_2) = (0, 0)$.

Auf diese Weise kann man aus zwei Ringen $\mathcal{O}_1$, $\mathcal{O}_2$ ein Ring von Elementpaaren bilden – die sog. direkte Summe von $\mathcal{O}_1$ und $\mathcal{O}_2$.

3.) Körper.[30] Ein Ring heisst Körper, wenn in ihm gilt:

IV 1.) es gibt ein $a \neq 0$

2.) $ax = b$ hat eine Lösung für $a \neq 0$

3.) $xa = b$ hat eine Lösung für $a \neq 0$

Bei kommutativen Ringen ist freilich IV 3.) überflüssig.

In Körpern gibt es immer Einheit: denn für ein $a \neq 0$ bestimmen wir e mit $ae = a$; dann bei beliebigem b bestimmen wir c so dass $ac = b$; also $be = e(ac) = (ea)c = ac = b$.

Zu jedem Element $\neq 0$ gibt es auch ein Inverses, d.h. die Lösung von $a \cdot x = e$, welches wir mir a^{-1} bezeichnen.[31]

Weiter ist der Körper ein Ring ohne Nullteiler; denn aus[32]

$$ab = 0, \quad a \neq 0 \quad \text{folgt} \quad a^{-1}ab = 0, \quad eb = 0, \quad b = 0.$$

Wie bei Gruppen sieht man ein, dass man statt IV 2.), 3.) die Existenz der Einheit und des inversen Elementes fordern kann.

Im Körper, und allgemeiner im Ring ohne Nullteiler, gilt:

$$\text{aus} \quad b \neq 0, \quad bx = by \qquad \text{folgt} \qquad x = y.$$

Denn

$$b(x - y) = 0, \quad \text{also} \quad x - y = 0.$$

Man darf also durch b kürzen, und die Division ist eindeutig (wenn durchführbar).

---

[30] See MA-I, p. 41–42.

[31] See MA-I, p. 42.
The commutativity of multiplication was used substantially. More generally: for given $a \neq 0$, b there exist e, c such that $ea = a$, $ac = b$. Hence $eb = e(ac) = (ea)c = ac = b$, i.e., e is the left identity. Similarly, we prove the existence of the right identity f. Therefore, $e = ef = f$ is an identity. If u, v is right, resp. left inverse of a, i.e. $au = e$, $va = e$, then $u = (va)u = v(au) = v$ is the inverse of a.

[32] See MA-I, p. 42.

Für die Lösung von $bx = a$ schreiben wir im Körper (für $b \neq 0$) $\frac{a}{b}$.[33] Im Körper gilt

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$

denn ich soll zeigen $\frac{a}{b} \cdot \frac{c}{d} \cdot bd = ac$; es ist aber $\frac{a}{b} \cdot b = a$, $\frac{c}{d} d = c$, w.z.b.w. Ebenso

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}.$$

Ein Ring ohne Nullteiler heisst auch ein Integritätsbereich.[34]

Ein Integritätsbereich mit endlich vielen, aber mehr als einem Element, ist ein Körper.

Denn: es seien $a_1, a_2, \ldots, a_n$ alle seine Elemente; $a \neq 0$ ein von ihnen. Dann sind auch $aa_1, aa_2, \ldots, aa_n$ alle Elemente, da sie verschieden sind; denn aus $aa_i = aa_k$ folgt $a(a_i - a_k) = 0$, $a_i = a_k$.

Wenn also b ein beliebiges Element ist, so ist $aa_i = b$ bei geeignetem a_i.[35]

In zwei Bereichen $\mathcal{O}$, $\overline{\mathcal{O}}$ sei Addition und Multiplikation definiert; man sagt, dass $\mathcal{O}$ zu $\overline{\mathcal{O}}$ meromorph ist, wenn jedem a aus $\mathcal{O}$ ein $\overline{a}$ aus $\overline{\mathcal{O}}$ so zugeordnet ist,[36] dass $\overline{a}$ ganz $\overline{\mathcal{O}}$ durchläuft, wenn a ganz $\mathcal{O}$ durchläuft; und wenn aus $a \to \overline{a}$, $b \to \overline{b}$ folgt $a + b \to \overline{a} + \overline{b}$, $ab \to \overline{a}\,\overline{b}$.[37]

Wenn die Zuordnung überdies eineindeutig ist, so heissen $\mathcal{O}$, $\overline{\mathcal{O}}$ isomorph, $\mathcal{O} \cong \overline{\mathcal{O}}$.

Wenn $\mathcal{O} \cong \overline{\mathcal{O}}$ und $\mathcal{O}$ Ring, so ist auch $\overline{\mathcal{O}}$ Ring, wenn $\mathcal{O}$ Ring ohne Nullteiler, so auch $\overline{\mathcal{O}}$ Ring ohne Nullteiler u.s.w. Beim Meromorphismus ist es nicht so einfach; aber es gibt mindestens folgendes:

Wenn $\mathcal{O}$ meromorph zu $\overline{\mathcal{O}}$ und $\mathcal{O}$ ein Ring, so auch $\overline{\mathcal{O}}$ ein Ring.[38]

Beweis. Zu drei Elementen $\overline{a}$, $\overline{b}$, $\overline{c}$ aus $\overline{\mathcal{O}}$ suchen wir irgendwelche entsprechende a, b, c aus $\mathcal{O}$; dann ist

---

[33] In MA-I, pp. 41–44, the fraction notation $\frac{a}{b}$ is not used, apparently because the multiplication is not generally commutative.

[34] See MA-I, p. 39.
The commutativity of multiplication is tacitly assumed. Let us underline that in his lecture and in MA-I, van der Waerden does not assume the existence of an identity in integral domains.

[35] See MA-I, p. 43.

[36] Bezeichnung $a \to \overline{a}$. [The note in Jarník's records.]

[37] See MA-I, pp. 44–46.
Today we are speaking about epimorphism $\mathcal{O} \to \overline{\mathcal{O}}$, resp. about homomorphism of ring $\mathcal{O}$ onto ring $\overline{\mathcal{O}}$. The notion *Bereich* is not specified more precisely here. In MA-I, pp. 37, 44, van der Waerden speaks about a system of double composition – *System mit doppelter Komposition.*

[38] See MA-I, p. 45: *Das homomorphe Bild eines Ringes ist wieder ein Ring.*

$$a + (b + c) = (a + b) + c;$$

also $$\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c};$$

ebenso bei den weiteren Rechenregeln. Was die Subtraktion betrifft: zu $\overline{a}$, $\overline{b}$ finden wir irgendwelche zugeordnete a, b und x mit $b + x = a$; dann ist

$$\overline{b} + \overline{x} = \overline{a}.$$

Wenn überdies $\mathcal{O}$ ein Einheitselement hat, so auch $\overline{\mathcal{O}}$; denn aus $ae = a$ für alle a folgt $\overline{a}\,\overline{e} = \overline{a}$ für alle $\overline{a}$.

Für Ring ohne Nullteiler braucht eine analoge Beziehung nicht zu gelten.

Wir werden nun systematisch untersuchen, wie man aus Ringen wieder Ringe bilden kann.

§ 4. Quotientenkörper. Ringbildung I

Wenn sich ein Ring $\mathcal{O}$ in einen Körper Ω einbetten lässt, so hat $\mathcal{O}$ sicher keine Nullteiler.

Es sei ein Ring $\mathcal{O}$ von mindestens 2 Elementen in einem Körper Ω enthalten:[39] $\mathcal{O} \subseteq \Omega$. Ich bilde in Ω alle Quotienten $\frac{a}{b}$, wo a, b zu $\mathcal{O}$ gehören und $b \neq 0$. Die bilden einen Körper; denn einen Ring bilden sie, da

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

und dann ist auch die Division durchführbar, denn

$$\frac{a}{b} \cdot x = \frac{c}{d} \quad \text{ist durch} \quad x = \frac{bc}{ad}$$

lösbar, falls $\frac{a}{b} \neq 0$. Dies ist der Quotientenkörper, der „kleinste Körper“, der in Ω liegt und $\mathcal{O}$ enthält. Er enthält 0, da $0 = \frac{0}{r}$, wo r ein von Null verschiedenes Element von $\mathcal{O}$ ist, und weiter ist jedes von Null verschiedenes Element b von $\mathcal{O}$ auch in der Form $\frac{b^2}{b}$ darstellbar.[40]

---

[39] Wir benutzen folgende mengentheoretische Bezeichnungen: $a \in \mathfrak{A}$: a ist Element von $\mathfrak{A}$; $\mathfrak{B} \subseteq \mathfrak{A}$, $\mathfrak{B} \subset \mathfrak{A}$: $\mathfrak{B}$ ist Teilmenge, bzw. echte Teilmenge von $\mathfrak{A}$; statt dessen auch $\mathfrak{A} \supseteq \mathfrak{B}$, $\mathfrak{A} \supset \mathfrak{B}$. [The note in Jarník's records.]
This note shows that set symbolism has not yet been stabilised and commonly used in 1927.

[40] See MA-I, p. 46, where a ring is supposed to be commutative, whereas a field to be non-commutative in general (division ring, skew field, sfield). In MA-I, p. 47, we find this formulation: *Der Quotientenkörper* $\mathfrak{P}$ *ist durch den Ring* $\mathfrak{R}$ *bis auf Isomorphie eindeutig bestimmt, wenn es überhaupt einen Quotientenkörper zum Ring* $\mathfrak{R}$ *gibt.*

Wenn $\mathcal{O}$ noch in einem anderen Körper Ω' enthalten ist, so ist der Quotientenkörper von $\mathcal{O}$ in Ω mit dem Quotientenkörper von $\mathcal{O}$ in Ω' isomorph. (Es genügt, jeden Quotienten $\frac{a}{b}$ in Ω dem Quotienten $\frac{a}{b}$ in Ω' zuzuordnen, wo a, b Elemente aus $\mathcal{O}$ mit $b \neq 0$ sind.)

14
XI

Wir zeigen statt ‖ etwas allgemeiner: Es seien $\mathcal{O}$, $\overline{\mathcal{O}}$ zwei Ringe, Ω, $\overline{\Omega}$ zwei Körper, $\mathcal{O} \cong \overline{\mathcal{O}}$, $\mathcal{O} \subseteq \Omega$, $\overline{\mathcal{O}} \subseteq \overline{\Omega}$. Es sei Σ der Quotientenkörper von $\mathcal{O}$ in Ω, $\overline{\Sigma}$ der Quotientenkörper von $\overline{\mathcal{O}}$ in $\overline{\Omega}$; dann ist

$$\Sigma \cong \overline{\Sigma}.$$

Beweis. Elemente von Σ sind $\frac{a}{b}$ (a, b aus $\mathcal{O}$, $b \neq 0$); dem Element $\frac{a}{b}$ lassen wir das Element $\frac{\overline{a}}{\overline{b}}$ aus $\overline{\Sigma}$ entsprechen, wenn durch den Isomorphismus $\mathcal{O} \cong \overline{\mathcal{O}}$[41] $a \to \overline{a}$, $b \to \overline{b}$ zugeordnet werden. Es ist dann $\frac{a}{b} = \frac{c}{d}$ dann und nur dann, wenn $ad = bc$; dann ist aber auch $\overline{a}\overline{d} = \overline{b}\overline{c}$, also $\frac{\overline{a}}{\overline{b}} = \frac{\overline{c}}{\overline{d}}$. Gleiche Elemente gehen wieder in gleiche Elemente über: die Zuordnung von Σ, $\overline{\Sigma}$ ist eineindeutig.

Zu

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{wird also} \qquad \frac{\overline{a}\overline{d} + \overline{b}\overline{c}}{\overline{b}\overline{d}} = \frac{\overline{a}}{\overline{b}} + \frac{\overline{c}}{\overline{d}}$$

zugeordnet, ebenso

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a\,c}{b\,d} \quad \to \quad \frac{\overline{a}\,\overline{c}}{\overline{b}\,\overline{d}} = \frac{\overline{a}}{\overline{b}} \cdot \frac{\overline{c}}{\overline{d}}.$$

Also ist die Beziehung zwischen Σ und $\overline{\Sigma}$ in der Tat ein Isomorphismus.

Wir haben bisher vorausgesetzt, dass der Ring $\mathcal{O}$ in einen Körper Ω eingebettet war, und haben daraus auf die Existenz des Quotientenkörpers geschlossen; jetzt wollen wir die Voraussetzung der Existenz von Ω fallen lassen und beweisen: Jeder Ring $\mathcal{O}$ ohne Nullteiler hat einen Quotientenkörper.[42]

Beweis. Wir betrachten alle Zahlenpaare (a, b), wo a, b aus $\mathcal{O}$ sind und $b \neq 0$. Wir definieren: zwei solche Paare heissen äquivalent, $(a, b) \sim (c, d)$, wenn $ad = bc$. Dieser Äquivalenzbegriff ist offenbar reflexiv und symmetrisch, aber auch transitiv; denn aus $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$ folgt $ad = bc$, $cf = de$, also

$$adf = bcf = bde, \quad \text{also} \quad (d \neq 0\,!) \quad af = be, \quad \text{d.h.} \quad (a, b) \sim (e, f).$$

[41] In Jarník's records, erroneously is written $\Sigma \cong \overline{\Sigma}$.

[42] See MA-I, pp. 47–49.

The commutativity is assumed once again. In MA-I, p. 49, there is this notification: *Die Möglichkeit der Einbettung nichtkommutativer Ringe ohne Nullteiler in einen sie umfassenden Körper bildet ein ungelöstes Problem, außer in ganz speziellen Fällen.*

Durch diese Äquivalenz werden also alle Paare (a, b) in Klassen von untereinander äquivalenten Paaren eingeteilt; die Klasse der mit (a, b) äquivalenten Paare bezeichnen wir mit $\frac{a}{b}$; es ist $\frac{a}{b} = \frac{c}{d}$ genau dann, wenn $ad = bc$.

Wir definieren Addition und Multiplikation von Klassen:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Wir sollen beweisen, dass diese Definitionen eindeutig sind, also bei der Addition sollen wir zeigen: aus $\frac{a}{b} = \frac{a'}{b'}$ folgt

$$\frac{ad + bc}{bd} = \frac{a'd + b'c}{b'd};$$

es ist aber in der Tat

$$(ad + bc)b'd = (a'd + b'c)bd,$$

wegen $a'b = ab'$. Ebenso bei dem Produkt. Nun sollen wir zeigen, dass diese Paare einen Körper bilden:

das assoziative Gesetz bei Addition beweist man so:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf},$$

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf}.$$

Ebenso die übrigen Rechenregeln. Die Lösbarkeit der Gleichungen

$$\frac{a}{b} + X = \frac{c}{d}, \qquad \frac{a}{b} \cdot X = \frac{c}{d}$$

zeigt man sofort, indem man zeigt, dass sie durch

$$X = \frac{cb - ad}{bd}, \qquad \text{bzw.} \qquad \frac{cb}{ad}$$

erfüllt werden; dabei muss freilich im zweiten Fall $\frac{a}{b} \neq 0$, d.h. $a \neq 0$, vorausgesetzt werden. Die Elemente $\frac{a}{b}$ bilden also einen Körper, der aber noch nicht den Ring $\mathcal{O}$ enthält. Das erreichen wir aber dadurch, dass wir jedes Element $\frac{a}{c}$, welches sich in der Form $\frac{rb}{b}$ schreiben lässt, mit r identifizieren; diese Identifikation ist in der Tat eindeutig, denn aus

$$\frac{rb}{b} = \frac{sd}{d} \qquad \text{folgt} \qquad rbd = sbd, \qquad \text{also} \qquad r = s.$$

Damit ist der Quotientenkörper konstruiert.

Wir werden im Folgenden die Ringe mit grossen lateinischen, ihre Quotientenkörper mit entsprechenden grossen griechischen Buchstaben bezeichnen, also z.B. $\mathcal{R}$, $\mathcal{P}$, $\mathcal{O}$, Ω u.s.w. Für den Ring von ganzen Zahlen und seinen Quotientenkörper von allen rationalen Zahlen führen wir die feste Bezeichnung $\mathcal{C}$, Γ ein.

Wenn $\mathcal{O}$ ein Ring mit Nullteiler, so kann man ihn sicher nicht in einen Quotientenkörper einbetten, wohl aber in einen Quotientenring von Quotienten $\frac{a}{b}$, wo b Nichtnullteiler sind (die Konstruktion lässt sich durchführen, weil ein Produkt von Nichtnullteilern wieder ein Nichtnullteiler ist).[43]

§ 5. Ringbildung II. Polynomring

Es sei $\mathcal{O}$ ein Ring; ich bilde formal alle endliche Summen $\sum a_i x^i$, wo a_i Ringelemente, x ein neuer Buchstabe ist. Diese Summen heissen Polynome, x die „Unbestimmte". Statt $a_0 x^0$ schreiben wir einfach a_0.[44]

Man definiert: gleich sind zwei solche Polynome, wenn sie formal gleich sind (bis auf Glieder mit Koeffizienten Null).

Addition: $\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$

Multiplikation: $\sum a_i x^i \cdot \sum b_k x^k = \sum_l (\sum_{i+k=l} a_i b_k) x^l$

Für Konstanten gehen diese Definitionen in die alten Definitionen im Ring $\mathcal{O}$ über.

Die Regeln für einen Ring sind offenbar erfüllt: nur das assoziative und distributive Gesetz für Multiplikation bedarf einer Verifikation:

$$\Big(\sum a_i x^i \sum b_k x^k\Big) \sum c_m x^m = \sum \Big(\sum_{l+m=n} c_m \sum_{i+k=l} a_i b_k \Big) x^n =$$
$$= \sum_n \Big(\sum_{i+k+m=n} a_i b_k c_m \Big) x^n,$$
$$\sum a_i x^i \Big(\sum b_k x^k \sum c_m x^m\Big) = \sum \Big(\sum_{i+l=n} a_i \sum_{k+m=l} b_k c_m \Big) x^n =$$
$$= \sum_n \Big(\sum_{i+k+m=n} a_i b_k c_m \Big) x^n;$$

$$\sum a_i x^i \Big(\sum b_k x^k + \sum c_k x^k\Big) = \sum a_i x^i \sum (b_k + c_k) x^k =$$
$$= \sum_l \Big(\sum_{i+k=l} a_i (b_k + c_k) \Big) x^l =$$
$$= \sum_l \Big(\sum_{i+k=l} a_i b_k \Big) x^l + \sum_l \Big(\sum_{i+k=l} a_i c_k \Big) x^l =$$
$$= \sum a_i x^i \sum b_k x^k + \sum a_i x^i \sum c_k x^k.$$

[43] See MA-I, p. 49.

[44] For the whole Section 5 see MA-I, pp. 49–53.

Endlich wird die Gleichung $\sum a_i x^i + Y = \sum b_i x^i$ durch $Y = \sum (b_i - a_i) x^i$ befriedigt. Also bilden diese Polynome einen Ring: „Polynomring mit dem Koeffizientenbereich $\mathcal{O}$“, Bezeichnung: $\mathcal{O}[x]$.

Wir können auch mehrere Unbestimmte nacheinander adjungieren: $\mathcal{O}[x_1][x_2]$; das sind Polynome $\sum \Big(\sum a_{ki} x_1^i \Big) x_2^k$; ebenso $\mathcal{O}[x_2][x_1]$ wird durch alle Polynome $\sum \Big(\sum a_{ki} x_2^k \Big) x_1^i$ gebildet; wir setzen

$$\sum \Big(\sum a_{ki} x_1^i \Big) x_2^k \quad = \quad \sum \Big(\sum a_{ki} x_2^k \Big) x_1^i;$$

dann ist $\mathcal{O}[x_1][x_2]$ mit $\mathcal{O}[x_2][x_1]$ identisch; wir können diesen Ring mit $\mathcal{O}[x_1, x_2]$ bezeichnen und ihn als durch „gleichzeitige Adjunktion“ von x_1 und x_2 entstanden denken. Seine Elemente schreiben wir einfach in der Form $\sum a_{ik} x_1^i x_2^k$.

Durch Induktion können wir dann $\mathcal{O}[x_1, x_2, \ldots, x_n]$ einführen; und noch allgemeiner: wenn M eine beliebige Menge von Unbestimmten ist, so bilden wir alle Polynome in endlich vielen von diesen Unbestimmten, also die Vereinigungsmenge aller $\mathcal{O}[x, y, \ldots, z]$. Das ist der sog. Polynombereich von unendlich vielen Unbestimmten der Menge M. Nun Spezialisationen:

1.) Wenn $\mathcal{O}$ ein Einheitselement hat, so bleibt dieses Element auch im $\mathcal{O}[x]$ offenbar Einheitselement.

Den höchsten Exponenten von x in einem Element von $\mathcal{O}[x]$ mit nicht verschwindendem Koeffizienten nennt man Grad des Elementes. Alle Elemente bis auf 0 haben einen Grad.

2.) Wenn $\mathcal{O}$ ohne Nullteiler, so ist Grad des Produktes gleich der Summe der Grade einzelner Faktoren; denn aus $f(x) = a_n x^n + \ldots$, $a_n \neq 0$, $g(x) = b_m x^m + \ldots$, $b_m \neq 0$, folgt $f(x)g(x) = a_n b_m x^{n+m} + \ldots$, $a_n b_m \neq 0$.

Also: wenn $\mathcal{O}$ ein Integritätsbereich, so ist auch $\mathcal{O}[x]$ ein Integritätsbereich.

Dies übertragt sich sofort durch Induktion auf Polynomringe mit mehreren, sogar unendlich vielen Unbestimmten. Auch der Satz von dem Grad des Produktes übertragt sich sofort auf mehrere oder unendlich viele Unbestimmten, wenn $\mathcal{O}$ ohne Nullteiler.

Als Grad definieren wir die höchste Summe der Exponenten von x_1, x_2, ... in einem Glied. Dann gilt die eindeutige Zerlegung $f = f_0 + f_1 + \cdots + f_\varrho$ in homogene Bestandteile des Grades 0, 1, ..., ϱ; ebenso $g = g_0 + g_1 + \cdots + g_\sigma$; $f_\varrho g_\sigma$ geben dann die höchsten Glieder des Produktes, womit die Behauptung bewiesen ist.

18
XI

Gilt eine algebraische Relation im Polynombereich $\mathcal{O}[x]$, so gilt sie auch, wenn man für x eine Grösse aus $\mathcal{O}$ oder aus einem Oberring von $\mathcal{O}$ einsetzt. Auch dies ist ohne weiteres auf Polynome mit mehreren Unbestimmten auszudehnen.

§ 6. Ringbildung III. Restklassenring

Es sei $\mathcal{R}$ ein Ring und $\overline{\mathcal{R}}$ ein dazu meromorpher Ring: $\mathcal{R} \sim \overline{\mathcal{R}}$. Man fragt: wie konstruiert man einen zu $\overline{\mathcal{R}}$ isomorphen Ring?[45]

Es sei a ein Element von $\mathcal{R}$, $\overline{a}$ das zugeordnete Element von $\overline{\mathcal{R}}$; es sei $\mathcal{R}_a$ die Klasse derjenigen Elemente von $\mathcal{R}$, denen ein und dasselbe Element $\overline{a}$ in $\overline{\mathcal{R}}$ entspricht. Wir wollen schreiben $a \equiv a'$, sobald zu a und zu a' dasselbe Element von $\overline{\mathcal{R}}$ zugeordnet wird, d.h. sobald a und a' einer und derselben Klasse $\mathcal{R}_a$ angehören. Wenn $\mathcal{R}_a$ zu $\overline{a}$, $\mathcal{R}_b$ zu $\overline{b}$ gehört, so gehört $\mathcal{R}_{a+b}$ zu $\overline{a}+\overline{b}$, $\mathcal{R}_{ab}$ zu $\overline{a}\overline{b}$. Demnach sind die Klassen $\mathcal{R}_{a+b}$ und $\mathcal{R}_{ab}$ von der Wahl von a in $\mathcal{R}_a$ und von b in $\mathcal{R}_b$ unabhängig; d.h.

$$(1) \qquad \left\{ \begin{array}{l} \text{aus} \quad a \equiv a', \quad b \equiv b' \quad \text{folgt} \quad a+b \equiv a'+b', \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad ab \equiv a'b'. \end{array} \right.$$

Wenn man diese Klassen also als neue Elemente mit den Regeln

$$\mathcal{R}_a + \mathcal{R}_b = \mathcal{R}_{a+b}, \qquad \mathcal{R}_a \mathcal{R}_b = \mathcal{R}_{ab}$$

auffasst, so bilden sie einen zu $\overline{\mathcal{R}}$ isomorphen Bereich, also auch einen Ring.

Umgekehrt: wenn eine Klasseneinteilung von $\mathcal{R} : a \equiv a'$ die Beziehungen (1) erfüllt sind, so bestimmen die Klassen $\mathcal{R}_a$, $\mathcal{R}_b$ eindeutig eine Summenklasse $\mathcal{R}_{a+b}$ und eine Produktklasse $\mathcal{R}_{ab}$.

Ordnet man diesen Klassen dann mit den entsprechenden Rechenregeln irgendwie neue Elemente $\overline{a}$, $\overline{b}$, ... zu, so entsteht eine zu $\mathcal{R}$ meromorphe Menge $\overline{\mathcal{R}}$, also ein Ring.

Also: Ein jeder zu $\mathcal{R}$ meromorpher Ring kann durch eine Klasseneinteilung von $\mathcal{R}$ mit (1) bis auf Isomorphie erzeugt werden; und umgekehrt, jede solche Klasseneinteilung definiert eine solche Meromorphie.

Aus $a \equiv b$ folgt durch Addition von $-b$ auf beiden Seiten $a - b \equiv b - b \equiv 0$, und ungekehrt: aus $a - b \equiv 0$ folgt $a \equiv b$. Die „Kongruenzrelation“ $\equiv$ ist also

[45] In MA-I, pp. 53–60, the material of Section 6 is presented differently.

festgestellt, sobald man weiss, welche Elemente von $\mathcal{R}$ kongruent Null sind. Aus $a \equiv 0$, $b \equiv 0$ folgt $a - b \equiv 0$ (Moduleigenschaft), aus $a \equiv 0$ folgt $ra \equiv 0$, wenn r aus $\mathcal{R}$ ist. Also bilden die Elemente von $\mathcal{R}$, die kongruent Null sind, eine Menge, die mit a und b auch $a - b$ und mit a auch ra enthält, mit anderen Benennung: ein Ideal in $\mathcal{R}$. Ist umgekehrt ein Ideal $\mathfrak{a}$ in $\mathcal{R}$ gegeben, und schreiben wir $a \equiv b\ (\mathfrak{a})$, sobald $a - b$ in $\mathfrak{a}$ ist, so ist diese Kongruenzrelation offenbar reflexiv, symmetrisch und transitiv und definiert also eine Klasseneinteilung und aus $a \equiv a',\ b \equiv b'\ \ (\mathfrak{a})$ folgt, dass $(a - a') + (b - b')$ in $\mathfrak{a}$ liegt, d.h.

$$a + b \equiv a' + b'\ (\mathfrak{a});$$

weiter liegt auch $(a-a')b = ab - a'b$ und auch $a'(b-b') = a'b - a'b'$ in $\mathfrak{a}$, also auch $(ab - a'b) + (a'b - a'b') = ab - a'b'$ in $\mathfrak{a}$, also ist

$$ab \equiv a'b'\ (\mathfrak{a}).$$

Die Relation $\equiv$ erfüllt also auch (1). Jedes Ideal führt also umgekehrt zu einer Kongruenzrelation und dadurch zu einem Meromorphismus; bei diesem Meromorphismus gehen kongruente Elemente in gleiche über.

Die einfachste Art, bei gegebenem $\mathfrak{a}$ den Ring $\overline{\mathcal{R}}$ zu erhalten, ist, dass man die Klassen $\mathcal{R}_a$ selbst als Elemente von $\overline{\mathcal{R}}$ wählt, also definiert

$$\mathcal{R}_a + \mathcal{R}_b = \mathcal{R}_{a+b}\,, \qquad \mathcal{R}_a \mathcal{R}_b = \mathcal{R}_{ab}\,.$$

Die Klassen $\mathcal{R}_a$ nennt man Restklassen nach dem Ideal $\mathfrak{a}$, den durch sie gebildeten Ring den Restklassenring von $\mathcal{R}$ nach $\mathfrak{a}$. Zeichen: $\mathcal{R}/\mathfrak{a}$. Nach obigem ist jedes meromorphe Abbild $\overline{\mathcal{R}}$ von $\mathcal{R}$ einem Restklassenring $\mathcal{R}/\mathfrak{a}$ isomorph.

Beispiele:

1.) Wenn $\mathfrak{a} = \mathcal{R}$, so wird jedem Element von $\mathcal{R}$ die Null zugeordnet; der Restklassenring besteht aus einer einzigen Klasse.

2.) Wenn $\mathfrak{a} = (0)$, d.h. $\mathfrak{a}$ aus dem einzigen Element Null besteht, so sind zwei Elemente von $\mathcal{R}$ nur dann kongruent, wenn sie gleich sind; der Meromorphismus wird zum Isomorphismus.

3.) Wenn $\mathcal{R}$ ein Körper ist, so ist entweder $\mathfrak{a} = (0)$ oder $\mathfrak{a} = \mathcal{R}$; denn wenn $\mathfrak{a}$ ein von Null verschiedenes Element a enthält, und b ein beliebiges Element aus $\mathcal{R}$ ist, so ist auch $\frac{b}{a} \cdot a = b$ ein Element von $\mathfrak{a}$.

Einfachste Eigenschaften der Ideale

Definition. $(a_1, a_2, \ldots, a_r)$ bedeutet das Ideal aller Summen

$$g_1 a_1 + g_2 a_2 + \cdots + g_r a_r + n_1 a_1 + \cdots + n_r a_r,$$

wo g_i Elemente aus dem Ring $\mathcal{R}$ sind, n_i ganze rationale Zahlen; man sagt, die a_i bilden eine Idealbasis, sie erzeugen das Ideal.

Bemerkung: Wenn $\mathcal{R}$ nicht das Einheitselement besitzt, so darf man die Elemente $n_i a_i$ gegenüber den $g_i a_i$ nicht weglassen: denn z.B. a_i ist bei $a_i \neq 0$ nicht notwendig in der Form $g_i a_i$, g_i aus $\mathcal{R}$, darstellbar.

Allgemeiner: Jede Menge M von Elementen aus $\mathcal{R}$ erzeugt ein Ideal; dies ist die Menge aller endlichen Summen

$$\sum g_i a_i + \sum n_i a_i \quad (a_i \text{ aus } M,\ g_i \text{ aus } \mathcal{R},\ n_i \text{ ganz rational}).$$

Im Spezialfall, dass ein Ideal[46] eine eingliedrige Basis a besitzt, nennt man das Ideal (a), d.h. die Menge aller Summen $ga + na$, ein Hauptideal.[47]

Ist a ein Element von $\mathfrak{a}$, $a \equiv 0\ (\mathfrak{a})$, so nennt man a teilbar durch $\mathfrak{a}$. Ist $\mathfrak{b} \subseteq \mathfrak{a}$, so schreibt man dafür $\mathfrak{b} \equiv 0\ (\mathfrak{a})$ und sagt: $\mathfrak{b}$ ist teilbar durch $\mathfrak{a}$, $\mathfrak{b}$ ist ein Vielfaches von $\mathfrak{a}$ oder $\mathfrak{a}$ ist ein Teiler von $\mathfrak{b}$. Wenn schärfer $\mathfrak{b} \subset \mathfrak{a}$ ist, so spricht man von einem echten Teiler oder Vielfachen.[48]

21
XI

Beispiel. Es sei $\mathcal{C}$ der Ring der ganzen rationalen Zahlen; es sei n ganz; wir betrachten das Hauptideal (n). Die Restklassen R_0, R_1, …, R_{n-1} sind repräsentiert durch ihre Reste $0, 1, \ldots, n-1$ und sind untereinander verschieden. Sie bilden einen Ring mit R_0 als Nullelement, R_1 als Einheitselement; $\mathcal{C}$ ist diesem Ring meromorph.

Wenn n zusammengesetzt ist, so hat dieser Ring Nullteiler; z.B. bei $n = 6$ ist $R_2 R_3 = R_0$. Wenn aber n eine Primzahl, so ist er ohne Nullteiler, also ein Körper, weil er nur endlich viele Elemente hat.[49]

In $\mathcal{C}$ ist jedes Ideal ein Hauptideal.[50]

Beweis. Wenn $\mathfrak{a}$ kein Nullideal ist, so enthält es eine von Null verschieden Zahl, also auch eine positive, also auch eine kleinste posivite Zahl n. $\mathfrak{a}$ enthält also alle Vielfache von n. Umgekehrt, wenn a zu Ideal $\mathfrak{a}$ gehört, so sei $a = n\overline{n} + r$ mit $0 \leq r < n$; wäre $r > 0$, so wäre auch $r = a - n\overline{n}$ eine Zahl aus $\mathfrak{a}$, gegen Voraussetzung; also ist $r = 0$, $a =$ Vielfaches von n, w.z.b.w.

Der Durchschnitt[51] von zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ (Bezeichnung: $\mathfrak{a} \cap \mathfrak{b}$ oder $[\mathfrak{a}, \mathfrak{b}]$) ist offenbar wieder ein Ideal: denn wenn a, a' sowohl zu $\mathfrak{a}$ als zu $\mathfrak{b}$ gehören, so auch

[46] In Jarník's records, at this place, the word *Integral* is written by mistake.
[47] See MA-I, p. 54.
[48] See MA-I, p. 58.
[49] See MA-I, pp. 57–58.
[50] See MA-I, p. 60.
[51] For the following text see MA-I, p. 60.

$a \pm a'$, ra' (r aus $\mathcal{R}$). Ebenso ist der Durchschnitt

$$\mathfrak{a} \cap \mathfrak{b} \cap \mathfrak{c} \cap \mathfrak{d} \cap \dots \quad \text{oder} \quad [\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \dots]$$

von beliebig vielen Idealen ein Ideal; und es ist ein gemeinsames Vielfaches von diesen Idealen (d.h. in allen enthalten) und zwar das mengentheoretisch umfassendste; man nennt es deshalb auch das kleinste gemeinsame Vielfache.

Als Idealsumme von zwei Idealen $\mathfrak{a} + \mathfrak{b}$ definiert man das von der Vereinigungsmenge von $\mathfrak{a}$, $\mathfrak{b}$ erzeugte Ideal; das ist, wie sofort zu sehen, die Menge aller Summen $a + b$, wo $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Statt $\mathfrak{a} + \mathfrak{b}$ schreibt man auch $(\mathfrak{a}, \mathfrak{b})$; das ist ein gemeinsamer Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, und zwar der mengentheoretisch kleinste; daher der Name „grösster gemeinsamer Teiler." Ebenso definiert man für beliebig viele Ideale:

grösster gemeinsamer Teiler $= (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots) = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \dots =$

$=$ Menge von allen endlichen Summen $a_i + a_k + \dots + a_n$ mit $a_i \in \mathfrak{a}_i$.

Z.B.: wenn $f_1, f_2, \dots, f_r$ Elemente aus $\mathcal{R}$ sind, so ist $(f_1, f_2, \dots, f_r)$ der grösste gemeinsame Teiler der Hauptideale (f_1), (f_2), $\dots$, (f_r).

Ein Ideal $\mathfrak{g}$ heisst prim, wenn der Restklassenring $\mathcal{R}/\mathfrak{g}$ keine Nullteiler hat, d.h. wenn aus

$$ab \equiv 0 \ (\mathfrak{g}) \quad \text{und} \quad a \not\equiv 0 \ (\mathfrak{g}) \quad \text{folgt} \quad b \equiv 0 \ (\mathfrak{g}).$$

Das „Einheitsideal" $\mathcal{R}$ ist immer prim oder Primideal: denn alle Elemente sind kongruent 0 $(\mathcal{R})$.

Es sei nun $\mathcal{O}$ ein Ring mit Einheitselement; $\mathfrak{g}$ sei ein Ideal, das keine echte Teiler ausser $\mathcal{O}$ hat. Ich behaupte: $\mathcal{O}/\mathfrak{g}$ ist ein Körper; also ist $\mathfrak{g}$ Primideal.[52]

Beweis. Ich soll in $\mathcal{O}/\mathfrak{g}$ die Lösbarkeit von $ax = b$ für $a \neq 0$ zeigen, d.h. die Lösbarkeit von

$$ax \equiv b \ (\mathfrak{g}), \quad \text{wenn} \quad a \not\equiv 0 \ (\mathfrak{g}).$$

Es ist $(a, \mathfrak{g})$, d.h. die Menge $ra + \mathfrak{g}$ (r aus $\mathcal{O}$), ein echter Teiler von $\mathfrak{g}$, also gleich $\mathcal{O}$:

$$(a, \mathfrak{g}) = \mathcal{O}.$$

Jedes Element b von $\mathcal{O}$ lässt sich also in der Form $b = ra +$ Zahl aus $\mathfrak{g}$ darstellen, d.h.

$$b \equiv ra \ (\mathfrak{g}).$$

w.z.b.w.

---

[52] See MA-I, pp. 58–59.
See MA-I, p. 59: *Jedes von* $\mathfrak{o}$ *verschiedene teilerlose Ideal* $\mathfrak{p}$ *in einem Ring* $\mathfrak{o}$ *mit Einselement ist prim, und der Restklassenring* $\mathfrak{o}/\mathfrak{p}$ *ist ein Körper. Ist umgekehrt* $\mathfrak{o}/\mathfrak{p}$ *ein Körper, so ist* $\mathfrak{p}$ *teilerlos.* (p. 59)

Man kann den Beweis ein wenig abstrakter führen (vgl. um 3 Seiten später).[53]

Es seien $\mathfrak{a}$, $\mathfrak{b}$ zwei Ideale in $\mathcal{O}$, $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathcal{O}$; es lässt sich zeigen: dem $\mathfrak{b}$ entspricht im Restklassenring $\mathcal{O}/\mathfrak{a}$[54] der Ring $\overline{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}$; und umgekehrt: alle Ideale des Restklassenringes $\mathcal{O}/\mathfrak{a}$ entsprechen gewissen Idealen zwischen $\mathfrak{a}$ und $\mathcal{O}$. In unserem Fall für $\mathfrak{a} = \mathfrak{g}$ gibt es also keine Ideale zwischen $\mathfrak{g}$ und $\mathcal{O}$, also ist u.s.w.

§ 6[a]. Weiteres über Polynomringe

Divisionsalgorithmus. Sind $f(x)$, $g(x)$ Polynome mit Koeffizienten aus einem Körper K, $g(x) \neq 0$, so liefert die gewöhnliche Division

$$f(x) = g(x)q(x) + r(x),$$

wo $r(x) = 0$ oder $r(x)$ einen kleineren Grad als $g(x)$ hat. Ist a_0 der Koeffizient des höchsten Gliedes in $g(x)$, so werden bei der Division keine anderen Nenner als Potenzen von a_0 eingeführt. Ist $a_0 = 1$, so treten keine Nenner auf, und die Division lässt sich auch dann durchführen, wenn die Koeffizienten einem beliebigen Ring mit Einheitselement entnommen sind.[55]

Hat $f(x)$ im Körper K eine Nullstelle a_1, d.h. ist $f(a_1) = 0$, so lässt $f(x)$ bei Division durch $x - a_1$ keinen Rest, mithin $f(x) = (x - a_1)f_1(x)$. Ist a_2 eine weitere Nullstelle, $a_2 \neq a_1$, so ist a_2 auch Nullstelle von $f_1(x)$, also ist $f_1(x)$ teilbar durch $x - a_2$, also

$$f(x) = (x - a_1)(x - a_2)f_2(x).$$

So weitergehend sieht man:

Ein Polynom $f(x) \neq 0$ hat im Körper K höchstens so viele Nullstellen, wie sein Grad beträgt.

Dasselbe gilt, wenn K ein Integritätsbereich ist, da man ihn in einen Körper einbetten kann.[56]

Folgerungen.[57] Ist $\mathcal{R}$ ein Integritätsbereich mit unendlich vielen Elementen, und $f(x_1, x_2, \ldots, x_n) \neq 0$ (f aus $\mathcal{R}[x_1, x_2, \ldots, x_n]$), so gibt es in $\mathcal{R}$ ein Element a_n mit $f(x_1, x_2, \ldots, x_{n-1}, a_n) \neq 0$. Daraus durch Induktion: Es gibt in $\mathcal{R}$ auch Elemente $a_1, a_2, \ldots, a_n$, so dass

$$f(a_1, a_2, a_3, \ldots, a_n) \neq 0.$$

---

[53] See the beginning of the lecture dated by November 25.
[54] The symbol $\mathcal{O}/\mathfrak{a}$ is inserted.
[55] See MA-I, pp. 52–53.
[56] See MA-I, p. 69.
[57] See MA-I, p. 70.

Der Quotientenkörper eines Polynombereiches $K[x_1, x_2, \dots]$ heisst der Körper der rationalen Funktionen von $x_1, x_2, \dots$ über K. Bezeichnung: $K(x_1, x_2, \dots)$.

Die angegebenen Folgerungen brauchen für endliche Körper nicht gelten; z.B. wenn K der Restklassenring mod 2 ist, so ist $x(x-1)$ stets gleich Null, wenn man für x einen Wert aus K einsetzt, obwohl $x(x-1) \neq 0$.

Wir betrachten $K[x]$, wo K ein Körper: hier ist jedes Ideal ein Hauptideal; denn es sei g der Polynom $\neq 0$ niedrigsten Grades im Ideal: dann ist für jedes f aus dem Ideal

$$f = gq + r,$$

wo der Grad von r kleiner als derjenige von g ist, oder $r = 0$ ist. Wäre $r \neq 0$, so wäre auch $r = f - gq$ ein Element des Ideals, gegen die Voraussetzung. Also sind alle f aus dem Ideal Multipla von g, w.z.b.w.[58]

25 / XI

Es sei $\mathcal{O}$ ein Ring mit Einheitselement; $\mathfrak{g}$ sei ein Ideal aus $\mathcal{O}$, das keine echte Teiler ausser $\mathcal{O}$ besitzt.

Behauptung: $\mathcal{O}/\mathfrak{g}$ ist ein Körper, hat also keine Nullteiler, also ist $\mathfrak{g}$ ein Primideal.[59]

Ich werde den abstrakten Beweis noch einmal ausführlich führen.[60]

Es sei $\mathcal{O} \sim \overline{\mathcal{O}}$; es ist also $\mathcal{O}/\mathfrak{n} \cong \overline{\mathcal{O}}$. Es sei $\overline{\mathfrak{a}}$ ein Ideal in $\overline{\mathcal{O}}$; $\mathfrak{a}$ sei die Menge der Elemente aus $\mathcal{O}$, die den Elementen von $\overline{\mathfrak{a}}$ im Meromorphismus entsprechen. $\mathfrak{a}$ ist ein Ideal; denn wenn a, b in $\mathfrak{a}$, r in $\mathcal{O}$ liegen, und mit $\overline{a}$, $\overline{b}$, $\overline{r}$ die zugeordneten Elemente von $\overline{\mathcal{O}}$ bezeichnet werden, so ist

$$a \pm b \to \overline{a} \pm \overline{b} \in \overline{\mathfrak{a}},$$

$$ra \to \overline{r}\,\overline{a} \in \overline{\mathfrak{a}}.$$

$\mathfrak{a}$ enthält $\mathfrak{n}$; denn alle Elemente von $\mathfrak{n}$ entsprechen dem Element 0 aus $\overline{\mathcal{O}}$.

Umgekehrt, es sei $\mathfrak{a} \supseteq \mathfrak{n}$ ein Ideal aus $\mathcal{O}$; die Elemente von $\overline{\mathcal{O}}$, die zu $\mathfrak{a}$ zugeordnet werden, bilden ein Ideal; denn aus

$$a \in \mathfrak{a}, \quad b \in \mathfrak{a}, \quad r \in \mathcal{O} \quad \text{folgt} \quad a \pm b \to \overline{a} \pm \overline{b}, \quad ra \to \overline{r}\,\overline{a}.$$

Und $\mathfrak{a}$ enthält mit einem Element a offenbar alle Elemente $a + n$ mit $n \in \mathfrak{n}$, also die ganze Restklasse nach $\mathfrak{n}$. Die Ideale im $\mathcal{O}$ über $\mathfrak{n}$ und die Ideale in $\overline{\mathcal{O}}$ entsprechen sich also eineindeutig.

---

[58] See MA-I, p. 60.

[59] See MA-I, p. 59.

[60] The proof was given at the end of Section 6. The final note of Section 6 is to be proved now.

In unseren Fall: $\mathcal{O}/\mathfrak{g} = \overline{\mathcal{O}}$; die Zuordnung heisst

$$\mathcal{O} \to \overline{\mathcal{O}},$$
$$\mathfrak{g} \to (0).$$

Es gibt also kein Ideal zwischen $\overline{\mathcal{O}}$ und (0). Daraus folgt: wenn $a \neq 0$ aus $\mathcal{O}/\mathfrak{g}$, so ist (a) nicht das Nullideal, als gleich $\overline{\mathcal{O}}$; also ist jedes andere Element b aus $\mathcal{O}/\mathfrak{g}$ in (a) enthalten, d.h. $b = ra$, wo $r \in \mathcal{O}/\mathfrak{g}$; d.h. $\mathcal{O}/\mathfrak{g}$ ist ein Körper w.z.b.w.

Man kann es so aussprechen: „Maximale“ (im mengentheoretischen Sinn) Ideale in $\mathcal{O}$ (mit Einheitselement) sind Primideale und ihr Restklassenring ist ein Körper.

§ 7. Idealtheorie der euklidischen Ringe

Ein euklidischer Ring ist ein Ring ohne Nullteiler und mit dem Einheitselement, wo jedes Ideal Hauptideal ist. Z.B.[61]

1.) Ring der ganzen rationalen Zahlen.
2.) Polynombereich $\Sigma[x]$, wo Σ Körper.[62]
3.) Der Ring der ganzen Gaussschen Zahlen $a + b\,\mathrm{i}$ (a, b ganz rational).[63]

Beweis zu 3.). Wenn $\alpha = a + b\,\mathrm{i}$, $\gamma = c + d\,\mathrm{i}$, $\gamma \neq 0$ (a, b, c, d ganz rat.), so kann ich zwei Gausssche Zahlen ε, ϱ so finden, dass $\alpha = \varepsilon\gamma + \varrho$, $N(\varrho) < N(\gamma)$. Dabei ist $N(\alpha) = |\alpha|^2 = a^2 + b^2$.

Denn: $\frac{\alpha}{\gamma} = g + h\,\mathrm{i}$, g, h rational. Ich finde die zu g, h nächsten ganzen rat. Zahlen e, f:

$$\frac{\alpha}{\gamma} = e + f\,\mathrm{i} + r + s\,\mathrm{i}, \quad \text{wo} \quad |r| \leq \frac{1}{2}, \quad |s| \leq \frac{1}{2},$$
$$= \varepsilon + r + s\,\mathrm{i} \quad (\varepsilon \text{ ganze G. Zahl}),$$
$$\alpha = \varepsilon\gamma + \varrho, \quad \text{wo} \quad N(\varrho) = N\big(\gamma \cdot (r + s\,\mathrm{i})\big) \leq N(\gamma) \cdot \frac{1}{2} < N(\gamma).$$

Nun es sei $\mathfrak{a}$ ein Ideal aus dem Ring der ganzen Gaussschen Zahlen, nicht Nullideal. Ich greife eine von seinen Zahlen mit möglichst kleiner positiver Norm; es sei α diese Zahl; β eine andere Zahl von $\mathfrak{a}$; dann gibt es ε, ϱ (ganz) so, dass $\beta = \varepsilon\alpha + \varrho$, $N(\varrho) < N(\alpha)$; weil $\varrho \in \mathfrak{a}$, so muss nach Voraussetzung $\varrho = 0$, $\beta = \varepsilon\alpha$, d.h. $\mathfrak{a} = (\alpha)$ – Hauptideal.

---

[61] In MA-I, p. 60, there is already a current term *Hauptidealring*.

[62] For the first and second example see MA-I, p. 60.

[63] For the proof and the following examples see MA-I, p. 62. In the sixth example, there should be $\big|N(r + s\sqrt{2})\big| \leq \frac{1}{2} < 1$, which does not matter.

Wir sehen, dass der euklidische Charakter wesentlich von dem Divisionssatz abhängt; wesentlich davon, dass $N(r+s\,\mathrm{i})<1$ ist für $|r|\le\frac{1}{2}$, $|s|\le\frac{1}{2}$. Er wird also in analogen Ringen gelten, wo eine solche geeignete Normdefinition möglich ist; z.B:

4.) $a+b\varrho$, a,b ganz rational, ϱ primitive 3. Einheitswurzel. Wir setzen

$$N(a+b\varrho)=(a+b\varrho)(a+b\varrho^2)=a^2+b^2-ab,$$
$$N(r+s\varrho)\le\frac{3}{4}<1\qquad\text{für}\quad|r|\le\frac{1}{2},\quad|s|\le\frac{1}{2}.$$

5.) $a+b\sqrt{-2}$, a,b ganz rational,

$$N(a+b\sqrt{-2})=a^2+2b^2,$$
$$N(r+s\sqrt{-2})\le\frac{3}{4}<1\qquad\text{für}\quad|r|\le\frac{1}{2},\quad|s|\le\frac{1}{2}.$$

6.) $a+b\sqrt{2}$, a,b ganz,

$$N(a+b\sqrt{2})=a^2-2b^2,$$
$$\left|N(r+s\sqrt{2})\right|\le\frac{3}{4}<1\qquad\text{für}\quad|r|\le\frac{1}{2},\quad|s|\le\frac{1}{2}.$$

Im euklidischen Ring $\mathcal{O}$ gilt folgender Satz: zu zwei Elementen a,b aus $\mathcal{O}$ gibt es mindestens einen gemeinsamen Teiler von der Form

$$d=la+mb.$$

Beweis. (a,b) ist ein Hauptideal (d);

$$\begin{aligned}&\text{also}\quad a=\ \text{Vielfaches von } d\\ &\qquad\quad b=\ \text{Vielfaches von } d\\ (*)\qquad &\qquad\quad d=la+mb.\end{aligned}$$

Um d zu finden, ist es in konkreten Fällen gewöhnlich notwendig, den sub 3.) erklärten Divisionsprozess durchzuführen.[64]

Wenn nun $\overline{d}$ ein gemeinsamer Teiler von a, b ist, so ist $\overline{d}$ gewiss auch Teiler von d – das ist klar nach $(*)$.[65]

---

[64] See MA-I, p. 61.

[65] The element d is the greatest common divisor of elements a, b. See MA-I, p. 61: *In einem Hauptidealring besitzen je zwei Elemente a,b einen größten gemeinsamen Teiler d, der sich in der Gestalt* (1) [tj. $(*)$] *darstellen läßt.*

In euklidischen Ringen gibt es eine eindeutige Faktorzerlegung. Hierzu sind noch einige Definitionen notwendig:[66]

1.) In einem Ring mit Einheitselement heisst jedes Element e Einheit, wenn es im Ring ein Inverses besitzt: $e \cdot e^{-1} = 1$.

2.) b heisst Teiler von a, wenn $a = cb$, c aus dem Ring.[67] Es sei $a \neq 0$; dann heisst b ein echter Teiler von a, wenn $b|a$, aber nicht $a|b$; mit anderen Worten: wenn in $a = cb$, c keine Einheit ist; denn aus $a = cb$, c Einheit, folgt $b = c^{-1}a$; und aus $a = cb$, $b = da$ folgt umgekehrt $b \neq 0$, $b = dcb$, $1 = dc$, d.h. c ist Einheit.[68]

3.) Ein Element p (p nicht 0, nicht Einheit) des Ringes heisst Primzahl, wenn jeder echter Teiler von p eine Einheit ist. D.h. aus $p = cb$ folgt $c =$ Einheit oder $b =$ Einheit.[69]

Wenn p eine Primzahl im euklidischen Ring, so ist (p) ein Primideal und der Restklassenring ein Körper.[70]

Beweis. p hat keine echte Teiler ausser Einheiten. Wenn $(p) \equiv 0$ $(\mathfrak{a})$, $\mathfrak{a} \neq \mathcal{O}$, $\mathfrak{a} \neq (p)$, so ist $\mathfrak{a} = (n)$, also $(p) \equiv 0$ (n), $p = r \cdot n$; also r eine Einheit. (Es ist aber offenbar $(m) = (em)$, wenn e eine Einheit; denn em ist ein Vielfaches von m und m ein Veilfaches von em. Umgekehrt, aus $(m) = (\overline{m})$ folgt $m|\overline{m}$, $\overline{m}|m$, also $m =$ Einheit $\cdot\, \overline{m}$.)

Also ist $(p) = (n)$ gegen Voraussetzung; (p) hat also keine echte Teiler ausser $\mathcal{O}$. Also ist der Restklassenring ein Körper und (p) ein Primideal, w.z.b.w.

Weil der Restklassenring bei Primidealen keine Nullteiler hat, so folgt: falls p Primzahl, $ab \equiv 0$ (p), so ist entweder $a \equiv 0$ (p) oder $b \equiv 0$ (p).[71]

28
XI

Jedem Element n eines euklidischen Ringes entspricht ein Ideal, nämlich das Ideal (n); und zwar entspricht denjenigen Zahlen, die sich nur um Einheiten

[66] See MA-I, p. 63.

[67] The notion of a divisor has been used above. For the divisibility of ideals see Section 6.

[68] In MA-I, p. 63, the notion of *assoziirte Größen* is introduced; it is not used here.

[69] It would probably be preferable to avoid the term prime number (*Primzahl*), which is commonly used, especially in the particular case of the domain of the integers, and in this way to define an irreducible element (*irreduzibles/unzerlegbares Element*). For principal ideal domains (resp. for unique factorization domains), the notions of irreducible element and of prime number (prime element) coincide.
Compare with MA-I, p. 63: *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 Element oder ein Primelement.* (*Speziell bei ganzen Zahlen auch: Primzahl; bei Polynomen auch: irreduzibles Polynom.*)

[70] See MA-I, p. 63: *In einem Hauptidealring erzeugt ein unzerlegbares Element, das keine Einheit ist, ein teilerloses Primideal* (*dessen Restklassenring also ein Körper ist*).

[71] See MA-I, p. 64: *Ist ein Produkt durch das Primelement p teilbar, so muß ein Faktor es sein ...* This is the definition of a prime element.

unterscheiden, dasselbe Ideal; umgekehrt, aus $(m) = (n)$ folgt, dass m ein Teiler von n ist und umgekehrt, also $m = \varepsilon n$, wo ε Einheit; den Primzahlen entsprechen Primideale.[72]

Wenn Σ ein Körper, so sind z.B. die Primzahlen von $\Sigma[x]$ die irreduziblen Polynome. Cauchy hat eben die komplexen Zahlen durch den Restklassenring mod $x^2 + 1$ in dem Ring der Polynome mit reellen Koeffizienten eingeführt.[73]

Satz. Jedes Element eines euklidischen Ringes lässt sich eindeutig in die Form bringen

$$a = \varepsilon p_1 p_2 \dots p_r,$$
$$\downarrow$$
Einheit

wo $p_1, p_2, \dots, p_r$ keine Einheiten und Primzahlen sind. Das soll bedeuten: in jeder analogen Zerlegung $a = \varepsilon' p_1' p_2' \dots p_{r'}'$ ist $r' = r$ und bis auf Anordnung $p_i' = p_i \xi_i$, ξ_i Einheit.[74]

Beweis.

1.) Eindeutigkeit beweist man so:[75] Für $r = 1$ (also a Primzahl) ist alles trivial. Es sei also die Eindeutigkeit für diejenigen Zahlen bewiesen, die sich in weniger als r Primfaktoren zerlegen lassen. Dann teilt p_1 das Produkt $p_1' \dots p_{r'}'$, also mindestens einen Faktor;[76] z.B. p_1'; weil p_1' Primzahl, so ist $p_1' = \xi p_1$, ξ Einheit. Durch kürzen:

$$\varepsilon p_2 p_3 \dots p_r = \varepsilon' \xi p_2' \dots p_{r'}';$$

und nun ist für diese Zahlen ($r - 1$ statt r) schon alles bewiesen.

2.) Die Möglichkeit der Zerlegung ist in Ringen, wo es eine vernünftige Normdefinition gibt, leicht zu erbringen. Im allgemeinen führt man den Beweis so: Es sei a gegen Vor. nicht durch Primzahlen darstellbar; also ist a zerlegbar, $a = bc$, b, c keine Einheiten, und z.B. b nicht durch Primzahlen darstellbar u.s.w. So bekommt man eine Folge

$$a_1, a_2, a_3, \dots, a_i, \dots,$$

---

[72] See MA-I, p. 63.
In his records, Jarník continues by the following text: *und zusammengesetzten Zahlen entsprechen keine Primideale, denn wenn* $a = bc$ (b, c *keine Einheiten*) *so ist* ... However, this text is crossed out.

[73] Van der Waerden recalled this fact also at the end of the lecture of December 2.

[74] The formulation of this theorem is not successful enough. On the one hand, the considered element must be non-zero, on the other hand the notion of associated elements could be used, but it had not been introduced. The corresponding theorem in MA-I, p. 65, excludes the zero element: *In einem Hauptidealring läßt sich jedes Element* $\neq 0$ *als Produkt von Primfaktoren darstellen, und die Darstellung ist bis auf Einheitsfaktoren eindeutig.*

[75] See MA-I, p. 65.

[76] In MA-I, the author refers to the auxiliary proposition I on page 64: *Ist ein Produkt durch das Primelement p teilbar, so muß ein Faktor es sein ...*

wo a_i ein echter Teiler von a_{i-1} ist.[77] Es sei $\mathfrak{a}$ die Menge aller Zahlen, die mindestens durch ein a_i teilbar sind; das ist ein Ideal, denn aus $a_i|a$, $a_k|b$, $k \geq i$, folgt $a_k|a \pm b$, $a_k|rb$ (r aus dem Ring). Also ist es ein Ideal, also ein Hauptideal (c). c ist auch eine Zahl von (c), muss also z.B. durch a_i teilbar sein: $c = da_i$. a_{i+1} ist aber auch in (c) enthalten, also $a_{i+1} = ec$; daher $a_{i+1} = eda_i$, aber $a_i = fa_{i+1}$, $a_{i+1} = edfa_{i+1}$, $1 = edf$, also ist f eine Einheit, gegen Voraussetzung, dass a_{i+1} ein echter Teiler von a_i ist.

Insbesondere gilt also die Zerlegbarkeit in $\Sigma[x]$, wo Σ ein Körper.[78]

Wir wollen noch folgenden Satz beweisen:[79]

Wenn $\mathcal{S}$ ein Ring ohne Nullteiler, mit Einheitselement ist, und in ihm die eindeutige Zerlegbarkeit in Primzahlen gilt, so gilt sie auch in $\mathcal{S}[x]$.

Beweis. Wenn $a = p_1^{\varrho_1} p_2^{\varrho_2} \dots p_r^{\varrho_r}$, $b = p_1^{\sigma_1} p_2^{\sigma_2} \dots p_r^{\sigma_r}$ zwei Elemente aus $\mathcal{S}$ sind (p_i Primzahlen), so definieren wir den grössten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von a, b durch

$$p_1^{\min(\varrho_1,\sigma_1)} p_2^{\min(\varrho_2,\sigma_2)} \dots, \quad \text{bzw.} \quad p_1^{\max(\varrho_1,\sigma_1)} p_2^{\max(\varrho_2,\sigma_2)} \dots$$

Sie haben offenbar die Eigenschaften des grössten gemeins. Teilers, bzw. kleinst. gem. Vielfachen. Wenn ab durch eine Primzahl q teilbar ist, so ist entweder a oder b durch die Primzahl teilbar; sonst hätten wir nämlich eine Zerlegung von ab in Primfaktoren, wo q nicht vorkommt, und eine andere von $ab = q \cdot c$, wo q vorkommt.[80]

Bei einer Funktion[81] $f(x) = a_m x^m + \dots + a_0$ aus $\mathcal{S}[x]$ nennen wir den gr. gem. Teiler von $a_m, a_{m-1}, \dots, a_0$ ihren Inhalt. Wenn er gleich d ist, so lässt sich schreiben

$$f(x) = d(b_m x^m + \dots + b_0),$$

wo $b_m x^m + \dots + b_0$ ein Polynom mit Inhal 1, eine sog. Einheitsform ist.[82]

Produkt von zweier Einheitsformen f, g ist wieder eine Einheitsform;[83] denn sonst wäre

$$f(x)g(x) \equiv 0 \pmod{p},$$

[77] In MA-I, p. 65, the author refers to the auxiliary proposition II on page 64: *Eine Kette von Elementen $a_1, a_2, \dots$, deren jedes folgende ein echter Teiler des vorangehenden ist, kann nur endlichviele Glieder enthalten.*

[78] See MA-I, p. 66.

[79] See MA-I, p. 73–76.

This is a generalization of the previous theorem. Instead of the term prime number, it would be more suitable to use the term irreducible element.

The following proof is not transparent enough. Some preliminaries could have been prepared as lemmas. Van der Waerden did not follow this way probably in view of a more general situation: $\mathcal{S}$ is not a principal ideal ring.

[80] In MA-I, this part of the proof is not included, the author refers to the exercice on page 67 (*Aufgabe* 7).

[81] A polynomial is meant.

[82] See MA-I, p. 74, where this part is more comprehensible.

[83] See MA-I, p. 74, where this proposition is called *Hilfssatz 1.*

wo p eine Primzahl ist und die Kongruenz bedeuten soll, dass alle Koeffizienten von $f(x)g(x)$ durch p teilbar sind. In $f(x)$ gibt es aber einen Koeffizienten, der nicht durch p teilbar ist (weil Einheitsform), ebenso in g.

Es sei $\mathcal{S}/(p) = \overline{\mathcal{S}}$; dieser Ring ist ohne Nullteiler, da aus $ab \equiv 0\ (p)$ folgt $a \equiv 0$ oder $b \equiv 0\ (p)$. $\mathcal{S}$ ist auf $\overline{\mathcal{S}}$ meromorph abgebildet. Ich bilde nun den Ring $\overline{\mathcal{S}}[x]$; zu $f(x)$, $g(x)$ sind in $\overline{\mathcal{S}}[x]$ zwei Polynome $\overline{f}(x) \neq 0$, $\overline{g}(x) \neq 0$ zugeordnet; zu $f(x)g(x)$ ihr Produkt $\overline{f}(x)\overline{g}(x) = 0$; also hätte $\overline{\mathcal{S}}[x]$ Nullteiler, was aber nicht der Fall ist, weil $\overline{\mathcal{S}}$ keine hat.

Ich will nun $\mathcal{S}[x]$ in $\Sigma[x]$ einbetten (Σ Quotientenkörper von $\mathcal{S}$).

Es sei nun $\varphi(x)$ ein Polynom aus $\Sigma[x]$:

$$\varphi(x) = \Sigma\alpha_i x^i = \frac{c}{d} f(x)$$

(ich bringe alle α_i auf gemeinsamen Nenner d, nehme im Zähler den Inhalt c heraus, so dass $f(x)$ eine Einheitsform ist).

Wenn nun $\varphi(x) = \frac{c'}{d'} f'(x)$ (c', d' aus S, $f'(x)$ Einheitsform), so ist

$$cd' f(x) = c' d f'(x),$$

also der Inhalt der linken Seite $= cd' =$ Inhalt der rechten Seite (bis auf Einheiten) $= c'de$, e Einheit.[84]

$$\frac{c}{d} = \frac{c'}{d'} e, \quad \text{also} \quad f' = ef.$$

Jedem $\varphi(x)$ ist also bis auf Einheiten eine und nur eine Einheitsform zugeordnet; umgekehrt entspricht jeder Einheitsform ein und nur ein Polynom $\varphi(x)$ aus $\Sigma[x]$ bis auf Faktoren aus Σ.

Wenn $\psi(x) = \frac{c'}{d'} f'(x)$, so ist

$$\varphi(x)\psi(x) = \frac{cc'}{dd'} f(x) f'(x);$$

dem Produkt ist das Produkt zugeordnet.

Weil aber $\Sigma[x]$ (weil Σ ein Körper) ein euklidischer Ring ist, so lässt sich jedes Polynom aus $\Sigma[x]$ eindeutig in Primfaktoren zerlegen, und dasselbe übertragt sich in unserer Zuordnung auf die Einheitsformen, und weil auch in $\mathcal{S}$ die eindeutige Zerlegung gilt, so lässt sich diese Zerlegung auf beliebige Funktionen aus $\mathcal{S}[x]$ übertragen:

$$\begin{array}{ccc} f(x) & = & d \cdot e(x) \\ & & \downarrow \quad \downarrow \\ & & \text{Inhalt} \quad \text{Einheitsform} \end{array}$$

wir zerlegen einfach den Inhalt und die Einheitsform. w.z.b.w.

[84] On the following line, for the sake of uniformity, it should be written more precisely: $f'(x) = ef(x)$.

Wir haben nebenbei noch bewiesen: Wenn $f(x)$ in $\mathcal{S}[x]$ irreduzibel ist (also auch Einheitsform), so bleibt sie in $\Sigma[x]$ irreduzibel – denn einer Zerlegung in $\Sigma[x]$ würde eine Zerlegung in $S[x]$ entsprechen.[85]

Folgerung. Wenn Σ ein Körper, so folgt durch Induktion sofort aus unserem Satz:[86]

In $\Sigma[x_1, x_2, \ldots, x_n]$ gilt die eindeutige Zerlegung in Primfaktoren, wenn Σ ein Körper.

$\frac{2}{\text{XII}}$

Kapitel II. Körpertheorie

§ 1. Primkörper

Ein Körper, der keinen echten Unterkörper enthält, heisst Primkörper.[87]

Satz. Jeder Körper Ω enthält einen und nur einen Primkörper Π.

Beweis. Wir nehmen das Einheitselement e von Ω und alle Elemente ne (n ganz rational); die bilden einen Ring $\mathcal{R}$, denn

$$ne + me = (n+m)e, \qquad neme = nme^2 = nme.$$

Der Quotientenkörper Π von $\mathcal{R}$ leistet das gewünschte: denn jeder Teilkörper von Ω muss e, also auch ne und die Brüche $\frac{ne}{me}$ enthalten, muss also Π enthalten. Π ist der Durchschnitt von allen Unterkörpern von Ω.

Es genügt, die Struktur von $\mathcal{R}$ zu betrachten. $\mathcal{R}$ wird durch die Zuordnung

$$n \leftrightarrow ne$$

$$\text{wegen} \qquad m+n \leftrightarrow (m+n)e = me + ne$$

$$mn \leftrightarrow mne = mene$$

ein meromorphes Abbild von $\mathcal{C}$ (Ring der ganzen Zahlen); also ist $\mathcal{R}$ isomorph mit einem Restklassenring von $\mathcal{C}$; d.h. mit

$$\mathcal{C}/(0), \qquad \mathcal{C}/(n) \quad (n>1) \qquad \text{oder} \qquad \mathcal{C}/(1).$$

---

[85] See MA-I, p. 76.

[86] See MA-I, p. 76, where a more general formulation is given – not for fields, but for integral domains (with an identity element) in which the unique factorization theorem holds.

[87] For the whole Section 1 see MA-I, pp. 86–88, where the author obtains the prime field as an intersection of all subfields.

$\mathcal{C}/(1)$ kommt nicht in Frage, da $\mathcal{R}$ mehr als ein Element hat, nämlich sicher 0 und e. $\mathcal{C}/(n)$, wo n keine Primzahl, auch nicht, weil $\mathcal{R}$ ohne Nullteiler ist. Also ist entweder

1.) $\mathcal{R} \cong \mathcal{C}/(0)$, also $\mathcal{R} \cong \mathcal{C}$

oder

2.) $\mathcal{R} \cong \mathcal{C}/(p)$, p Primzahl.

Man sagt, der Primkörper sei im Falle 1.) von Charakteristik 0, im Falle 2.) von Charakteristik p.

Im 1. Falle ist $0 \cdot e$ das einzige Vielfache von e, welches gleich Null ist; im zweiten Falle ist genau dann $ne = 0$, wenn n durch p teilbar ist. Π ist isomorph im ersten Falle dem Körper $\mathcal{P}$ der rationalen Zahlen, im 2. Falle ist schon $\mathcal{C}/(p)$ ein Körper, also

$$\Pi = \mathcal{R} \cong \mathcal{C}/(p).$$

Die Struktur von Π ist also durch die Charakteristik völlig bestimmt.

Charakteristik eines beliebigen Körpers heisst die Charakteristik seines Primkörpers.

§ 2. Einfache Körpererweiterungen

Wir wollen im folgenden Körper aus Primkörpern aufbauen.[88]

Es seien Σ, Ω zwei Körper, $\Sigma \subseteq \Omega$. Es sei M eine Menge von Elementen aus Ω. Wir wollen nun den kleinsten Körper $\Sigma(M)$ und den kleinsten Ring $\Sigma[M]$ bilden, der Σ und M enthält. $\Sigma[M]$ muss alle Polynome

$$(*) \qquad f(m_1, m_2, \dots)$$

enthalten, wo die Koeffizienten zu Σ, die m_i zu M gehören; und das genügt bereits, da die Menge der Polynome $(*)$ einen Ring, also den gesuchten Ring $\Sigma[M]$ bildet. $\Sigma(M)$ ist dann einfach der Quotientenkörper von $\Sigma[M]$. Wir sprechen von der Ring- bzw. Körperadjunktion von M zu Σ.[89]

Wir betrachten nun die Adjunktion eines einzigen Elementes ξ.[90] Der Polynombereich $\Sigma[x]$ und $\Sigma[\xi]$ stehen in meromorphem Verhältnis

$$\Sigma[x] \sim \Sigma[\xi],$$

wo die Meromorphie durch

$$f(x) \leftrightarrow f(\xi)$$

[88] For an almost entire Section 2 see MA-I, pp. 88–94.

[89] For the field adjunction see MA-I, pp. 88–89, where the author defined $\Sigma(M)$ as an intersection of all subfields that containing both Σ and M.

[90] See MA-I, pp. 89–94.

(f Polynom mit Koeff. aus Σ) festgestellt wird. Also ist

$$\Sigma[\xi] \cong \Sigma[x]/\mathfrak{a}\,;$$

dabei ist $\mathfrak{a}$ ein Ideal aus $\Sigma[x]$. $\mathfrak{a}$ muss ein Primideal sein, denn $\Sigma[\xi]$ hat keine Nullteiler (wegen $\Sigma[\xi] \subseteq \Omega$). Einheitsideal kommt auch nicht in Betracht, da Σ schon mehr als ein Element enthält; dazu kommt noch das Nullideal in Betracht. Die Primideale in $\Sigma[x]$ werden aber durch in $\Sigma[x]$ irreduzible Polynome $f(x)$ mit Koeff. aus Σ erzeugt; also ist entweder

1.) $\Sigma[\xi] \cong \Sigma[x]/f(x)$ ($f(x)$ irreduzibel),[91]

oder

2.) $\Sigma[\xi] \cong \Sigma[x]$.

Im ersten Fall ist also $\Sigma(\xi) = \Sigma[\xi]$, im zweiten $\Sigma(\xi) \cong \Sigma(x)$. Im ersten Fall ist $f(\xi) = 0$, im zweiten ist kein von Null formal verschiedenes Polynom in ξ gleich Null.

Im 1. Fall genügt ξ einer algebraischen Gleichung; man sagt: ξ ist algebraisch in bezug auf Σ.

Im 2. Fall genügt ξ keiner algebraischen Gleichung; man sagt: ξ ist transzendent in bezug auf Σ. Eine Unbestimmte und ein transzendentes Element führen also zu isomorphen Körpern.

Nun sei ein Körper Σ vorgelegt, und ich will zu Σ ein Element ξ adjungieren (bisher hatten wir einen Körper $\Omega \supseteq \Sigma$, in welchem ξ enthalten war – das soll jetzt nicht der Fall sein, wir sollen umgekehrt gerade einen solchen Körper konstruieren).[92]

Und zwar wollen wir erstens verlangen, dass ξ transzendent in bezug auf Σ ist; dann nehmen wir einfach ξ als eine Unbestimmte, und bilden den Polynombereich $\Sigma[\xi]$ und den Körper der rationalen Funktionen $\Sigma(\xi)$ der Unbestimmten ξ über Σ.

Zweitens wollen wir verlangen, dass ξ einer bestimmten algebraischen Gleichung $f(\xi) = 0$ genügt, wo f irreduzibel in Σ ist. Ich bilde zu diesem Zweck $\Sigma[x]/f(x)$; die Elemente sind also Restklassen von $\Sigma[x]$ modulo $f(x)$. Es sei $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$; jede Restklasse enthält genau einen Repräsentanten der Form

$$b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0.$$

Dieser Restklasse ordne ich das neue Symbol

$$b_{n-1}\xi^{n-1} + \cdots + b_0$$

[91] Formally, it should be $\Sigma[\xi] \cong \Sigma[x]/(f(x))$, resp. $\Sigma[\xi] \cong \Sigma[x]/(f)$. Likewise further.

[92] Van der Waerden similarly proceeded in Section 4 of the first chapter by a construction of the field of fractions (fraction field, quotient field, field of quotients).

zu (welches für $b_{n-1} = b_{n-2} = \cdots = b_1 = 0$ mit dem Element b_0 von Σ übereinstimmt) und mit diesen Symbolen rechne ich nach den Rechenregeln für die zugehörigen Restklassen; es ist dann in dieser Zuordnung

$$\begin{aligned} ex &\leftrightarrow e\xi \\ \xi^n + a_{n-1}\xi^{n-1} + \ldots &\leftrightarrow x^n + a_{n-1}x^{n-1} + \ldots \equiv 0, \end{aligned}$$

also $f(\xi) = 0$.

Z.B. hat Cauchy auf diese Weise die komplexen Zahlen als Restklassen mod x^2+1 eingeführt; ebenso können wir so $\sqrt{2}$ symbolisch durch Restklassen mod x^2-2 einführen; alle Körper, die wir durch verschiedene zulässige Deutungen von ξ erhalten, sind untereinander isomorph; z.B. alle die Körper, die ich durch Adjunktion der verschiedenen Wurzeln einer irred. Gleichung bekomme – das deutet schon an einen Zusammenhang mit den Automorphismen der Galoisschen Gruppe. Auch die algebraischen Funktionen – wenn Σ ein Körper der rat. Funktionen ist – können so vorteilhaft eingeführt werden.[93]

5
XII

Wenn wir also zu Σ ein in bezug auf Σ algebraisches Element ξ adjungieren, so erkennen wir aus dem vorangehenden sofort:

1.) Alles, was sich rational durch ξ mit Koeff. aus Σ ausdrücken lässt, lässt sich auch ganz rational durch ξ mit Koeff. aus Σ ausdrücken (da $\Sigma(\xi) = \Sigma[\xi]$).

2.) Alle Elemente von $\Sigma(\xi)$ lassen sich eindeutig in die Gestalt bringen

$$b_{n-1}\xi^{n-1} + \cdots + b_0, \qquad b_i \text{ aus } \Sigma,$$

wenn $\underline{n}$ die frühere Bedeutung hat. $\underline{n}$ heisst der Grad von ξ in bezug auf Σ.

3.) Wenn $\Sigma(\eta)$ eine andere Erweiterung von Σ ist, wo aber η derselben Gleichung $f(\eta) = 0$ wie ξ genügt ($f(x)$ irreduzibel in $\Sigma[x]$), so ist auch

$$\Sigma(\eta) = \Sigma[\eta] \cong \Sigma[x]/f(x),$$

also

$$\Sigma(\eta) \cong \Sigma(\xi),$$

und zwar können wir den Isomorphismus durch die Zuordnung

$$\sum_i a_i\eta^i \leftrightarrow \sum_i a_i\xi^i$$

herstellen. Zwei Wurzeln eines und desselben irreduziblen Polynoms in $\Sigma[x]$ erzeugen isomorphe Körper.

[93] Cauchy's construction of the field of complex numbers has already been mentioned in Section 7 of the first chapter.

Noch etwas allgemeiner: Wenn $\Sigma \cong \overline{\Sigma}$, $f(x)$ irreduzibel in $\Sigma[x]$, und $a \leftrightarrow \overline{a}$, $f(x) \leftrightarrow \overline{f}(x)$; wenn weiter $f(\xi) = 0$, $\overline{f}(\overline{\xi}) = 0$, so wird durch

$$\sum_i b_i \xi^i \;\leftrightarrow\; \sum_i \overline{b_i}\, \overline{\xi}^i$$

ein Isomorphismus

$$\Sigma(\xi) \cong \overline{\Sigma}\,(\overline{\xi})$$

erzeugt, bei welchem die Elemente von Σ, $\overline{\Sigma}$ nach dem ursprünglichen Isomorphismus zugeordnet werden, man sagt, der neue Isomorphismus ist eine Fortsetzung des alten.

Zwei isomorphe Erweiterungen Ω, Ω' eines Körpers Σ, wo alle Elemente des Grundkörpers Σ sich selbst zugeordnet werden, heissen „äquivalente Erweiterungen von Σ“. Die Elemente ξ, ξ', die dabei ineinander übergehen, heissen äquivalent in bezug auf Σ.

Wenn die beiden Erweiterungen Ω, Ω' in einem Erweiterungskörper Λ enthalten sind, sagt man, dass Ω, Ω' konjugiert in bez. auf Σ, und ebenso ξ, ξ' konjugiert in bez. auf Σ sind.

Die verschiedenen Nullstellen eines irreduziblen Polynoms $f(x)$ aus $\Sigma[x]$, die in einem und demselben Erweiterungskörper von Σ liegen, sind also konjugiert bez. Σ.

§ 3. Lineare Abhängigkeit in bezug auf einen Körper

Es sei ein Körper Σ und ein Bereich von Grössen u, v, w, … gegeben, die man addieren und mit den Elementen des Körpers multiplizieren darf, wobei die üblichen Rechenregeln gelten:[94]

1.) $u + v = v + u$
2.) $(u + v) + w = u + (v + w)$
3.) $\sigma(u + v) = \sigma u + \sigma v$
4.) $(\sigma + \tau)u = \sigma u + \tau u$
5.) $\sigma(\tau u) = (\sigma\tau)u$
6.) $\varepsilon u = u$, wenn ε das Einheitselement von Σ ist.

$u_1, u_2, \ldots, u_n$ heissen dann linear unabhängig in bezug auf Σ, wenn aus

$$\sum_{i=1}^{n} \alpha_i u_i = 0, \quad \alpha_i \in \Sigma, \quad \text{folgt} \quad \alpha_i = 0;$$

[94] For the whole Section 3 see MA-I, pp. 95–97. Van der Waerden in MA-I, p. 95, considered a ring containing a field with the common identity; therefore he needed no axioms. In his lectures, he presented the axiomatic definition of a vector space; it was still necessary to add the axiom of the zero element o, for example in the form $0 \cdot u = o$ for all u.

sonst linear abhängig in bezug auf Σ. Wenn aber $u_1, u_2, \ldots, u_n$ linear abhängig in bezug auf Σ sind, so gilt

$$\sum_{i=1}^{n} \alpha_i u_i = 0, \quad \text{wo z.B.} \quad \alpha_1 \neq 0,$$

also

$$u_1 = -\frac{\alpha_2}{\alpha_1} u_2 - \frac{\alpha_3}{\alpha_1} u_3 - \ldots,$$

d.h. eine von den Grössen $u_1, u_2, \ldots, u_n$ ist von den anderen „linear abhängig“ in bezug auf Σ.

Zwei Systeme von solchen Grössen $u, v, \ldots$ M, N heissen linear äquivalent, wenn sowohl M von N als auch N von M linear abhängig ist. „M ist linear abhängig von N“ soll bedeuten, dass jede Grösse u aus M sich in der Form einer endlichen Summe $u = \sum \alpha_i v_i$ mit $\alpha_i \in \Sigma$, $v_i \in N$ darstellen lässt. Die Eigenschaft, dass ein System von einem anderen linear abhängig ist, ist transitiv, also auch die lineare Äquivalenz. (Alle diese Begriffe sind in bezug auf den Grundkörper Σ zu verstehen.)

Nun gilt der wichtige Austauschsatz:[95]

Wenn ein System U von Elementen $u_1, u_2, \ldots$ und ein endliches System V: $v_1, v_2, \ldots, v_s$ gegeben ist, wenn die v untereinander linear unabhängig sind und V von U linear abhängt, so gibt es in U ein Teilsystem von genau s Elementen

$$u_{i_1}, u_{i_2}, \ldots, u_{i_s},$$

so dass die Ersetzung von $u_{i_1}, u_{i_2}, \ldots, u_{i_s}$ durch $v_1, v_2, \ldots, v_s$ U in ein äquivalentes System überführt (alles in bezug auf einen Grundkö. Σ).

Beweis. Für $s = 0$ ist es trivial.

Also gehen wir durch Induktion weiter. Es sei dies bereits für $s-1$ Elemente bewiesen.

Das System U', der aus U durch Ersetzung von $u_{i_1}, \ldots, u_{i_{s-1}}$ durch $v_1, \ldots, v_{s-1}$ entsteht, sei mit U äquivalent. v_s ist von U, also auch von U' linear abhängig, also

$$v_s = \sum_{i=1}^{s-1} \alpha_i v_i + \sum \beta_k u_k,$$

wo die zweite Summe über einige der übriggebliebenen u_k zu erstrecken ist. Hier ist mindestens ein β_k von Null verschieden, also lässt sich das zugehörige u_k – wir bezeichnen es mit u_{i_s} – durch $v_1, \ldots, v_s$ und die übrigen u_k ausdrücken:

$$u_{i_s} = \sum_{i=1}^{s} \alpha'_i v_i + \sum \beta'_k u_k.$$

Daraus ist die Richtigkeit der Behauptung sofort zu entnehmen (nach Steinitz).

[95] In MA-I, p. 96, the author considered a finite set $u_1, u_2, \ldots$

Aus diesem Satz lässt sich die Theorie der linearen Gleichungen ohne Determinanten aufbauen.

Folgerungen. Wenn die linear unabh. Grössen $v_1, v_2, \ldots, v_s$ linear von U abhängen, so enthält U wenigstens s Elemente.

Insbesondere also: s Elemente, die von $s-1$ Elementen linear abhängen, sind immer linear abhängig.

Wenn

$$u_1, u_2, \ldots, u_m,$$

$$v_1, v_2, \ldots, v_n$$

zwei unabhängige äquivalente Systeme sind, so ist $m = n$.

Eine Menge $\mathcal{M}$ von Elementen $u, v, w, \ldots$ heisst in bezug auf Σ von endlichem linearem Rang, wenn alle Elemente von $\mathcal{M}$ von endlich vielen unter ihnen linear abhängen. Von diesen letzteren kann ich die event. linear abhängigen noch unterdrücken, und bekomme so endlich viele linear unabhängige Elemente von $\mathcal{M}$, von welchen alle anderen Elemente aus $\mathcal{M}$ linear abhängen – eine unabhängige lineare Basis[96] von $\mathcal{M}$ (alles in bezug auf Σ). Wenn

$$M_1 : u_1, u_2, u_3, \ldots, u_m,$$

$$N_1 : v_1, v_2, v_3, \ldots, v_n$$

zwei linear unabhängige Basen von $\mathcal{M}$ sind, so sind sie offenbar linear äquivalent, also $m = n$. n heisst der Rang von $\mathcal{M}$ bez. Σ.[97] Eine Untermenge $\mathcal{N}$ von $\mathcal{M}$ hat dann auch einen endlichen linearen Rang, der $\leq n$ ist, da alle Elemente der Untermenge $\mathcal{N}$ linear von der Basis von $\mathcal{M}$ abhängen.

Nach dem Austauschsatz kann ich jede unabh. lineare Basis von $\mathcal{N}$ zu einer Basis von $\mathcal{M}$ ergänzen.

§ 4. Endliche und algebraische Körpererweiterungen

Es sei Σ ein Körper, Ω sein Erweiterungskörper. Wenn Ω einen endlichen linearen Rang in bez. auf Σ hat, so heisst Ω eine endliche Erweiterung von Σ; sonst eine unedliche Erweiterung.[98]

Beispiel: $\Sigma(x)$ ist eine unendliche Erweiterung von Σ, da $1, x, x^2, \ldots$ linear unabhängig bez. Σ sind. $\Sigma(\xi)$, wo ξ algebraisch n-ten Grades über Σ, ist eine

[96] In MA-I, p. 97, a more appropriate term *linear-unabhängige Basis* is given.

[97] See MA-I, p. 97, where two equivalent terms are given: *Man nennt sie den Grad oder linearen Rang der endlichen Erweiterung* $\mathfrak{G}$ *in bezug auf* Δ.

[98] For the whole Section 4 see viz MA-I, pp. 96–99.

endliche Erweiterung; denn jedes Element lässt sich durch $\sum_0^{n-1} a_i\xi^i$ linear ausdrücken; weil diese Darstellung eindeutig ist, so bilden $1, \xi, \xi^2, \ldots, \xi^{n-1}$ eine lineare Basis von $\Sigma(\xi)$ bez. Σ. Einfache algebraische Erweiterungen sind also endliche Erweiterungen. Der lineare Rang von Ω in bez. auf Σ heisst der Körpergrad von Ω über Σ, in Zeichen: $\big(\Omega/\Sigma\big)$.

Ω heisst eine algebraische Erweiterung von Σ, wenn jedes Element von Ω algebraisch in bezug auf Σ ist. Jede endliche Erweiterung ist algebraisch; denn, wenn ξ aus Ω, so müssen die $n+1$ Grössen $1, \xi, \xi^2, \ldots, \xi^n$ linear abhängig sein, wenn $\big(\Omega/\Sigma\big) = n$. Also gilt eine Gleichung $\sum_0^n a_i\xi^i = 0$, wo nicht alle a_i gleich Null sind. Nichtalgebraische Erweiterungen heissen transzendente Erweiterungen.

Satz. Wenn Σ eine endliche Erweiterung von K, Ω eine endliche Erweiterung von Σ, so ist auch Ω eine endliche Erweiterung von K. Und es gilt

$$\big(\Omega/K\big) \;=\; \big(\Omega/\Sigma\big)\big(\Sigma/K\big).$$

Beweis.[99] Es sei $u_1, \ldots, u_r$ eine Basis von Σ über K, $v_1, \ldots, v_s$ eine Basis von Ω über Σ. Dann ist, wenn w aus Ω:

$$\begin{aligned} w &= \Sigma\alpha_i v_i \qquad (\alpha_i \;\text{ aus }\; \Sigma) \\ &= \Sigma\Sigma\beta_{ik} u_k v_i \quad (\beta_{ik} \;\text{ aus }\; K). \end{aligned}$$

Die $u_k v_i$ sind linear unabhängig bez. K, denn aus (β_{ik} aus K)

$$\Sigma\beta_{ik} u_k v_i = 0 \qquad \text{folgt} \qquad \sum_k \beta_{ik} u_k = 0, \quad \text{also} \quad \beta_{ik} = 0;$$

die rs Zahlen $u_k v_i$ bilden also eine unabh. lineare Basis von Ω bez. K, w.z.b.w.

$\frac{9}{\text{XII}}$

Es sei $K \subseteq \Sigma \subseteq \Omega$; Ω algebraisch über Σ, Σ algebraisch über K. Behauptung: Ω ist algebraisch über K.[100]

Beweis. Es sei $\omega \in \Omega$; dann ist

$$\omega^n + \sigma_{n-1}\omega^{n-1} + \cdots + \sigma_0 = 0,$$

[99] For this theorem and its proof see MA-I, p. 98; the equality provided is called there *Gradrelation.*

[100] See MA-I, p. 99: *Ist α algebraisch in bezug auf Σ und Σ algebraisch in bezug auf Δ, so ist α algebraisch in bezug auf Δ.*

wo $\sigma_i \in \Sigma$. Der Körper $K(\sigma_0)$ ist einfache alg. Erw. von K, also endliche Erweiterung von K[101]; $K(\sigma_0, \sigma_1)$ ist eine einfache alg., also endliche Erweiterung von $K(\sigma_0)$, also nach dem vorangehenden eine endliche Erweiterung von K; u.s.w. Schliesslich ist $K(\sigma_0, \sigma_1, \ldots, \sigma_{n-1})$ eine endliche Erweiterung von K; $K(\sigma_0, \sigma_1, \ldots, \sigma_{n-1}, \omega)$ eine einfache algebr., also endliche Erweiterung von $K(\sigma_0, \ldots, \sigma_{n-1})$, also eine endliche Erweiterung von K; daher ist ω algebraisch über K, w.z.b.w.

Durch sukzessive Adjunktion von Grössen, wobei jede folgende algebraisch ist über den Körper, der durch die Adjunktion der vorangehenden entsteht, entsteht offenbar eine endliche Erweiterung. Umgekehrt: Jede endliche Erweiterung entsteht durch Adjunktion von endlich vielen algebraischen Grössen – es genügt nämlich, die Basis zu adjungieren.

§ 5. Galoissche Erweiterungen

Es sei ein Kö. K und ein $f(x)$ aus $K[x]$ gegeben; ich suche einen Körper über K, in welchem $f(x)$ in Linearfaktoren zerfällt.[102] Ich adjungiere zunächst zu K eine Nullstelle x_1 von $f(x)$; dann fahre ich es so fort; wenn nach Adjunktion von $x_1, x_2, \ldots, x_k$ $f(x)$ in $K(x_1, x_2, \ldots, x_k)$ schon in

$$f(x) = (x - x_1) \ldots (x - x_k)\, \psi_1(x)\, \psi_2(x) \ \ldots$$

($\psi_1, \psi_2, \ldots$ irreduzibel in $K(x_1, \ldots, x_k)$), so adjungiere ich eine Nullstelle von $\psi_1(x)$, und bekomme $K(x_1, \ldots, x_{k+1})$, wo sich von $\psi_1(x)$ wieder (mindestens) ein linearer Faktor, nämlich $x - x_{k+1}$, abspaltet. So kann ich fortfahren, bis ich zu einem Körper komme $K(x_1, x_2, \ldots, x_n)$, in welchem

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n)$$

ist.[103] Dieser Körper heisst Zerfällungskörper oder Wurzelkörper von $f(x)$ in bezug auf K.[104]

Ich behaupte: sein Typus[105] ist eindeutig bestimmt; d.h. wenn in einem Körper $\Omega \supseteq K$ $f(x)$ zerfällt: $f(x) = (x-\xi_1) \ldots (x-\xi_n)$, so ist $K(\xi_1, \xi_2, \ldots, \xi_n)$ isomorph bez. K zu $K(x_1, x_2, \ldots, x_n)$ und man kann einen solchen Isomorphismus herstellen, indem man einfach die $x_1, \ldots, x_n$ der Reihe nach den passend umnumerierten $\xi_1, \ldots, \xi_n$ zuordnet.

---

[101] Added: *von K*.

[102] For the first part of Section 5 see MA-I, pp. 99–102.

[103] Van der Waerden considered a so-called monic polynomial. In MA-I, p. 100, he reminds the reader of this non-essential restriction in a footnote: *Den höchsten Koeffizienten von $f(x)$ wollen wir hier und im folgenden gleich 1 annehmen, was offenbar nichts ausmacht.*

[104] In MA-I, p. 99, van der Waerden used the term *Zerfällungskörper* only; the term *Wurzelkörper* was used in another meaning in MA-I, p. 119.

[105] The term *Typus*, which van der Waerden used in his lectures, was avoided in the monograph MA, as already noted at the end of Section 2 of the first chapter.

Beweis (durch Induktion). Es sei schon (nach passender Umnumerierung)

$$K(x_1, \ldots, x_k) \cong K(\xi_1, \ldots, \xi_k)$$

bez. K, wo $x_i \leftrightarrow \xi_i$. Es ist dann in $K(x_1, \ldots, x_k)$

$$f(x) = (x - x_1) \ldots (x - x_k)\, \varphi_1(x) \ \ldots \ \varphi_r(x)$$

und in $K(\xi_1, \ldots, \xi_k)$ hat man entsprechende Zerlegung

$$f(x) = (x - \xi_1) \ldots (x - \xi_k)\, \psi_1(x) \ \ldots \ \psi_r(x);$$

in $K(x_1, \ldots, x_k)$ adjungiere ich noch eine Nullstelle x_{k+1} von $\varphi_1(x)$; in $K(\xi_1, \ldots, \xi_k)$ zerfällt $f(x)$, also auch $\psi_1(x)$: es sei ξ_{k+1} eine Nullstelle von $\psi_1(x)$; ich adjungiere noch ξ_{k+1} zu $K(\xi_1, \ldots, \xi_k)$. Dann sind aber auch $K(x_1, \ldots, x_{k+1})$, $K(\xi_1, \ldots, \xi_{k+1})$ in der verlangten Weise isomorph.

Dabei ist (bei dieser sukzessiven Adjunktion von x_1, ξ_1, x_2, ξ_2, $\ldots$) sogar jeder Isomorphismus eine Erweiterung des vorangehenden.

Die Eigenschaften der Nullstellen sind also von der Konstruktion des Wurzelkörpers unabhängig; insbesondre hängt die Vielfachheit der Wurzeln nicht von der Konstruktion des Wurzelkörpers ab.[106]

Wir wenden uns nun der Frage zu: Wann hat ein Polynom in seinem Zerfällungskörper mehrfache Nullsteller?

Wenn $f(x)$ ein Polynom, so entwickeln wir

$$f(x + h) = f(x) + hf'(x) + h^2 \cdot \quad + \ldots$$

und nennen $f'(x)$ die Ableitung von $f(x)$. Man stellt leicht fest, dass

$$\Big(\sum a_k x^k\Big)' = \sum k a_k x^{k-1},$$

und dass die gewöhnlichen Rechenregeln der Differentialrechnung gelten.

Wenn nun $f(x)$ eine doppelte Nullstelle hat,[107]

$$f(x) = (x - \xi_1)^2 (x - \xi_2) \ldots,$$

so ist $f'(x)$ offenbar durch $x - \xi_1$ teilbar; also haben $f(x)$, $f'(x)$ im Wurzelkörper einen gemeinsamen Teiler. Sonst ist aber, wenn

$$f(x) = (x - \xi_1)(x - \xi_2) \ldots (x - \xi_n) \qquad (\xi_i \neq \xi_k \ \text{ für } \ i \neq k)$$

$$f'(x) = (x - \xi_1) \cdots + \ \text{ Glieder ohne } \ (x - \xi_1);$$

[106] For the following text see MA-I, pp. 67–68.
[107] See MA-I, pp. 70, 102, 113.

also ist notwendig $(f, f') = 1$.[108] Die Eigenschaft, dass $(f, f') = 1$ oder $\neq 1$ ist, bleibt erhalten, wenn wir vom Wurzelkörper zu K selbst übergehen: denn man bestimmt ja den grössten gemeinsamen Teiler von zwei Polynomen in $K[x]$ durch den euklidischen Algorithmus, also rational.

Es kann vorkommen, dass ein irreduzibles Polynom mehrfache Wurzeln hat. Z.B: Es sei Π der Primkörper der Charakteristik p:

$$\Pi = \{0, 1, 2, \ldots, p-1\}$$

Wir bilden den Polynombereich $\Pi[x]$ und seinen Quotientenkörper $\Pi(x) = \Sigma$. In Σ ist[109] $f(z) = z^p - x$ irreduzibel; denn sonst wäre es schon in $\Pi[x, z]$ reduzibel (Gausssches Lemma); das ist aber unmöglich, da $f(z)$ in x linear ist. Die Ableitung ist $f'(z) = pz^{p-1} = 0$, also $(f, f') = z^p - x$, es gibt mehrfache Nullstellen; hier sogar eine p-fache Nullstelle:

Ich adjungiere eine Nullstelle ξ; dann ist

$$\xi^p = x, \quad \text{also} \quad z^p - x = z^p - \xi^p = (z - \xi)^p.$$

Dieser Umstand kann aber bei Charakteristik 0 nicht eintreten.[110]

Im Köper der Charakteristik 0 hat jedes irreduzible Polynom lauter einfache Nullstellen.

Beweis.

$$f(x) = x^n + a_{n-1}x^{n-1} + \ \ldots \quad \text{irreduzibel}$$

$$f'(x) = nx^{n-1} + \ldots ;$$

also ist f' vom Grad $n-1$, $f(x)$ kann also mit f' keinen gemeinsamen Teiler haben.

Wir unterscheiden zwei Arten von irreduziblen Polynomen:

1.) die <u>separablen</u> – welche in ihrem Wurzelkörper nur einfache Nullstellen haben,

2.) die <u>inseparablen</u> – die übrigen.

Im Körper der Charakteristik 0 ist also jedes irreduzible Polynom separabel; im Körper der Charakteristik p ist aus demselben Grund jedes Polynom separabel, dessen Ableitung nicht Null ist.

---

[108] For the symbol of the greatest common divisor see Section 6 of the first chapter. The relation $(f, f') \neq 1$ means that (f, f') has a non-zero degree.

[109] Absolutely correctly, there should be *In* $\Sigma[z]$ *ist* ... These minor offenses against strict correctness occur here and there. For instance, van der Waerden uses in the same meaning f and $f(x)$. After all, in lectures it is usual.

[110] For the following text see MA-I, pp. 113–114.

Wann ist die Ableitung eines Polynoms im Körper der Charakteristik p gleich Null? Es muss $\Sigma k a_k x^{k-1} = 0$, also $a_k = 0$ für alle k, die nicht durch p teilbar sind; d.h. das Polynom muss die Form

$$\sum_{\lambda} a_{\lambda p} x^{\lambda p} = f(x^p)$$

haben; und dann ist auch die Ableitung wirklich Null; dann ist also

$$\big(f(x), f'(x)\big) = f(x),$$

und das Polynom, wenn irreduzibel, ist inseparabel.[111]

12 / XII

Ein Körper Ω über Σ heisst Galoissch über Σ, wenn jedes in $\Sigma[x]$ irreduzible Polynom, welches in Ω eine Wurzel hat, in Ω[112] vollständig zerfällt.[113]

Behauptung. Der Wurzelkörper $\Sigma(x_1, x_2, \ldots, x_n)$ eines Polynoms $f(x)$ aus $\Sigma[x]$ ist Galoissch über Σ.[114]

Beweis. Es sei $g(x)$ irreduzibel in $\Sigma[x]$, ξ eine Nullstelle von $g(x)$ in

$$\Omega = \Sigma(x_1, x_2, \ldots, x_n).$$

Wir wollen voraussetzen, dass $g(x)$ nicht vollständig in Ω zerfällt, dann ist

$$g(x) = (x - \xi)\, \varphi(x)\, \psi(x)\, \ldots,$$

wo $\varphi(x), \psi(x), \ldots$ irreduzibel in Ω, und etwa $\varphi(x)$ vom höheren als ersten Grad; es sei η eine Nullstelle von $\varphi(x)$ in einem Erweiterungskö. von Ω.

In $\Omega(\eta)$ betrachte ich $\Sigma(\xi)$ und $\Sigma(\eta)$, die sind isomorph bez. Σ, da $g(x)$ irreduzibel in $\Sigma[x]$. Ich adjungiere $x_1, x_2, \ldots, x_n$ zu $\Sigma(\xi)$ und $\Sigma(\eta)$; dann ist offenbar $\Sigma(x_1, x_2, \ldots, x_n, \xi) \cong \Sigma(x_1, x_2, \ldots, x_n, \eta)$ wobei Σ in sich selbst übergeht und auch die x_i bis auf die Reihenfolge. (Denn $f(x)$ zerfällt vollständig

---

[111] See MA-I, p. 113: *Für Charakteristik Null hat ein in $\Delta[x]$ irreduzibles Polynom $f(x)$ nur einfache Nullstellen; für Charakteristik p hat $f(x)$ (wofern es nicht konstant ist) dann und nur dann vielfache Nullstellen, wenn $f(x)$ sich als Funktion von x^p schreiben läßt.*

[112] Instead of Ω there should be correctly $\Omega[x]$.

[113] For the following parts see MA-I, pp. 103–104.
In MA-I, p. 103, the definition is given in this form (an algebraic extension is required): *Ein Körper Σ heißt Galoissch oder normal über Δ, wenn er erstens algebraisch in bezug auf Δ ist und zweitens jedes in $\Delta[x]$ irreduzible Polynom $g(x)$, das in Σ eine Nullstelle α hat, in $\Sigma[x]$ ganz in Linearfaktoren zerfällt.*

[114] See MA-I, p. 103: *Ein Körper, der aus Δ durch Adjunktion aller Nullstellen eines oder mehrerer oder sogar unendlichvieler Polynome aus $\Delta[x]$ entsteht, ist Galoissch.*

in Ω, die Wurzeln von $f(x)$ müssen den Wurzeln von $f(x)$ zugeordnet werden.) ξ lässt sich durch die x_i rational ausdrücken, weil $\xi \in \Omega$; also auch η ist durch die x_i rational ausdrückbar, gegen Vorauss.[115]

Eine algebraische Zahl σ bez. Σ wollen wir bez. Σ separabel nennen, wenn σ in $\Sigma[x]$ einer irreduz. separablen Gleichung genügt.[116]

Es seien n alg. Zahlen bez. Σ gegeben: $\sigma_1, \sigma_2, \ldots, \sigma_n$ und es sei σ_i separabel in bez. auf $\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_{i-1})$. Es sei weiter $\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_n)$ Galoissch über Σ. Zu den Hauptkapiteln der Galoisschen Theorie gehört das Studium von allen Automorphismen von $\Omega = \Sigma(\sigma_1, \sigma_2, \ldots, \sigma_n)$ bez. Σ.

Wir behaupten: die Anzahl dieser Automorphismen ist gleich dem Grad des Galoisschen Körpers über Σ.

Beweis. Wir betrachten $\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_i) = \Sigma_i$ und setzen voraus, dass die Anzahl von allen Isomorphismen bez. Σ von Σ_i zu den Teilkörpern von Ω gleich dem Grad des Körpers Σ_i über Σ ist. (Für $i = 0$ ist es trivialerweise richtig.) Nun sei

$$\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_i) \;\cong\; \Sigma(\sigma_1', \sigma_2', \ldots, \sigma_i')$$

ein von diesen Isomorphismen, wo $\sigma_k \leftrightarrow \sigma_k'$. Es sei λ der Körpergrad von $\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_{i+1})$ über $\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_i)$; σ_{i+1} genügt einer separablen irred. Gleichung in $\Sigma_i[x]$ $\varphi(x) = 0$ vom Grad λ mit verschiedenen Wurzeln. Ich bilde die zugehörige Gleichung $\varphi'(x) = 0$, die ihr wegen des Isomorphismus in $\Sigma(\sigma_1', \ldots, \sigma_i')$ entspricht. $\varphi(x)$ ist ein Faktor eines in Σ irreduziblen Polynoms $f(x)$; also ist auch $\varphi'(x)$ ein Faktor dieses Polynoms. Weil $f(x)$ in Ω eine Wurzel, σ_{i+1}, hat, so zerfällt $f(x)$ und daher auch $\varphi'(x)$ vollständig in Ω, und hat dort λ verschiedene Wurzeln; jede von diesen kann man zu σ_{i+1}' wählen und kommt so zu einem Isomorphismus

$$\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_{i+1}) \;\cong\; \Sigma(\sigma_1', \sigma_2', \ldots, \sigma_{i+1}') \quad (\Sigma),$$

der eine Fortsetzung des vorangehenden Isomorphismus ist. So fortfahrend, kommen wir endlich zu Isomorphismen

$$\Sigma(\sigma_1, \sigma_2, \ldots, \sigma_n) \;\cong\; \Sigma(\sigma_1', \ldots, \sigma_n'),$$

wo der Grad über Σ auf beiden Seiten übereinstimmt, und $\Sigma(\sigma_1', \ldots, \sigma_n')$ in $\Sigma(\sigma_1, \ldots, \sigma_n)$ enthalten ist, also $\Sigma(\sigma_1, \ldots, \sigma_n) = \Sigma(\sigma_1', \ldots, \sigma_n')$; also bekommen wir Automorphismen von $\Sigma(\sigma_1, \ldots, \sigma_n)$ bez. Σ, und zwar genau in

---

[115] In Jarník's records, the following text is crossed out: *Es seien $\sigma_1, \sigma_2, \ldots, \sigma_n$ endlich viele alg. Zahlen bezüglich Σ, und es sei ...* Van der Waerden apparently started to develop arguments which follow, but then he realized that he would had to define first the notion of a separable element.

[116] See MA-I, pp. 114–118. In his lectures, it is spoken on an algebraic number instead of an algebraic element (see § 2), and on a separable equation in place of a separable polynomial. See MA-I, p. 114, where the definition of a separable element is given as follows: *Ist Θ Nullstelle eines in $\Delta[x]$ irreduziblen Polynoms mit lauter getrennten (einfachen) Nullstellen, so heißt Θ separabel oder von erster Art in bezug auf Δ.*

der angegebenen Anzahl (da sich die Anzahl bei jedem Schritt genau mit λ multipliziert). Dies sind aber auch alle solche Automorphismen: denn ein jeder solcher Automorphismus enthält einen Isomorphismus

$$\Sigma(\sigma_1, \ldots, \sigma_i, \sigma_{i+1}) \;\cong\; \Sigma(\sigma'_1, \ldots, \sigma'_i, \sigma'_{i+1})$$

mit der Zuordnung $\sigma_k \leftrightarrow \sigma'_k$; dieser entsteht aber aus dem zugehörigen Isomorphismus zwischen

$$\Sigma(\sigma_1 \ldots \sigma_i) \;\cong\; \Sigma(\sigma'_1, \ldots, \sigma'_i)$$

genau dadurch, dass man links die Wurzel σ_{i+1} von $\varphi(x) = 0$, rechts eine Wurzel der entsprechenden Gleichung $\varphi'(x) = 0$ adjungiert; dies war aber eben unseres Konstruktionsverfahren. w.z.b.w.

Wenn aber eine von den n Adjunktionen inseparabel war, so haben wir bei der Wahl von σ'_{i+1} weniger als λ Möglichkeiten, also ist dann die Anzahl der Automorphismen kleiner als der Körpergrad.

Ich definiere: Ein algebraischer Körper Ω über Σ heisse separabel bez. Σ, wenn alle seine Elemente separabel bez. Σ sind. Wir sehen, das unser Galoisscher Körper Ω ein separabler Körper ist: denn sonst könnte man ihn auch so erzeugen, dass man zuerst eine inseparable Zahl adjungieren würde, was aber unmöglich ist, da dann die Anzahl der Automorphismen von Ω kleiner als sein Körpergrad sein müsste.

Wenn man bedenkt, dass man jeden Körper $\Sigma(\alpha_1, \alpha_2, \ldots, \alpha_n)$ (α_i algebr. bez. Σ) zu einem Galoisschen Körper über Σ erweitern kann, indem man noch die übrigen Wurzeln der zu $\alpha_1, \ldots, \alpha_n$ gehörigen irred. Gleichungen in Σ adjungiert, erkennt man: Adjunktion von endlich vielen separablen Elemente bez. Σ gibt einen separablen Körper bez Σ.

Wenn ξ, η in einem Galoisschen Körper Ω über Σ liegen und konjugiert sind, so kann man einen Automorphismus von Ω bez. Σ finden der ξ in η überführt: man gehe von dem Isomorphismus $\Sigma(\xi) \cong \Sigma(\eta)$ (Σ) mit $\xi \leftrightarrow \eta$ aus und setze ihn wie früher fort.

§ 6. Algebraisch abgeschossene Körper

Ein Körper Ω heisst algebraisch abgeschlossen, wenn jedes Polynom mit Koeffizienten aus Ω in Ω vollständig zerfällt.[117]

K sei ein Körper, Ω seine algebraische Erweiterung: wenn in Ω alle Polynome aus $K[x]$ vollständig zerfallen, so ist Ω algebraisch abgeschlossen.[118]

---

[117] Absolutely correctly proposition as well as in what follows: … *in* $\Omega[x]$ *vollständig zerfällt.* The same apples for the following proposition and in the sequel.
For this part see MA-I, pp. 198–203.

[118] In MA-I, p. 199, this proposition is called *Hilfssatz 1.*

Beweis. Es sei ξ algebraisch bez. Ω; dann ist auch ξ algebr. bez. K, also liegt ξ in Ω, w.z.b.w.

Wenn K nur abzählbar viele Elemente hat (was in den Anwendungen meistens der Fall ist), so kann man eine algebraische Erweiterung Ω von K konstruieren, die algebraisch abgeschlossen ist.[119]

Beweis. $f_1(x), f_2(x), \ldots$ seien alle (abzählbar viele) Polynome aus $K[x]$; ich adjungiere zuerst die Nullstellen von $f_1(x)$, dann diejenigen von $f_2(x)$ u.s.w. Die Vereinigung Ω der sukzessiven Erweiterungskörper $K_1, K_2, K_3, \ldots$ ist eine algebraische Erweiterung von K, und jedes Polynom $f_n(x)$ zerfällt in K_n, also umsomehr in Ω.

Es sei $\overline{\Omega}$ eine andere algebraische Erweiterung von K, die algebraisch abgeschlossen ist. In $\overline{\Omega}$ zerfallen wieder alle $f_1(x), f_2(x), \ldots$ vollständig; ich bilde erst $\overline{K_1}$ durch Adjunktion die Wurzeln in $\overline{\Omega}$ von $f_1(x)$; dann adjungiere ich die Wurzeln in $\overline{\Omega}$ von $f_2(x)$; so entsteht $\overline{K_2}$ u.s.w. Es ist

$$K_1 \cong \overline{K_1}, \qquad K_2 \cong \overline{K_2}, \quad \ldots ,$$

und zwar lässt sich jeder folgende Isomorphismus als Fortsetzung des vorangehenden bestimmen. Die Vereinigungsmenge $\overline{V}$ von $\overline{K_1}, \overline{K_2}, \ldots$ ist in $\overline{\Omega}$ enthalten und enthält alle in bez. auf K algebraische Elemente, also ist $\overline{V} = \overline{\Omega}$; also ist $\overline{\Omega} \cong \Omega \ (K)$. Der algebraische Körper über K, der algebraisch abgeschlossen ist, hat also einen bestimmten Typus bez. K.

Wir bekommen so einen und im Wesentlichen auch nur einen algebraischen Körper über K, der algebraisch abgeschlossen ist – einen algebraischen Maximalkörper über K.

Man könnte mit Hilfe des Wohlordnungssatzes die Voraussetzung der Abzählbarkeit auch fallen lassen.

§ 7. Transzendente Erweiterungskörper

Es seien $K \subseteq L$ zwei Körper, $u_1, u_2, \ldots, u_n$ n Elemente aus L; diese heissen algebraisch unabhängig in bezug auf K, wenn keine Relation

$$f(u_1, u_2, \ldots, u_n) = 0$$

(f Polynom mit Koeffizienten aus K) ausser der identischen gilt.[120]

Eine Adjunktion von endlich vielen algebr. unabhängigen Elementen zu K heisst eine rein transzendente Erweiterung von K.

---

[119] In his lecture, van der Waerden confined himself to a countable field, while in MA-I, pp. 199–203, he proceeded in generality.
The last sentence of this Section draws attention to a possibility of a general procedure.

[120] The subject matter of Section 7 is very briefly outlined. In MA-I, Sections 61 and 62 (pp. 203–208) deal with this topic.

Jedem Polynom $f(x_1, x_2, \ldots, x_n)$ mit Koeffizienten aus K ($x_1, x_2, \ldots, x_n$ unbestimmte) ordne ich $f(u_1, u_2, \ldots, u_n)$ zu; diese Zuordnung ist offenbar eineindeutig und isomorph, also

$$K[u_1, \ldots, u_n] \cong K[x_1, \ldots, x_n]$$

und durch Quotientenbildung

$$K(u_1, \ldots, u_n) \cong K(x_1, \ldots, x_n).$$

Wenn nun $u_1, u_2, \ldots, u_n$ algebraisch abhängig in bezug auf K sind, also

$$f(u_1, u_2, \ldots, u_n) = 0,$$

so lässt sich eine von den u_k algebraisch durch die anderen ausdrücken, z.B. u_i ist algebraisch in bezug auf $K(u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n)$.

Wenn w algebraisch von $v_1, \ldots, v_n$ abhängt und $v_1, \ldots, v_n$ algebraisch von $u_1, \ldots, u_m$ abhängen, so hängt nach den vorigen Sätzen auch w von $u_1, u_2, \ldots, u_m$ algebraisch ab.

Auf den beiden analogen Tatsachen haben wir die Theorie der linearen Abhängigkeit, bzw. Unabhängigkeit gegründet; also bestehen mutatos mutandis alle dort bewiesenen Sätze.

1.) Wenn zwei Systeme $u_1, u_2, \ldots, u_n$; $v_1, v_2, \ldots, v_m$ algebraisch äquivalent und jedes von ihnen algebraisch unabhängig ist, so ist $m = n$.

2.) Ein System M (aus einem Erweiterungsköper Ω von K) sei von endlichem Transzendenzgrad n über K, wenn alle Elemente von M algebraisch von n algebraisch unabhängigen abhängen; dieser Transzendenzgrad ist unabhängig von der Wahl der n algebr. unabh. Elemente.

Wenn nun Ω vom endlichen Transzendenzgrad n über K ist, so kann man zuerst n alg. unabh. Elemente von Ω adjungieren (also eine rein transzendente Erweiterung) und dann die übrigen, die schon von den vorigen algebraisch abhängen (also eine algebraische Erweiterung). Ich kann also eine Erweiterung vom endlichen Transzendenzgrad durch eine rein transzendente und eine algebraische ersetzen.

Alles vorangehende liesse sich mit Hilfe des Wohlordnungssatzes auch auf unendlich hohe Transzendenzgrade ausdehnen.

§ 8. Algebraische Funktionen

Sei K ein unendlicher Körper, $x_1, \ldots, x_n$ Unbestimmte.

Algebraische Funktionen von $x_1, \ldots, x_n$ = Elemente einer algebraischen Erweiterung des rationalen Funktionenkörpers $K(x_1, \ldots, x_n)$.[121]

[121] The subject of Section 8 is elaborated in more details in MA-II, pp. 54–58.

Sind $y_1, y_2, \ldots, y_m$ solche algebraische Funktionen, und setzt man für $i = 1, \ldots, m$

$$K_i = K(x_1, \ldots, x_n, y_1, y_2, \ldots, y_i),$$

so ist jedes y_i Nullstelle eines in K_{i-1} irreduziblen Polynoms $h_i(z)$, dessen höchster Koeffizient als $= 1$ angenommen werden darf. Die übrigen Koeffizienten a_{ik} sind Elemente von K_{i-1}, können also rational in den x, ganz rational in $y_1, \ldots, y_{i-1}$ geschrieben werden (§ 2).

Ein reguläres Argumentwertsystem für die Funktionen y ist ein solches Wertsystem $x'_1, x'_2, \ldots, x'_n$ aus K (oder aus einem algebr. Erweiterungskörper von K) dass für diese Werte kein Nenner der Funktionen a_{ik} verschwindet. Solche gibt es in K immer. Ein zugehöriges Funktionswertsystem zu diesen Argumenten wird gefunden, indem man sukzessive in $h_1(z), \ldots, h_m(z)$ die Spezialisierung der x und y zu den x' und $y'_1, \ldots, y'_{i-1}$ vornimmt und y'_i als Nullstelle des spezialisierten Polynoms $h'_i(z)$ in einem algebraischen Erweiterungskörper von K bestimmt.[122]

Ist f ein K-Polynom in $n+m$ Unbestimmten und $f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$, so ist $f(x'_1, \ldots, x'_n, y'_1, \ldots, y'_m) = 0$ für alle regulären x' in K und zugehörigen y', und umgekehrt.

Beweis. Der erste Teil des Satzes ist für Polynome $f(x_1, x_2, \ldots, x_n)$ klar; er sei für Polynome $f(x_1, \ldots, x_n, y_1, \ldots, y_{i-1})$ schon bewiesen. Aus

$$f(x_1, \ldots, x_n, y_1, \ldots, y_i) = 0$$

folgt

$$f(x_1, \ldots, x_n, y_1, \ldots, y_{i-1}, z) \equiv 0 \quad \big(h_i(z)\big)$$

oder

$$f(x_1, \ldots, x_n, y_1, \ldots, y_{i-1}, z) - q_i(z)\, h_i(z) = 0.$$

Nach dem Divisionsalgorithmus lässt sich $q_i(z)$ berechnen, dabei treten nur solche Grössen im Nenner auf, die in h_i schon im Nenner standen, die also bei der regulären Spezialisierung nicht verschwinden. Multipliziert man nun mit dem Produkt dieser Nenner auf, so kann man nach Induktionsvoraussetzung spezialisieren. Dividiert man wieder durch die Nenner durch, so kommt

$$f(x'_1, \ldots, y'_1, \ldots, y'_{i-1}, z) - q'_i(z)\, h'_i(z) = 0,$$

also $$f(x'_1, \ldots, y'_1, \ldots, y'_{i-1}, y'_i) = 0, \qquad \text{q.e.d.}$$

Zweiter Teil: Wäre $f(x'_1, \ldots, y'_1, \ldots, y'_m) = 0$ für alle zugelassenen x' und y' und trotzdem $f(x_1, \ldots, y_1, \ldots, y_m) \neq 0$, so könnte man setzen

$$\frac{1}{f(x_1, \ldots, y_1, \ldots, y_m)} = y_{m+1}$$

[122] For the following theorem see MA-II, pp. 57–58. In these lectures, for polynomials over K the term *K-polynom* is sometimes used.

und könnte $x'_1, \ldots, x'_n$ bestimmen als reguläres Argumentwertsystem der Funktionen $y_1, \ldots, y_m, y_{m+1}$. Aus

$$1 - f(x_1, \ldots, y_1, \ldots, y_m)\, y_{m+1} = 0$$

folgt nach dem ersten Teil des Satzes

$$1 - f(x'_1, \ldots, y'_1, \ldots, y'_m)\, y'_{m+1} = 0 \qquad \text{oder} \qquad 1 = 0.$$

§ 9. Erweiterungen erster und zweiter Art

(separable und inseparable Erweiterungen)

Differentialrechnung für Polynome:[123]

Definition von $f'(x)$: $f(x+h) = f(x) + hf'(x) + (h^2)$.

(1) $(f+g)' = f' + g'$,

(2) $(fg)' = fg' + f'g$,

(3) $\left(\sum a_n x^n\right)' = \sum n a_n x^{n-1}$.

Dann und nur dann hat ein K-Polynom $f(x)$ in einem Erweiterungskörper von K mehrfache Nullstellen, wenn f und f' einen nicht konstanten g. g. T. haben.

Dieser g. g. T. ist rational bestimmbar, also ein K-Polynom.[124]

Folge.[125] Ein in K irreduzibles Polynom $f(x)$ hat keine mehrfache Nullstellen, es sei denn das $f'(x)$ identisch verschwindet. Dieses kommt nur vor bei der Charakteristik p, und zwar wenn $f(x)$ nur Glieder mit x^{kp} enthält. Ein solches Polynom, sowie dessen Nullstellen, heisst inseparabel (Steinitz: von zweiter Art), jedes irred. Polynom mit getrennten Nullstellen separabel. In endlichen Körpern und solchen der Charakt. Null gibt es nur separable Polynome.

Eine endliche Körpererweiterung $K(a_1, a_2, \ldots, a_r) = K_r$ hat in einem passenden Erweiterungskörper soviele Isomorphismen, die ihr in konjugierte Körper überführen, wie der Grad (K_r/K) beträgt, falls jedes a_i separabel in bezug auf $K_{i-1} = K(a_1, \ldots, a_{i-1})$ ist, sonst weniger.

---

[123] See MA-I, pp. 67–69, 113–118.
The basic properties of the derivative of a polynomial, of separable and inseparable polynomials, as well as a relation of the number of isomorphisms of the field $K(\sigma_1, \ldots, \sigma_n)$ over K and the degree of the extension $K(\sigma_1, \ldots, \sigma_n) \supset K$ have already been discussed in Section 5 of the second chapter.

[124] In the previous proposition, instead of the relation $(f, f') \neq 1$, the formulation *f und f' einen nicht konstanten g. g. T. haben* is used.

[125] This paragraph is defective.

Beweis.[126] Jeder Isomorphismus $K_{i-1} \cong \overline{K}_{i-1}$ lässt sich in m_i Weisen fortsetzen in $K_{i-1}(a_i) \cong \overline{K}_{i-1}(\overline{a}_i)$, wenn m_i die Anzahl der verschiedenen Wurzeln der in $\overline{K}_{i-1}$ irred. Gleich. für $\overline{a}_i$ oder der in K_{i-1} irred. Gleich. für a_i ist. Nun ist $m_i = (K_i/K_{i-1})$ oder $m_i < (K_i/K_{i-1})$, je nachdem a_i separabel ist oder nicht. Multiplikation aller m_i gibt die Gesamtzahl der Isomorphismen.

Folgen: Die Eigenschaft der Separabilität aller a_i in bezug auf K_{i-1} ist unabhängig von Wahl und Reihenfolge der Erzeugenden a_i. Sukzessive Adjunktion von separablen Grössen ergibt einen Körper, in dem alle Grössen separabel sind (Separabler Erweiterungskörper).

Ist K_r Galoissch, also mit allen konjugierten Körpern in einem beliebigen Erweiterungskörper identisch (da er zu jeder Grösse auch alle konjugierte enthält, so hat K_r soviele Automorphismen, welche die Elemente von K fest lassen, wie der Grad (K_r/K) beträgt. (Galoissche Gruppe). Diese Automorphismen führen jedes Element in alle konjugierte über.

Ein Element eines separablen Galoisschen Körpers, das mit allen seinen konjugierten identisch ist, liegt im Grundkörper K.

Kapitel III. Idealtheorie in Polynombereichen

Litteratur: S. unter Macaulay und v. d. Waerden.[127]

§ 18. Der Hilbertsche Basissatz

Wenn in einem Ring $\mathcal{R}$ jedes Ideal eine endliche Basis hat, so sagt man: in $\mathcal{R}$ gilt der Basissatz. In Körpern, in euklidischen Ringen gilt der Basissatz.[128]

Wenn in $\mathcal{R}$ der Basissatz gilt, und wenn $\mathcal{R}$ ein Einheitselement besitzt, so gilt in $\mathcal{R}[x]$ der Basissatz.

Beweis. Sei $\mathfrak{a}$ ein Ideal in $\mathcal{R}[x]$, und $\mathfrak{a}_0$ die Gesamtheit der Koeffizienten der höchsten Potenzen von x in allen Polynomen von $\mathfrak{a}$. $\mathfrak{a}_0$ ist ein Ideal, hat also eine endliche Basis $(a_1, \ldots, a_r)$, gehörig zu Polynomen $(f_1, \ldots, f_r)$. Ist n der höchste Grad der Polynome f_i, so kann man modulo $(f_1, \ldots, f_r)$ den Grad eines jeden Polynoms erniedrigen bis auf $n-1$. Sei nun $\mathfrak{a}_1$ das Ideal der Koeffizienten

[126] For more details see MA-I, pp. 116–118.

[127] A reference to these two sources has already been given at the end of Section 1 of the first chapter – see the footnote.

[128] For the whole Section 18 see MA-II, pp. 23–25, where a more detailed proof of the following theorem is provided.

von x^{n-1} in diesen Polynomen vom Grad $\leq n-1$. $\mathfrak{a}_1$ hat eine endliche Basis, gehörig zu den Polynomen $f_{r+1}, \ldots, f_s$; dann kann man modulo $(f_{r+1}, \ldots, f_s)$ jeden Grad auf $n-2$ herabdrücken. U.s.w.

Folgen.

1.) Ist K ein Körper, so gilt in $K[x_1, x_2, \ldots, x_n]$ der Basissatz.

2.) Ist E der Ring der ganzen Zahlen oder überhaupt ein euklidischer Ring, so gilt in $E[x_1, x_2, \ldots, x_n]$ der Basissatz.

§ 19. Algebraische Mannigfaltigkeiten

Raum C_n oder $C_n(K)$ = Gesamtheit aller Wertsysteme $a_1, a_2, \ldots, a_n$ aus einem Körper K. Elemente: Punkte.[129]

Algebraische Mannigfaltigkeit = Gesamtheit der gemeinsamen Nullstellen in C_n von endlichvielen Polynomen $f_1, \ldots, f_r$ aus $K[x_1, \ldots, x_n]$ = Gesamtheit der Nullsteller in C_n des Ideals $(f_1, \ldots, f_r)$. (Nullstelle eines Ideals = gemeinsame Nullstelle aller Polynome des Ideals.)[130]

Unter allen Idealen mit derselben Nullstellen Mannigfaltigkeit M ist ausgezeichnet das zugehörige Ideal von M: die Gesamtheit aller Polynome, die M enthalten (d.i. auf M überall verschwinden).

Die Mannigfaltigkeit einer Idealsumme $(\mathfrak{a}, \mathfrak{b})$ ist der Durchschnitt der Mannigfaltigkeiten von $\mathfrak{a}$ und $\mathfrak{b}$ (klar).

Die Mannigfaltigkeit eines Durchschnitts $\mathfrak{a} \cap \mathfrak{b}$ ist die Vereinigung der Mannigfaltigkeiten $M_\mathfrak{a}$, $M_\mathfrak{b}$ von $\mathfrak{a}$ und $\mathfrak{b}$.

Beweis. Jeder Punkt von $M_\mathfrak{a}$ oder $M_\mathfrak{b}$ ist Nullstelle von $\mathfrak{a} \cap \mathfrak{b}$. Würde ein Punkt a Nullstelle von $\mathfrak{a} \cap \mathfrak{b}$ sein, ohne auf $M_\mathfrak{a}$ oder $M_\mathfrak{b}$ zu liegen, so würde es in $\mathfrak{a}$ ein f und in $\mathfrak{b}$ ein g geben so dass $f(a) \neq 0$, $g(a) \neq 0$, also $f(a)g(a) \neq 0$. Aber $f \cdot g$ gehört zu $\mathfrak{a} \cap \mathfrak{b}$, muss also in a verschwinden.

Eine Mannigfaltigkeit M heisst irreduzibel oder unzerlegbar, wenn sie nicht Vereinigung von zwei echten algebraischen Teilmannigfaltigkeiten M_1, M_2 ist. Andernfalls zerfällt M in M_1 und M_2.

M ist dann und nur dann irreduzibel, wenn das zugehörige Ideal $\mathfrak{a}$ prim ist.

Beweis. Sei M unzerlegbar. Würde nun $f \cdot g$ M enthalten, aber f nicht und g nicht, so setze man M_1 = Gesamtheit der Punkte von M, wo $f = 0$, und M_2 entsprechend für $g = 0$. Dann zerfällt M in M_1 und M_2: Widerspruch.

---

[129] For the whole Section 19 see MA-II, pp. 51–54.

[130] Recall that, by the previous Section, each ideal in $K[x_1, \ldots, x_n]$ has a finite basis.

Sei M zerlegbar in M_1 und M_2. Es gibt auf M Punkte x_1, die nicht auf M_1, und Punkte x_2, die nicht auf M_2 liegen. Also gibt es Polynome f_1, die auf M_1, aber nicht in x_1, und f_2, die auf M_2, aber nicht in x_2 verschwinden. Das Produkt $f_1 f_2$ enthält M. Also ist $\mathfrak{a}$ nicht prim.

(Alle diese Sätze gelten auch noch, wenn dem Polynombereich ein Körper K, dem Raum aber ein Erweiterungskörper K' zugrundegelegt wird, was wir fortan tun werden. Eine Mannigfaltigkeit in $C_n(K')$, die in bezug auf K irreduzibel ist, kann bei Erweiterung von K zerfallen. Der Bequemlichkeit halber denken wir K' algebraisch-abgeschlossen, obzwar meist passende endliche Erweiterungskörper von K genügen.)

Wir suchen: Parameterdarstellungen für irreduzible Mannigfaltigkeiten, d.h. wir suchen jeweils $\xi_1, \ldots, \xi_n$ so als algebraische Funktionen von Parametern t_i zu bestimmen, dass man für reguläre Argumentwerte lauter Punkte von M erhält, und dass sich diese regulären Punkte irgendwie eindeutig zur vollen Mannigfaltigkeit M ergänzen lassen.[131]

2. Heft

Van der Waerden

Allgemeine Idealtheorie

Göttingen, Wintersemestr 1927–28.

§ 20. Nullstellentheorie der Primideale

1.) Ist $\Omega = K(\xi_1, \xi_2, \ldots, \xi_n)$ ein Erweiterungskörper von K, so bilden diejenigen Polynome f aus $\mathcal{R} = K[x_1, x_2, \ldots, x_n]$, für die $f(\xi_1, \xi_2, \ldots, \xi_n) = 0$ ist, ein Primideal.

Beweis. Klar.[132]

2.) Ist $\mathfrak{p}$ dieses Primideal, so ist Ω dem Quotientenkörper des Restklassenringes $\mathcal{R}/\mathfrak{p}$ isomorph, und zwar entsprechen den Restklassen von $x_1, \ldots, x_n$ die Elemente $\xi_1, \ldots, \xi_n$.

Beweis. Durch

$$f(x_1, x_2 \ldots x_n) \to f(\xi_1, \xi_2, \ldots, \xi_n)$$

[131] Both final paragraphs indicate the direction of the subsequent exposition.

[132] For this whole Section see MA-II, pp. 58–64 (§ 89. *Parameterdarstellung algebraischer Mannigfaltigkeiten*, pp. 58–61, § 90. *Die Dimensionszahl*, pp. 61–64), where the exposition is more detailed and largely different. For example, it is assumed from the beginning that $\xi_1, \xi_2, \ldots, \xi_n$ are algebraic functions. In the second edition of MA-II, Section 89 is reworked (§ 93. *Die Nullstellen eines Primideals*, pp. 52–56).

wird $\mathcal{R}$ auf $K[\xi_1, \xi_2, \ldots, \xi_n]$ meromorph abgebildet. Also ist $K[\xi_1, \ldots, \xi_n]$ isomorph dem Restklassenring von $\mathcal{R}$ nach dem Ideal der Polynome f, denen die Null zugeordnet wird; dieses Ideal ist aber $\mathfrak{p}$. Dann müssen aber auch die Quotientenkörper isomorph sein.

3.) Zu jedem Primideal $\mathfrak{p} \neq \mathcal{R}$ gibt es einen Körper $\Omega = K(\xi_1, \ldots, \xi_n)$, so dass $\mathfrak{p}$ besteht aus allen Polynomen f aus $\mathcal{R}$, für die $f(\xi_1, \xi_2, \ldots, \xi_n) = 0$.

Beweis. Den Polynomen f aus $\mathcal{R}$ ordnen wir Elemente φ einer neuen Menge zu, die K umfasst, wobei zweien nach $\mathfrak{p}$ kongruenten Polynomen das gleiche Element entsprechen soll, zweien inkongruenten aber verschiedene, und wobei die Elemente von K sich selbst entsprechen. Die den $x_1, x_2, \ldots, x_n$ ensprechenden Elemente nennen wir $\xi_1, \ldots, \xi_n$. Dann ist jeder Restklasse nach $\mathfrak{p}$ eineindeutig ein neues Element zugeordnet. Wir definieren nun Addition und Multiplikation für die neuen Elemente so wie für die entsprechenden Restklassen; die Zuordnung $f \to \varphi$ wird dann ein Meromorphismus. Dem Polynom $f(x) = \sum a_h x_1^{h_1} \ldots x_n^{h_n}$ wird zugeordnet $\sum a_h \xi_1^{h_1} \ldots \xi_n^{h_n} = f(\xi)$; also ist $f(\xi) = 0$ dann und nur dann, wenn $f \equiv 0\ (\mathfrak{p})$. Der Ring $K[\xi_1, \ldots, \xi_n]$ hat keine Nullteiler. Sein Quotientenkörper leistet das verlangte.

Der nach 3.) zu jedem Primideal $\neq \mathcal{R}$ konstruierbare, nach 1.) auch nur für Primideale existierende, nach 2.) bis auf Isomorphie eindeutig bestimmte Körper $\Omega = K(\xi_1, \ldots, \xi_n)$ dessen Erzeugende ξ_i die Eigenschaft haben; $f(\xi) = 0$ dann und nur dann, wenn $f \equiv 0\ (\mathfrak{p})$, heisst Nullstellenkörper von $\mathfrak{p}$; das Elementsystem $\xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$ allgemeine Nullstelle von $\mathfrak{p}$.

Man kann die ξ_i immer als algebraische Funktionen von v unabhängigen Parametern auffassen (z.B. gibt es unter den ξ_i selbst ein algebraisch-unabhängiges Teilsystem, von dem die übrigen algebraisch abhängen). Für reguläre Argumentwerte erhält man für die Funktionen ξ_i gewisse Funktionswerte $a_1, \ldots, a_n$ in einem algebraischen Erweiterungskörper von K. Da aus $f \equiv 0\ (\mathfrak{p})$ folgt $f(\xi) = 0$, und daraus nach § 17[133] $f(a) = 0$, so sind alle Punkte a Nullstellen von $\mathfrak{p}$, also Punkte der Mannigfaltigkeit von $\mathfrak{p}$ (die demnach für $\mathfrak{p} \neq \mathcal{R}$ niemals leer ist). Verschwindet ein Polynom f in allen Punkten der Mannigfaltigkeit M von $\mathfrak{p}$, so ist insbesondere in den Punkten a: $f(a) = 0$. Daraus folgt nach § 17: $f(\xi) = 0$, mithin $f \equiv 0\ (\mathfrak{p})$. Also ist ein Primideal durch seine Mannigfaltigkeit eindeutig bestimmt. (Geometrische Deutung der Primideale).

Die Funktionen $\xi_1, \ldots, \xi_n$ geben eine Parameterdarstellung von M in dem Sinne, dass erstens die regulären Argumentwerte lauter Punkte von M ergeben, zweitens man alle Punkte von M als Nullstellen des nach 1.) durch die ξ bestimmten Primideals findet.

Der Transzendenzgrad des Systems ξ, oder die Anzahl der notwendigen Parameter in der Parameterdarstellung, heisst die Dimension von $\mathfrak{p}$ oder die Dimension von M.

[133] Apparently, Section 8 of the second chapter is meant.

Sind $\mathfrak{p}$, $\mathfrak{p}'$ Primideale der Dimensionen d, d' und ist $\mathfrak{p}' \equiv 0\ (\mathfrak{p})$, so ist $d \leq d'$ und das Gleichheitszeichen gilt nur dann, wenn $\mathfrak{p} = \mathfrak{p}'$.

(Oder: Sind M, M' irred. Mannigfaltigkeiten der Dimensionen $d, d', \ldots$ u.s.w.)

Beweis. Seien ξ und ξ' allgemeine Nullstellen von $\mathfrak{p}$, $\mathfrak{p}'$. Aus $f \equiv 0\ (\mathfrak{p}')$ folgt $f \equiv 0\ (\mathfrak{p})$ m. a. W. aus $f(\xi') = 0$ folgt $f(\xi) = 0$. Sei nun, eventuell nach Umnennung der Indizes, $\xi_1, \ldots, \xi_d$ ein mit $\xi_1, \ldots, \xi_n$ äquivalentes algebraisch-unabhängiges System. Dann müssen auch $\xi'_1, \ldots, \xi'_d$ algebraisch-unabhängig sein. Daraus folgt schon $d' \geq d$. Ist aber $d' = d$, so sind die übrigen ξ'_i alg.-abhängig von $\xi'_1, \ldots \xi'_d$. Ich behaupte: aus $f(\xi) = 0$ folgt $f(\xi') = 0$. Wäre nämlich $f(\xi') \neq 0$, so könnte man das Körperelement $\frac{1}{f(\xi')}$ in der folgenden speziellen Form schreiben:

$$\frac{1}{f(\xi'_1, \ldots, \xi'_n)} = \frac{g(\xi'_1, \ldots, \xi'_n)}{h(\xi'_1, \ldots, \xi'_d)}.$$

Daraus

$$h(\xi'_1, \ldots, \xi'_d) = f(\xi'_1, \ldots, \xi'_n) g(\xi'_1, \ldots, \xi'_n),$$
$$h(\xi_1, \ldots, \xi_d) = f(\xi_1, \ldots, \xi_n) g(\xi_1, \ldots, \xi_n).$$

Da $\xi_1, \ldots, \xi_d$ unabhängig sind, so ist die linke Seite $\neq 0$, also muss $f(\xi_1, \ldots, \xi_n) \neq 0$ sein, entgegen Voraussetzung. Also in der Tat: aus $f(\xi) = 0$ folgt $f(\xi') = 0$. D.h. $\mathfrak{p} \equiv 0\ (\mathfrak{p}')$, mithin $\mathfrak{p} = \mathfrak{p}'$.

Hat $\mathfrak{p}'$ die Dimension d', so hat jede Nullstelle einen Transzendenzgrad $\leq d'$.

Denn jede Nullstelle bestimmt nach 1.) ein Ideal $\mathfrak{p}$; wendet man auf $\mathfrak{p}$ und $\mathfrak{p}'$ den obigen Satz an, so folgt die Behauptung.

Folge. Ist $\mathfrak{p}'$ nulldimensional, so ist jede Nullstelle algebraisch und allgemein. Wegen der Äquivalenz aller Nullstellenkörper sind ausserdem in jedem Erweiterungskörper von K alle Nullstellen konjugiert.[134]

Ein unzerlegbares nichtkonstantes Polynom p erzeugt ein $(n-1)$ dimensionales Primideal.

Beweis.[135] Wenn fg durch p teilbar ist, so muss es f oder g sein. Also ist (p) prim. Weiter ist, wenn p etwa x_n wirklich enthält, jedes nichtverschwindende

[134] Van der Waerden distinguishes general roots $\{\xi_1, \ldots, \xi_n\}$, whose degree of transcendence is equal to the dimension of the ideal $\mathfrak{p}$; the degree of transcendence of other roots is smaller. For details see MA-II, pp. 60–62.

[135] See *Aufgaben*, MA-II, p. 64:

1. *Ein Hauptideal (p), wo p ein unzerlegbares nichtkonstantes Polynom ist, ist ein $(n-1)$-dimensionales Primideal.*
2. *Umgekehrt: jedes $(n-1)$-dimensionale Primideal ist Hauptideal.*

$f(x_1, \ldots, x_{n-1}) \not\equiv 0\ (p)$, also sind in der allgemeinen Nullstelle $\xi_1, \xi_2, \ldots, \xi_{n-1}$ algebraisch-unabhängig.

§ 21. Geometrische Deutung beliebiger Ideale

Ein Polynom f bestimmt eine $n-1$ dimensionale Mannigfaltigkeit $f = 0$; zählen wir jeden irreduziblen $n-1$ dimensionalen Bestandteil dieser Mannigfaltigkeit so oft, wie der entsprech. Faktor in f vorkommt, so ist f durch diese Mannigfaltigkeiten bis auf Einheiten eindeutig bestimmt.

Ein Ideal, Gesamtheit von Polynomen, können wir demnach auch als Gesamtheit von solchen $(n-1)$-dim. Mannigf. oder „Hyperflächen" geometrisch deuten. Einem Primideal entspricht die Gesamtheit der Hyperflächen, die eine gegebene irred. Mannigf. enthalten. Wir untersuchen nun an einigen typischen Beispielen von Nichtprimidealen, durch welche Eigenschaften die zugehörige Gesamtheit von Hyperflächen charakterisiert ist (K = Körper der kompl. Zahlen; 3 Veränderliche $x\ y\ z$).

Ideal		Eigenschaft der Hyperflächen
(1)	(x^2)	Enthalten die Ebene $x = 0$ zweimal.
(2)	(x^2, xy, y^2)	Haben mindestens einen Doppelpunkt in allen Punkten der Geraden $x = y = 0$.
(3)	$(x^2, xy, y^2, xz, yz, z^2)$	Haben mindestens einen Doppelpunkt im Ursprung.
(4)	(x^2, y)	Berühren die Ebene $y = 0$ längs der Geraden $x = y = 0$.
(5)	$(x^2, xy, y^2, xz - y)$	Berühren die Fläche $xz - y = 0$ längs der Geraden $x = y = 0$.
(6)	(x^2, y^2)	Haben mindestens einen Doppelpunkt in allen Punkten der Geraden $x = y = 0$, während im Fall eines Doppelpunktes der Berührungskegel besteht aus 2 Ebenen, harmonisch zu den Ebenen $x = 0$, $y = 0$.
(7)	(x, yz)	Enthalten die Geraden $x = y = 0$ und $x = z = 0$.
(8)	(x, y^2, yz)	Enthalten die Gerade $x = y = 0$ und berühren die Ebene $x = 0$ im Punkt $x = y = z = 0$.
(9)	(x^2, yz)	Berühren die Ebenen $y = 0$, $z = 0$ nach den Geraden $x = y = 0$, $x = z = 0$.

Alle diese Ideale erscheinen definiert durch gewisse Relationen zwischen den Hyperflächen (Polynomen) des Ideals und gewissen irreduziblen Mannigfaltigkeiten. Abstraktion daraus: eine primäre Eigenschaft eines Polynoms f in bezug auf eine irreduzible Mannigf. M ist eine solche Relation zwischen f und M, die

1.) erhalten bleibt, wenn aus f solche Faktoren weggelassen werden, die M nicht enthalten,

2.) nur dann erfüllt ist, wenn f die Mann. M enthält,

3.) für jede hinreichend hohe Potenz $f = g^h$ erfüllt ist, sobald g die Mannigfaltigkeit M enthält.

Zwei primäre Eigenschaften in bezug auf dasselbe M ergeben zusammen eine primäre Eigenschaft. Demnach können die Ideale 1 – 6 der Tabelle je durch eine, 7 – 9 aber nur durch mehrere primäre Eigenschaften charakterisiert werden.

Ein Ideal, das durch eine primäre Eigenschaft charakterisiert werden kann, heisst primär. Oder: $\mathfrak{q}$ heisst primär, wenn es eine irreduzible Mannigfaltigkeit M gibt, so dass

1.) aus $fg \equiv 0\ (\mathfrak{q})$ folgt $f \equiv 0\ (\mathfrak{q})$, sobald g M nicht enthält,

2.) aus $f \equiv 0\ (\mathfrak{q})$ folgt: f enthält M,

3.) wenn g M enthält, so muss eine Potenz $g^h \equiv 0\ (\mathfrak{q})$ sein.

Ist $\mathfrak{p}$ das zu M gehörige Primideal, so kann man auch sagen:

$\mathfrak{q}$ heisst primär, wenn es ein Primideal $\mathfrak{p}$ gibt, so dass

1.) aus $fg \equiv 0\ (\mathfrak{q})$ und $g \not\equiv 0\ (\mathfrak{p})$ folgt $f \equiv 0\ (\mathfrak{q})$,

2.) aus $f \equiv 0\ (\mathfrak{q})$ folgt $f \equiv 0\ (\mathfrak{p})$,

3.) aus $g \equiv 0\ (\mathfrak{p})$ folgt $g^h \equiv 0\ (\mathfrak{q})$.

In dieser Form gilt die Definition für beliebige Ringe. Im Ring $\mathcal{C}$ der ganzen Zahlen werden die Primärideale von Primidealpotenzen erzeugt.

Die Bedingung, $\mathfrak{p}$ soll prim sein, ist überflüssig, nämlich Folge von 1.), 2.), 3.) so: Aus $fg \equiv 0\ (\mathfrak{p})$, $g \not\equiv 0\ (\mathfrak{p})$, $f \not\equiv 0\ (\mathfrak{p})$ würde nach 3.) folgen $f^h g^h \equiv 0\ (\mathfrak{q})$, daraus nach 1.) $f^h g^{h-1} \equiv 0\ (\mathfrak{q})$ u.s.w. mit fortwährender Erniedrigung beider Exponenten bis $f \equiv 0\ (\mathfrak{q})$; daraus nach 2.) $f \equiv 0\ (\mathfrak{p})$.

$\mathfrak{p}$ ist die Gesamtheit der f, von welchen eine Potenz zu $\mathfrak{q}$ gehört.

Klar nach 2.) und 3.). $\mathfrak{p}$ heisst das zugehörige Primideal von $\mathfrak{q}$.

Wegen der letzten Tatsache lässt sich 1.) auch so formulieren: Aus $fg \equiv 0\ (\mathfrak{q})$ und $f \not\equiv 0\ (\mathfrak{q})$ folgt $g^h \equiv 0\ (\mathfrak{q})$ (E. Noethersche Definition). Wenn umgekehrt $\mathfrak{q}$ diese Eigenschaft hat, und wenn man $\mathfrak{p}$ definiert als die Gesamtheit der f, von denen eine Potenz zu $\mathfrak{q}$ gehört, so ist $\mathfrak{p}$ ein Ideal, denn aus $f^h \equiv 0\ (\mathfrak{q})$ folgt

$(rf)^h \equiv 0\ (\mathfrak{q})$; aus $f^h \equiv 0\ (\mathfrak{q})$, $g^k \equiv 0\ (\mathfrak{q})$ folgt $(f-g)^{h+k-1} \equiv 0\ (\mathfrak{q})$; es folgen die Eigenschaften 1.), 2.), 3.).

Lässt sich jedes Ideal (wie die der Tabelle) durch primäre Eigenschaften geometrisch charakterisieren? Oder: Ist jedes Ideal Durchschnitt von endlich vielen Primäridealen? Ja (Nächstes Kapitel).

Kapitel IV. Allgemeine Idealtheorie

§ 22. Basissatz u. Teilerkettensatz

Die beiden folgenden Sätze sind äquivalent, d.h. wenn in einem Ring $\mathcal{R}$ der eine gilt, so auch der andere.[136]

Basissatz: Jedes Ideal hat eine endliche Basis.

Teilerkettensatz: Eine unendliche Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$, wo jedes $\mathfrak{a}_{i+1}$ ein echter Teiler von $\mathfrak{a}_i$ ist, ist unmöglich.

1.) Der Basissatz sei erfüllt. Ist dann eine Kette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ gegeben, so ist die Vereinigungsmenge aller $\mathfrak{a}_i$ wieder ein Ideal; sei $(f_1, f_2, \ldots, f_r)$ dessen Basis und $\mathfrak{a}_k$ ein Ideal der Kette, welches alle f_i umfasst; dann ist $\mathfrak{a}_{k+1} \subseteq (f_1, f_2, \ldots, f_r) \subseteq \mathfrak{a}_k$, entgegen Voraussetzung.

2.) Der Kettensatz sei erfüllt. Gäbe es dann ein Ideal $\mathfrak{a}$ ohne endliche Basis, so könnte man angeben:

   1.) ein Element f_1 in $\mathfrak{a}$,

   2.) ein Element f_2 in $\mathfrak{a}$, das nicht zu (f_1) gehört,

   3.) ein Element f_3 in $\mathfrak{a}$, das nicht zu (f_1, f_2) gehört u.s.w., was eine unendliche Teilerkette

$$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \ldots$$

   ergeben würde. Dieser Schluss beruht auf dem Auswahlpostulat.

Beispiel von einem Ring, wo der Basissatz nicht gilt: Polynombereich abzählbar unendlich vieler Unbestimmten $x_1, x_2, \ldots$ Das Ideal $(x_1, x_2, \ldots)$ hat keine endliche Basis.

---

[136] The content of Section 22 (see MA-II, pp. 25–27) immediately follows the text presented in Section 18 (see MA-II, pp. 23–25).

Andere Fassungen des Teilerkettensatzes sind:

Der Maximalsatz. In jeder nichtleeren Menge von Idealen gibt es ein umfassendstes Ideal, d.h. ein solches, das von keinem anderen Ideal der Menge umfasst wird.[137] (Würde es zu jedem Ideal der Menge ein noch umfassenderes gäben, so käme man, von einem Ideal $\mathfrak{a}_1$ der Menge ausgehend, auf eine Teilerkette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \dots$) (Auswahlpostulat)

Das Prinzip der Teilerinduktion. Wenn eine Eigenschaft E für jedes Ideal $\mathfrak{a}$ bewiesen werden kann unter der Voraussetzung, dass sie für alle echten Teiler von $\mathfrak{a}$[138] erfüllt ist, so kommt sie jedem Ideal zu (denn sonst $\mathfrak{a}$ müsste es in der Menge der Ideale, die die Eigenschaft E nicht besitzen, ein umfassendstes geben).

Aus Kap. III:[139]

Der Basissatz (also auch der Teilerkettensatz) gilt für Körper, Euklidische Ringe und Polynombereiche aus solchen. Gilt er für $\mathcal{R}$ und hat $\mathcal{R}$ ein Einheitselement, so gilt er auch für $\mathcal{R}[x]$.

Gilt der Teilerkettensatz für $\mathcal{R}$, so auch für jedes meromorphe Abbild $\overline{\mathcal{R}}$ von $\mathcal{R}$ (Restklassenring von $\mathcal{R}$)

Beweis.[140] Jedes Ideal $\overline{\mathfrak{a}}$ von $\overline{\mathcal{R}}$ definiert ein Ideal $\mathfrak{a}$ von $\mathcal{R}$: die Gesamtheit der Elemente, deren Bild zu $\overline{\mathfrak{a}}$ gehört. $\mathfrak{a}$ bestimmt umgekehrt $\overline{\mathfrak{a}}$ eindeutig als die Gesamtheit der Bilder der Elemente von $\mathfrak{a}$. Eine unendliche Kette $\overline{\mathfrak{a}}_1 \subset \overline{\mathfrak{a}}_2 \subset \dots$ würde demnach eine ebensolche $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$ ergeben.

Bemerkung. Ist $\mathfrak{n}$ das Ideal in $\mathcal{R}$, dem das Nullideal in $\overline{\mathcal{R}}$ entspricht, so ist nach § 6.[141] $\overline{\mathcal{R}} \cong \mathcal{R}/\mathfrak{n}$. Die Zuordnung $\mathfrak{a} \to \overline{\mathfrak{a}}$ ist eine eineindeutige zwischen den Idealen $\mathfrak{a}$ von $\mathcal{R}$, die $\mathfrak{n}$ umfassen, und den Idealen $\overline{\mathfrak{a}}$ von $\overline{\mathcal{R}}$. Ein Ideal $\mathfrak{b}$ in $\mathcal{R}$, das nicht $\mathfrak{n}$ umfasst, hat als Bild in $\overline{\mathcal{R}}$ auch ein Ideal $\overline{\mathfrak{b}}$, aber jetzt ist die Zuordnung nicht mehr umkehrbar eindeutig. Man hat allgemein:

$$\overline{(f_1, \dots, f_r)} = (\overline{f_1}, \dots, \overline{f_r})$$

$$\overline{(\mathfrak{a}, \mathfrak{b})} = (\overline{\mathfrak{a}}, \overline{\mathfrak{b}})$$

$$\overline{\mathfrak{a}\mathfrak{b}} = \overline{\mathfrak{a}} \cdot \overline{\mathfrak{b}} \quad \text{(siehe später § 24)}$$

---

[137] In MA-II, p. 27, it is called *maximales Ideal*.

[138] In MA-II, p. 27, at this place is a parenthesis with the following note: *insbesondere auch für das Einheitsideal*.

[139] In the following brief paragraph, results of Section 18 are recalled.

[140] In MA-II, p. 26, the previous proposition has this form: *Wenn der Teilerkettensatz in einem Ring $\mathfrak{o}$ gilt, so gilt er auch in jedem Restklassenbereich $\mathfrak{o}/\mathfrak{a}$.*

[141] See the final paragraph of Section 6 of the first chapter.

§ 23. Der Zerlegungssatz

Ein Ideal $\mathfrak{q}$ heisst nach § 21 primär, wenn aus $ab \equiv 0\ (\mathfrak{q})$ und $a \not\equiv 0\ (\mathfrak{q})$ folgt $b^h \equiv 0\ (\mathfrak{q})$.[142] Zu jedem Primärid. gehört ein Primid., bestehend aus allen Elementen, deren eine Potenz in $\mathfrak{q}$ liegt.

Nun gelte in $\mathcal{R}$ der Teilerkettensatz.[143]

Ist ein Ideal $\mathfrak{m}$ nicht primär, so lässt sich als Durchschnitt von zwei echten Teilern darstellen.

Beweis. Sei $ab \equiv 0\ (\mathfrak{m})$, $a \not\equiv 0\ (\mathfrak{m})$, $b^h \not\equiv 0\ (\mathfrak{m})$ für jedes h. Es sei $\mathfrak{a}_k$ die Menge der Elemente x, für die $x \cdot b^k \equiv 0\ (\mathfrak{m})$. Dann ist $\mathfrak{a}_k$ ein Ideal und $\mathfrak{a}_k \subseteq \mathfrak{a}_{k+1}$. Nach dem Teilerkettensatz muss einmal das Gleichheitszeichen eintreten. Also $\mathfrak{a}_j = \mathfrak{a}_{j+1}$. Unter $\mathcal{R} \cdot b^j$ versteht man die Menge aller Vielfachen $r \cdot b^j$. Die Menge $\mathcal{R}b^j$ ist ein Ideal. Man setze: $\mathfrak{b} = \big(\mathcal{R}b^j, \mathfrak{m}\big)$.

Dann ist $\mathfrak{m} \subset \mathfrak{b}$, denn alle Elemente von $\mathfrak{m}$ sind El. von $\mathfrak{b}$, aber b^{j+1} gehört zu $\mathfrak{b}$ und nicht zu $\mathfrak{m}$. Weiter, $\mathfrak{a} = \mathfrak{a}_1$ gesetzt: $\mathfrak{m} \subset \mathfrak{a}$; denn alle Elemente von $\mathfrak{m}$ gehören zu $\mathfrak{a}$, aber a gehört [144] zu $\mathfrak{a}$ und nicht zu $\mathfrak{m}$. Schliesslich ist $\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}$, denn wenn ein x zu $\mathfrak{m}$ gehört, so auch zu $\mathfrak{a}$ und $\mathfrak{b}$ und wenn x zu $\mathfrak{a}$ und $\mathfrak{b}$ gehört, so ist

$$\begin{aligned} xb &\equiv 0\ (\mathfrak{m}); \quad x \equiv rb^j\ (\mathfrak{m}) \\ r \cdot b^{j+1} &\equiv xb \equiv 0\ (\mathfrak{m}); \\ r &\equiv 0\ (\mathfrak{a}_{j+1}) \equiv 0\ (\mathfrak{a}_j); \\ rb^j &\equiv 0\ (\mathfrak{m}) \\ x &\equiv 0\ (\mathfrak{m}). \end{aligned}$$

Jedes Ideal ist Durchschnitt von endlich vielen Primäridealen:

$$\mathfrak{m} = \big[\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r\big].$$

Beweis. Der Satz sei für alle echten Teiler von $\mathfrak{m}$ schon bewiesen. Ist $\mathfrak{m}$ primär, so ist er klar. Ist $\mathfrak{m}$ nicht primär, so ist

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} = \big[\mathfrak{q}_1, \ldots, \mathfrak{q}_s\big], \qquad \mathfrak{b} = \big[\mathfrak{q}_{s+1}, \ldots, \mathfrak{q}_r\big],$$
$$\mathfrak{m} = \big[\mathfrak{q}_1, \ldots, \mathfrak{q}_s, \ldots, \mathfrak{q}_r\big], \quad \text{w.z.b.w.}$$

---

[142] See MA-II, pp. 31–32.
Quite exactly there should be: ... *daß es ein h gibt so, daß* $b^h \equiv 0\ (\mathfrak{q})$.

[143] Assumption for the entire following text.
For the complete text of Section 23 see MA-II, pp. 35–40.
In MA-II, p. 36, the following two statements have this form:
Jedes Ideal ist Durchschnitt von endlichvielen irreduziblen.
Jedes irreduzible Ideal ist primär.

[144] At this place, in Jarník's records, the word *nicht* is written erroneously.

Ein Durchschnitt von endlich vielen Primäridealen, die zum selben Primideal gehören, ist wieder primär zum selben Primideal $\mathfrak{p}$.

Beweis. Sei $\mathfrak{q} = \big[\mathfrak{q}_1, \dots, \mathfrak{q}_r\big]$.[145]

1.) Aus $ab \equiv 0\ (\mathfrak{q})$ und $a \not\equiv 0\ (\mathfrak{q})$ folgt $ab \equiv 0\ (\mathfrak{q}_i)$ für alle i und $a \not\equiv 0\ (\mathfrak{q}_i)$ für ein i, also $b \equiv 0\ (\mathfrak{p})$,

2.) aus $a \equiv 0\ (\mathfrak{q})$ folgt $a \equiv 0\ (\mathfrak{q}_1) \equiv 0\ (\mathfrak{p})$,

3.) aus $a \equiv 0\ (\mathfrak{p})$ folgt $a^{h_i} \equiv 0\ (\mathfrak{q}_i)$, also, wenn Max $h_i = h$, $a^h \equiv 0\ (\mathfrak{q})$.

Wir denken uns nun aus einer Darstellung $\mathfrak{m} = \big[\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\big]$ alle überflüssigen $\mathfrak{q}_i$ weggelassen; die Darstellung heisst dann unverkürzbar.

Weiter denken wir alle $\mathfrak{q}_i$, die zu je einem $\mathfrak{p}$ gehören, zusammengefasst zu je einem Primärideal. Es folgt:

Jedes Ideal $\mathfrak{m}$ lässt eine unverkürzbare Darstellung als Durchschnitt von Primäridealen, die zu lauter verschiedenen Primidealen gehören, zu.

In dieser Darstellung lassen sich keine Komponenten mehr zu Primäridealen zusammenfassen.[146] Die Darstellung ist nicht eindeutig:[147]

$$(x^2, xy) = \big[(x), (x^2, y + kx)\big]$$

für jedes k.

§ 24. Idealprodukte und -quotienten

Def. $\mathfrak{a} \cdot \mathfrak{b}$ ist die Gesamtheit aller Summen $\sum a_i b_i$, a_i in $\mathfrak{a}$, b_i in $\mathfrak{b}$.[148]

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

(2) $\mathfrak{ab} \cdot \mathfrak{c} = \mathfrak{a} \cdot \mathfrak{bc}$.

(3) $\mathfrak{a} \cdot \sum \mathfrak{b}_i = \sum \mathfrak{ab}_i$ bei endlichen oder unendl. Idealsummen.

(4) $(f_1, \dots, f_r)(g_1, \dots, g_s) = (\dots, f_i g_k, \dots)$ $\big($speziell: $(f) \cdot (g) = (fg)\big)$.

(5) $(f)\mathfrak{a} = f\mathfrak{a}$ $(=$ Gesamtheit aller fa, a in $\mathfrak{a})$.

(6) $\mathfrak{ab} \subseteq \mathfrak{a}$.

(7) $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

(8) $(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{ab}$.

---

[145] This proof is wrong. Correctly there should be: If $ab \equiv 0\ (\mathfrak{q})$ and $a \not\equiv 0\ (\mathfrak{q})$, then for each j is $ab \equiv 0\ (\mathfrak{q}_j)$ and exists i, for which $a \not\equiv 0\ (\mathfrak{q}_i)$. Thus, for some h is $b^h \equiv 0\ (\mathfrak{q}_i)$, and hence $b \equiv 0\ (\mathfrak{p})$. So there are k_j such that $b^{k_j} \equiv 0\ (\mathfrak{q}_j)$, thus $b^k \equiv 0\ (\mathfrak{q})$ for $k = \max k_j$.

[146] Vgl. den letzten Satz in § 24. [The note in Jarník's records.]

[147] In Jarník's records, there is mistakenly written: $(x^2, xy) = \big[(x), (x^2), (y + kx)\big]$. For more details see MA-II, pp. 39–40.

[148] See MA-II, pp. 27–30.

(9) $\mathfrak{a}\mathcal{R} = \mathfrak{a}$, falls $\mathcal{R}$ ein Einheitselem. besitzt.

(10) Ist $\mathfrak{p}$ prim, so folgt aus $\mathfrak{a}\mathfrak{b} \equiv 0\ (\mathfrak{p})$, $\mathfrak{a} \not\equiv 0\ (\mathfrak{p})$ stets $\mathfrak{b} \equiv 0\ (\mathfrak{p})$.

(11) Ist $\mathfrak{q}$ primär und hat das zugehörige Primideal $\mathfrak{p}$ eine endliche Basis, so ist $\mathfrak{p}^h \subseteq \mathfrak{q} \subseteq \mathfrak{p}$.[149]

Beweis. Man setze $\mathfrak{p} = (f_1, \dots, f_r)$, $f_i^{h_i} \equiv 0\ (\mathfrak{q})$,[150]

$$h = h_1 + h_2 + \cdots + h_r + 1 - r$$

und bilde die Basis von $\mathfrak{p}^h$ nach (4). Die kleinste Zahl h in (11) heisst der Exponent von $\mathfrak{q}$.

(12) Ist $\mathfrak{q}$ primär und h der Exponent, so folgt aus $\mathfrak{a}\mathfrak{b} \equiv 0\ (\mathfrak{q})$, $\mathfrak{a} \not\equiv 0\ (\mathfrak{q})$ stets $\mathfrak{b}^h \equiv 0\ (\mathfrak{q})$.[151]

Def. $\mathfrak{a} : \mathfrak{b}$ ist Gesamtheit aller c mit $c\mathfrak{b} \equiv 0\ (\mathfrak{a})$.[152]

(13) $[\dots, \mathfrak{a}, \dots] : \mathfrak{b} = [\dots \mathfrak{a} : \mathfrak{b}, \dots]$.

(14) $\mathfrak{a} : \sum \mathfrak{b} = [\dots, \mathfrak{a} : \mathfrak{b}, \dots]$.

(15) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}$.

(16) $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{b} \subseteq \mathcal{R}$.

(17) $\mathfrak{a} : \mathfrak{b} = \mathcal{R}$, wenn $\mathfrak{a} \supseteq \mathfrak{b}$. Spezialfall: $\mathfrak{a} : \mathfrak{a} = \mathcal{R}$.

(18) Ist $\mathfrak{q}$ primär, $\mathfrak{p}$ das zugehörige Primideal, und ist $\mathfrak{b} \not\equiv 0\ (\mathfrak{p})$, so ist $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$ (und umgekehrt).

(19) Ist $\mathfrak{a} = [\mathfrak{q}_1, \dots, \mathfrak{q}_n]$ und $\mathfrak{b}$ durch kein zugehöriges Primideal teilbar, so ist $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$ (und umgekehrt, wenn die Darstellung unverkzürzbar ist).

(20) Aus $\mathfrak{a} : \mathfrak{b}_1 = \mathfrak{a}$ und $\mathfrak{a} : \mathfrak{b}_2 = \mathfrak{a}$ folgt $\mathfrak{a} : \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a}$ und $\mathfrak{a} : (\mathfrak{b}_1 \cap \mathfrak{b}_2) = \mathfrak{a}$.

(21) Ist $\mathfrak{q}$ primär und $\mathfrak{a} \not\equiv 0\ (\mathfrak{q})$, so ist $\mathfrak{q} : \mathfrak{a}$ primär und zum selben Primideal gehörig.

Beweis.

1.) Aus $fg \equiv 0\ (\mathfrak{q} : \mathfrak{a})$, $g \not\equiv 0\ (\mathfrak{p})$ folgt $fg\,\mathfrak{a} \equiv 0\ (\mathfrak{q})$, $f\mathfrak{a} \equiv 0\ (\mathfrak{q})$, $f \equiv 0\ (\mathfrak{q} : \mathfrak{a})$.

2.) Aus $f \equiv 0\ (\mathfrak{p})$ folgt $f^h \equiv 0\ (\mathfrak{q}) \equiv 0\ (\mathfrak{q} : \mathfrak{a})$.

3.) Aus $f \equiv 0\ (\mathfrak{q} : \mathfrak{a})$ oder $f\mathfrak{a} \equiv 0\ (\mathfrak{q})$ folgt $\big($wegen $\mathfrak{a} \not\equiv 0\ (\mathfrak{q})\big)$ $f \equiv 0\ (\mathfrak{p})$.

---

[149] See MA-II, p. 34.
[150] The following relation in Jarník's records is wrong. It is corrected here.
[151] See MA-II, p. 35.
[152] See MA-II, p. 29.

Umkehrung eines Satzes von § 23:[153]

Wenn ein unverkürzbarer Durchschnitt von endlichvielen Primäridealen wieder primär ist, so gehören alle diese Primärideale zum selben Primideal.

Beweis. Sei $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ primär, $\mathfrak{p}$ das zugehörige Primideal. Setzt man $\mathfrak{b}_1 = [\mathfrak{q}_2, \ldots, \mathfrak{q}_r]$, so ist $\mathfrak{b}_1 \not\equiv 0\ (\mathfrak{a})$, also $\mathfrak{a} : \mathfrak{b}_1$ primär zum selben Primideal $\mathfrak{p}$. Aber nach (13) und (17) ist $\mathfrak{a} : \mathfrak{b}_1 = \mathfrak{q}_1 : \mathfrak{b}_1$ und dieses ist primär zum Primideal $\mathfrak{p}_1$, gehörig zu $\mathfrak{q}_1$. Also $\mathfrak{p}_1 = \mathfrak{p}$, und ebenso $\mathfrak{p}_2 = \mathfrak{p}_3 = \cdots = \mathfrak{p}_r = \mathfrak{p}$.

§ 25. Geometrische Anwendungen des Zerlegungssatzes

Der Zerlegungssatz von § 23. besagt für Polynomideale, dass jedes Ideal durch primäre Bedingungen, welche an irreduzible Mannigfaltigkeiten geknüpft ist, charakterisiert werden kann.[154] Diese nennt man die zugehörigen Mannigfaltigkeiten des Ideals; sie werden in eingebettete (welche in anderen ebensolchen enthalten sind) und isolierte unterschieden. Die isolierten konstituieren zusammen die Nullstellenmannigfaltigkeit des Ideals. Keine ist in der Vereinigung der anderen enthalten.

Also: Jede algebraische Mannigfaltigkeit lässt eine unverkürzbare Darstellung als Vereinigung von irreduziblen zu. Die Darstellung ist, wie man leicht sieht, eindeutig.

Wenn ein Polynom g keine der zugehörigen Mannigfaltigkeiten des Ideals $\mathfrak{a}$ enthält, so folgt in bezug auf die einzelnen Primärkomponenten von $\mathfrak{a}$, also auch in bezug auf $\mathfrak{a}$, aus $fg \equiv 0$ immer $f \equiv 0$ (Vgl. (18): $M : g = M$).[155]

Der Hilbertsche Nullstellensatz: Verschwindet ein Polynom f in allen Nullstellen eines Ideals $\mathfrak{a}$, so ist $f^h \equiv 0\ (\mathfrak{a})$, wo h eine nur von $\mathfrak{a}$ abhängige Zahl ist.

Allgemeiner: Verschwinden $f_1, \ldots, f_r$ in allen Nullstellen von $\mathfrak{a}$, so ist jedes Potenzprodukt von h Faktoren f_i in $\mathfrak{a}$ enthalten.

Beweis. Sei $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ und h der höchste der Exponenten von $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. Das Ideal $(f_1, \ldots, f_r)$ ist $\equiv 0$ nach jedem zugehörigen Primideal $\mathfrak{p}_i$, also ist $(f_1, \ldots, f_r)^h \equiv 0$ nach allen $\mathfrak{q}_i$, also nach $\mathfrak{a}$.

Folge. Ein Ideal ohne Nullstellen ist notwendig das Einheitsideal.

---

[153] See MA-II, pp. 37–38.
[154] See MA-II, pp. 64–67.
[155] For the following theorem see MA-II, pp. 11, 65–66.

§ 26. Die Eindeutigkeitssätze

I. Eindeutigkeit der Komponentenzahl und der zugehörigen Primideale.

Sind zwei unverkürzbare Darstellungen eines Ideals $\mathfrak{a}$ gegeben

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{r'}],$$

wo sowohl die $\mathfrak{q}_i$ als die $\mathfrak{q}'_i$ zu lauterverschiedenen Primidealen $\mathfrak{p}_i$, bzw. $\mathfrak{p}'_i$ gehören, so stimmen links und rechts die Anzahlen der Komponenten und die zugehörigen Primideale überein.

Beweis.[156] Unter den Primidealen $\mathfrak{p}_i$, $\mathfrak{p}'_i$ ist eines, etwa $\mathfrak{p}_1$, ein Umfassendetes. Dieses muss dann auch unter den $\mathfrak{p}'_i$ vorkommen, da sonst

$$\begin{aligned}\mathfrak{a} : \mathfrak{q}_1 &= [\mathfrak{q}_1 : \mathfrak{q}_1, \mathfrak{q}_2 : \mathfrak{q}_1, \ldots, \mathfrak{q}_r : \mathfrak{q}_1] \\ &= [\mathcal{R}, \mathfrak{q}_2, \ldots, \mathfrak{q}_r] = [\underline{\mathfrak{q}_2, \ldots, \mathfrak{q}_r}] \\ &= [\mathfrak{q}'_1 : \mathfrak{q}_1, \mathfrak{q}'_2 : \mathfrak{q}_1, \ldots, \mathfrak{q}'_{r'} : \mathfrak{q}_1,] \\ &= [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{r'}] = \underline{\mathfrak{a}}\end{aligned}$$

wäre, entgegen der Unverkürzbarkeit der Darstellung $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$.

Es sei also $\mathfrak{p}_1 = \mathfrak{p}'_1$; weiter sei $r \leq r'$. Die Beh. folgt für $r = 1$ aus dem letzten Satz von § 24. Sie sei für alle kleineren r schon bewiesen. Man findet durch dieselben Rechnungen wie vorhin.

$$\mathfrak{a} : \mathfrak{q}_1 = [\mathfrak{q}_2, \ldots, \mathfrak{q}_r] = [\mathfrak{q}'_1 : \mathfrak{q}_1, \mathfrak{q}'_2, \ldots, \mathfrak{q}'_{r'}].$$

Nach Induktionsvoraussetzung ist die letzte Darstellung verkürzbar, und da kein $\mathfrak{q}'_i$ weggestrichen werden kann, so muss $\mathfrak{q}'_1 : \mathfrak{q}_1$ weggestrichen werden können:

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_r] = [\mathfrak{q}'_2, \ldots \mathfrak{q}'_{r'}].$$

Hier müssen nach Induktionsvorauss. Anzahlen und zugehörige Primideale übereinstimmen, womit wegen $\mathfrak{p}_1 = \mathfrak{p}'_1$ alles bewiesen ist.

II. Eindeutigkeit der isolierten Komponenten. Ist $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$ eine unverkürzbare Darstellung von $\mathfrak{a}$ durch Primärideale, die zu lauter verschiedenen Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ gehören, so heissen diejenigen $\mathfrak{q}_i$, deren $\mathfrak{p}_i$ kein anderes $\mathfrak{p}_j$ mehr umfasst, isolierte Primärkomponenten. Allgemeiner heisst isolierte Komponente ein solches $\mathfrak{b} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_n]$, wo die $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ keins der $\mathfrak{p}_{n+1}, \ldots, \mathfrak{p}_s$ mehr umfassen.[157]

---

[156] This Section immediately follows Section 23. See MA-II, pp. 40–43. Let us emphasize that $\mathfrak{q}_i$ and $\mathfrak{q}'_j$ are primary ideals.

[157] In paragraph II, some wrongly written indices were corrected.

Jede isolierte Komponente $\mathfrak{b}$ eines gegebenen $\mathfrak{a}$ ist durch die Angabe der zugehörigen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ eindeutig bestimmt.

Beweis. Sei $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_s]$, $\mathfrak{p}_i = \mathfrak{p}'_i$ nach I, und $\mathfrak{b} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_n]$ isoliert, dann folgt wie oben

$$\mathfrak{a} : [\mathfrak{q}_{n+1}, \ldots, \mathfrak{q}_s] = [\mathfrak{q}_1, \ldots, \mathfrak{q}_n] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_n].$$

§ 27. Theorie der teilerfremden Ideale

$\mathcal{R}$ sei von jetzt an ein Ring mit Einheitselement.[158]

Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heissen teilerfremd, wenn sie keinen gemeinsamen Teiler ausser $\mathcal{R}$ haben, oder wenn $(\mathfrak{a}, \mathfrak{b}) = \mathcal{R}$ ist. Notwendig und hinreichend dazu ist die Möglichkeit einer Darstellung $1 = a + b$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$.

Ist $(\mathfrak{a}, \mathfrak{b}) = \mathcal{R}$ und $(\mathfrak{a}, \mathfrak{c}) = \mathcal{R}$, so folgt $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathcal{R}$ und $(\mathfrak{a}, \mathfrak{b} \cap \mathfrak{c}) = \mathcal{R}$.

Beweis. $\mathcal{R} = \mathcal{R}^2 = (\mathfrak{a}, \mathfrak{b})(\mathfrak{a}, \mathfrak{c}) \equiv 0\ (\mathfrak{a}, \mathfrak{b}\mathfrak{c}) \equiv 0\ (\mathfrak{a}, \mathfrak{b} \cap \mathfrak{c}) \equiv 0\ (\mathcal{R})$.

Sind $\mathfrak{q}_1$, $\mathfrak{q}_2$ Primärideale, so folgt aus der Teilerfremdheit der zugehörigen Primideale $\mathfrak{p}_1$, $\mathfrak{p}_2$ auch die von $\mathfrak{q}_1$, $\mathfrak{q}_2$.

Beweis. $1 = p_1 + p_2$, $p_1^h \in \mathfrak{q}_1$, $p_2^k \in \mathfrak{q}_2$, $1 = (p_1 + p_2)^{h+k-1} \equiv 0\ (\mathfrak{q}_1, \mathfrak{q}_2)$.

Ist $(\mathfrak{a}, \mathfrak{b}) = \mathcal{R}$, so $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

(§ 24, (7), (8))

Daraus durch Induktion:

Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ paarweise teilerfremd, so $[\mathfrak{a}_1, \ldots, \mathfrak{a}_r] = \prod_1^r \mathfrak{a}_i$.

Ist $(\mathfrak{a}, \mathfrak{b}) = \mathcal{R}$, so kann man die Kongruenzen $\xi \equiv \alpha\ (\mathfrak{a})$, $\xi \equiv \beta\ (\mathfrak{b})$ gleichzeitig lösen.

Beweis. Sei $1 = a + b$, $a \equiv 0\ (\mathfrak{a})$, $b \equiv 0\ (\mathfrak{b})$, $b \equiv 1\ (\mathfrak{a})$, $a \equiv 1\ (\mathfrak{b})$; es genügt $\xi = a\beta + b\alpha$.

Daraus durch Induktion:

Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ paarweise teilerfremd, so kann man die Kongruenzen

$$\xi \equiv \alpha_i\ (\mathfrak{a}_i)$$

gleichzeitig lösen.

[158] For the following text see MA-II, pp. 43–48.

Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ paarweise teilerfremd und setzt man

$$\mathfrak{b}_i = [\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}, \mathfrak{a}_{i+1}, \ldots, \mathfrak{a}_r],$$
$$\mathfrak{c} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_r],$$

so ist $\mathcal{R} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_r)$ und zwar ist die additive Darstellung aller Elemente von $\mathcal{R}$ durch die von $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_r$ eindeutig modulo $\mathfrak{c}$.

Beweis. Sei $b \in \mathcal{R}$. Wir bestimmen $b_1, \ldots, b_r$ aus

$(*)$ $\quad b_i \equiv b \ (\mathfrak{a}_i), \quad b_i \equiv 0 \ (\mathfrak{b}_i).$

Dann folgt $\sum b_i \equiv b$ modulo allen $\mathfrak{a}_i$, also modulo $\mathfrak{c}$. Ändert man etwa b_1 um ein passendes Element von $\mathfrak{c}$ ab, so wird sogar $\sum b_i = b$. Durch $(*)$ sind die b_i eindeutig bis auf Summanden aus $\mathfrak{c}$ bestimmt.

Ebenso beweist man noch: $\mathfrak{a}_i = (\mathfrak{b}_1, \ldots, \mathfrak{b}_{i-1}, \mathfrak{b}_{i+1}, \ldots, \mathfrak{b}_r)$.

Ist die Darstellung der Elemente von $\mathcal{R}$ als Summen von Elementen von $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_r$ absolut eindentig, so nennt man $\mathcal{R}$ direkte Summe:

$$\mathcal{R} = \mathfrak{b}_1 + \cdots + \mathfrak{b}_r.$$

Das passiert dann und nur dann, wenn $\mathfrak{c} = (0)$ ist.

Man kann das erzwingen durch Übergang zum Restklassenring $\overline{\mathcal{R}} = \mathcal{R}/\mathfrak{c}$. In diesem Restklassenring ist, wenn immer $\overline{M} = M/\mathfrak{c}$ gesetzt wird:

$$(0) = [\overline{\mathfrak{a}}_1, \ldots, \overline{\mathfrak{a}}_r] = [\overline{\mathfrak{a}}_i, \overline{\mathfrak{b}}_i]$$
$$\overline{\mathfrak{b}}_i = [\overline{\mathfrak{a}}_1, \ldots, \overline{\mathfrak{a}}_{i-1}, \overline{\mathfrak{a}}_{i+1}, \ldots, \overline{\mathfrak{a}}_r]$$
$$\overline{\mathcal{R}} = \overline{\mathfrak{b}}_1 + \cdots + \overline{\mathfrak{b}}_r = \overline{\mathfrak{a}}_i + \overline{\mathfrak{b}}_i$$
$$\overline{\mathfrak{a}}_i = \overline{\mathfrak{b}}_1 + \cdots + \overline{\mathfrak{b}}_{i-1} + \overline{\mathfrak{b}}_{i+1} + \cdots + \overline{\mathfrak{b}}_r$$
$$(\overline{\mathfrak{a}}_i, \overline{\mathfrak{a}}_k) = \overline{\mathcal{R}}, \quad [\overline{\mathfrak{b}}_i, \overline{\mathfrak{b}}_k] = (0) \quad (i \neq k)$$

Aus der letzten Relation folgt $\overline{\mathfrak{b}}_i \overline{\mathfrak{b}}_k = (0)$, folglich, wenn man

$$1 = \sum e_i \qquad (e_i \text{ in } \overline{\mathfrak{b}}_i)$$

setzt, $e_i e_k = 0$ und $e_i^2 = e_i$ (Orthogonalitätsrelationen).

Schliesslich gilt noch die Ringisomorphie:

$$\overline{\mathfrak{b}}_i \cong \overline{\mathcal{R}}/\overline{\mathfrak{a}}_i \qquad \text{oder} \qquad \mathfrak{b}_i/\mathfrak{c} \cong \mathcal{R}/\mathfrak{a}_i.$$

$\overline{\mathfrak{b}}_i = \mathfrak{b}_i/\mathfrak{c}$ ist ein Ring mit Einheitselement e_i.

§ 28. Der Vielfachenkettensatz

Wenn in einem Ring jede Kette von echten Idealvielfachen

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \dots$$

nach endlichvielen Schritten abbricht, so sagen wir, im Ring gilt der uneingeschränkte Vielfachenkettensatz.

Beispiele: 1.) endliche Ringe 2.) Körper 3.) Ringe von endlichem Rang in bezug auf einen Körper („hyperkomplexe Systeme“).

Wenn in einem Integritätsbereich (Ring ohne Nullteiler) der uneingeschränkte Vielfachenkettensatz gilt, so ist er ein Körper.

Beweis. Zu lösen ist $ax = b$, $a \neq 0$. Man bilde die Kette $a\mathcal{R}, a^2\mathcal{R}, \dots$ Nach Vielfachenkettensatz $a^m\mathcal{R} = a^{m+1}\mathcal{R}$, also gibt es eine Darstellung für $a^m b$:

$$a^m b = a^{m+1}c, \qquad b = ac \qquad \text{qed.}$$

Wenn in einem Ring jede Kette von echten Idealvielfachen

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \dots,$$

welche alle Teiler eines Ideals $\mathfrak{a} \neq (0)$ sind, nach endlichvielen Schritten[159] abbricht, so sagen wir: Im Ring gilt der eingeschränkte Vielfachenkettensatz. Äquivalent damit ist, dass in jedem Restklassenring $\mathcal{R}/\mathfrak{a}$, $\mathfrak{a} \neq (0)$, der uneingeschänkte Vielfachenkettensatz gelten soll.

Der eingeschr. Vielfachenkettensatz gilt z.B. in euklidischen Ringen, und wie wir später sehen werden, auch in endlichen Erweiterungen davon.

Dagegen nicht in Polynombereichen von mehr als eines Variablen oder im ganzzahligen Polynombereich von mehr als null Variablen.

Sei nun $\mathcal{R}$ ein Ring mit eingeschr. Vielfachenks. Dann hat man:

Der Restklassenring nach einem Primideal $\neq (0)$ is ein Körper.

Daraus: Ein Primideal $\neq (0)$ hat keine echte Teiler ausser $\mathcal{R}$.

Daraus: Zwei Primideale $\neq (0)$ sind teilerfremd.

In $\mathcal{R}$ gelte weiter des Teilerkettensatz. In einer Darstellung

$$\mathfrak{a} = \left[\mathfrak{q}_1, \dots, \mathfrak{q}_r\right] \tag{1}$$

[159] In Jarník's records, the word *Schritten* is mistakenly replaced by word *Idealen*.

eines Ideals $\mathfrak{a}$ nach § 23 sind alle nicht zu $\mathcal{R}$ gehörigen Primärkomponenten isoliert, also eindeutig bestimmt.

$\mathcal{R}$ habe weiter ein Einheitselement. Wegen $\mathcal{R}^h = \mathcal{R}$ gibt es dann keine zu $\mathcal{R}$ gehörigen Primärideale ausser $\mathcal{R}$.

Also: In einer Darstellung (1) sind alle $\mathfrak{q}_i$ eindeutig bestimmt.

Weiter: Je zwei Primärideale, die zu verschiedenen Primidealen $\neq \mathcal{R}$ gehören, sind teilerfremd.

Also können wir statt (1) auch $\mathfrak{a} = \prod \mathfrak{q}_i$ schreiben.[160]

Im nächsten Kapitel werden wir viele Beispiele von Ringen mit eingeschränktem Vielfks. begegnen. Auch wird sich zeigen, welche weitere Voraussetzungen nötig sind, damit die Primärideale Primidealpotenzen werden und somit jedes Ideal Produkt von Primidealpotenzen.

Kapitel V. Ganze algebraische Grössen

Litteratur: E. Noether, Abstrakter Aufbau …, Math. Annalen 96(1926).[161]

§ 29. Moduln in bezug auf einen Ring

Ein Modul war eine additiv geschriebene Abelsche Gruppe M (§ 2).[162] Ist zu einem Modul ein Multiplikatorenring $\mathcal{R}$ gegeben, und eine Multiplikation $r \cdot m = m'$ der Elemente von M mit den Elementen von $\mathcal{R}$ erklärt, mit den Eigenschaften

1.) $r \cdot m$ ist Element von M,
2.) $r(m_1 + m_2) = rm_1 + rm_2$,
3.) $rs \cdot m = r \cdot sm$,
4.) $(r + s)m = rm + sm$,

so nennt man M einen $\mathcal{R}$-Modul. Untermoduln eines $\mathcal{R}$-Moduls sind Untergruppen, die wieder $\mathcal{R}$-Moduln sind; also die mit m auch rm enthalten, wo $r \in \mathcal{R}$, und mit m_1 und m_2 auch $m_1 - m_2$. Man kann mit Kongruenzen nach einem Modul rechnen. $N \equiv 0\ (M)$ heisst: N Untermodul von M (M Teiler, N Vielfaches).

---

[160] In Jarník's records, an incorrectly attached index is corrected.
[161] See the note to the end of Section 1 of the first chapter.
[162] For Section 29 see MA-II, pp. 86–88, see also MA-II, pp. 109–110. Compare with Section 3 of the second chapter. See MA-I, p. 133.

Beispiele: Alle Ringe, die $\mathcal{R}$ umfassen, sind $\mathcal{R}$-Moduln. Die Ideale in $\mathcal{R}$ sind $\mathcal{R}$-Moduln.

Ein $\mathcal{R}$-Modul heisst endlich, wenn er eine endliche Basis $m_1, \ldots, m_s$ besitzt, so dass alle Elemente von M sich als Summen

$$\sum_1^s r_i m_i + \sum_1^s n_i m_i$$

schreiben lassen.

Der Teilerkettensatz für einen $\mathcal{R}$-Modul M besagt die Unmöglichtkeit eines unendlichen Kette von Untermoduln

$$M_1 \subset M_2 \subset \ldots$$

Ist insbesondere $M = \mathcal{R}$, so hat man den Teilerkettensatz für Ideale.

Wie früher ist der Teilerkettensatzt äquivalent mit dem Basissatz: Jeder Untermodul von M (und insbesondere M selbst) ist endlich.[163]

Gilt in $\mathcal{R}$ der Teilerkettensatz für Ideale, und ist M ein endlicher $\mathcal{R}$-Modul, so gilt auch für die Moduln in M der Teilerkettensatz (somit ist auch jeder Untermodul ein endlicher). Gilt für die Ideale in $\mathcal{R}$ der eingeschränkte Vielfachenkettensatz, so auch für die Moduln in M.

Beweis. Der Einfachheit halber setzen wir in $\mathcal{R}$ ein Einheitselement voraus, das auch bei Multiplikation mit Elementen von M als Einheitselement fungiert. Jedes Element von M hat dann die Gestalt

$$\sum_{i=1}^n r_i m_i.$$

Die „Länge“ einer solchen Summe sei das grösste i mit $r_i \neq 0$. Zu jedem Modul N[164] in M definieren wir Ideale $\mathfrak{n}_1, \ldots, \mathfrak{n}_n$ so: $\mathfrak{n}_i$ ist das Ideal aller r_i, die vorkommen in den Darstellungen derjenigen Elemente von N, die sich als Summen der Länge $\leq i$ darstellen lassen. Ist nun $N \subset N'$, so ist offenbar $\mathfrak{n}_i \subseteq \mathfrak{n}'_i$. Ich behaupte: für mindestens ein i ist $\mathfrak{n}_i \subset \mathfrak{n}'_i$. Sei nämlich b' ein Element von N', das nicht zu N gehört, und zwar ein solches von kürzester Länge i:

$$b' = r'_1 m_1 + \cdots + r'_i m_i.$$

[163] See MA-II, p. 87, where this equivalence is proved.
In the following text, at several places a more precise term *Untermodul* instead *Modul* should be used.

[164] We added the symbol N, which does not appear in Jarník's records.
Again, more precisely, the term *Untermodul* should be used.

Dann gehört r_i' zu $\mathfrak{n}_i'$, aber nicht zu $\mathfrak{n}_i$, denn sonst würde ein

$$b = r_1 m_1 + \cdots + r_{i-1} m_{i-1} + r_i' m_i$$

von N mit demselben r_i' existieren und $b' - b$ wäre ein Element von N', nicht von N, und von kürzerer Länge als b', was nicht geht. Ist also eine Kette $N \subset N' \subset N'' \subset \dots$ gegeben, so hat man für jedes i eine Kette $\mathfrak{n}_i \subseteq \mathfrak{n}_i' \subseteq \dots$ und mindestens eine dieser Ketten enthält unendlich viele $\subset$-Zeichen, was mit dem Teilerkettensatz in $\mathcal{R}$ unverträglich ist.

Ebenso schliesst man für Vielfachenketten.

Sei $\mathfrak{c}$ ein Ideal in $\mathcal{R}$. Ein Modul N in M heisst Teiler von $\mathfrak{c}$, wenn $\mathfrak{c}\, M \equiv 0\ (N)$ (d.h. jedes cm Element von N).

Gilt in $\mathcal{R}$ der Vielfachenkettensatz für die Teiler von $\mathfrak{c}$, so gilt in M der Vielfachenkettensatz für die Teiler von $\mathfrak{c}$.

Beweis. Wie vorhin. Alle Ideale $\mathfrak{n}_i$ sind Teiler von $\mathfrak{c}$.

Für $\mathcal{R}$-Moduln in einem Ring $\mathcal{S}$ (der etwa $\mathcal{R}$ umfasst) kann man Produkte, Summen und Quotienten definieren wie früher; es gelten u.A. die Rechenregeln (1) – (5) § 24.

§ 30. Theorie der ganzen Grössen

Eine Grösse a eines Erweiterungsringes von $\mathcal{R}$ heisst ganz oder ganz algebraisch in bezug auf $\mathcal{R}$, wenn eine Gleichung[165]

$$a^h = \sum_0^{h-1} r_i a^i + \sum_1^{h-1} n_i a^i \qquad \text{oder} \qquad a^h \equiv 0 \quad (a^{h-1}, \dots, a, \mathcal{R})$$

besteht, oder wenn der $\mathcal{R}$-Modul $(\mathcal{R}, a, a^2, a^3, \dots)$ eine endliche Basis besitzt.

Wir nehmen fortan an, $\mathcal{R}$ habe ein Einheitselement und lassen $\sum n_i a^i$ weg.

Kriterium.[166] Eine Grösse a ist ganz, wenn Grössen $g_1, \dots, g_n$ existieren, so dass

$$a = \sum r_i g_i \qquad (r_i \in \mathcal{R}),$$

$$a g_i = \sum r_{ik} g_k \quad (r_{ik} \in \mathcal{R}).$$

[165] See MA-II, pp. 88–97, where the exposition is slightly different. If the ring $\mathcal{R}$ does not have an identity, it is $r_0 a^0 = r_0$.

[166] In MA-II, this criterion is missing.

Beweis. Elimination der g_i ergibt:

$$\begin{vmatrix} a & r_1 & \dots & r_n \\ 0 & r_{11}-a & \dots & r_{1n} \\ & & \dots & \\ 0 & r_{n1} & \dots & r_{nn}-a \end{vmatrix} = 0.$$

Folgen:

1.) Summe und Produkt zweier ganzen Grössen b, c sind wieder ganz.

Beweis. Sei $b^h \equiv 0\ (\mathcal{R}, b_i, \dots, b^{h-1})$ und $c^k \equiv 0\ (\mathcal{R}, c, \dots, c^{k-1})$. Man wähle für $g_1, \dots, g_n$ alle Produkte $b^i c^j \ \ (i < h,\ j < k)$, und $a = b + c$, bzw. $a = b \cdot c$. Dann ist das Kriterium erfüllt.

2.) Eine Wurzel einer Gleichung

$$a^h + b_1 a^{h-1} + \cdots + b_h = 0$$

ist ganz, wenn die Koeffizienten $b_1, b_2, \dots, b_h$ es sind.

Beweis. Sei $b_i^{k_i} \equiv 0\ (\mathcal{R}, b_i, \dots, b_i^{k_i-1})$. Man nehme für $g_1, \dots, g_n$ alle Potenzprodukte $a^i b_1^{j_1} \dots b_h^{j_h} \ \ (i < h,\ j_1 < k_1,\ \dots,\ j_h < k_h)$. Dann ist das Kriterium erfüllt.

Daraus: Sind alle Elemente von $\mathcal{S}$ ganz in bezug auf $\mathcal{R}$, und a in bezug auf $\mathcal{S}$, so auch a in bezug auf $\mathcal{R}$.

Ein Integritätsbereich $\mathcal{R}$ heisst ganz-abgeschlossen in Quotientenkörper P, wenn jede Grösse aus P, die ganz in bezug auf $\mathcal{R}$ ist, in $\mathcal{R}$ liegt.[167]

Gilt in $\mathcal{R}$ die eindeutige Faktorzerlegung, so ist $\mathcal{R}$ ganz-abgeschlossen.

Beweis. Sei $a^h + r_1 a^{h-1} + \cdots + r_h = 0$. Wäre $a = \frac{r}{s}$ (unverkürzbar), so

$$r^h + r_1 s r^{h-1} + \cdots + r_h s^h = 0,$$

$$r^h \equiv 0\ (s),$$

also haben r und s doch einen Faktor gemein, oder s ist Einheit, also a in $\mathcal{R}$.

Sei nun $\mathcal{R}$ ein Integritätsbereich mit folgenden Eigenschaften:

I. Teilerkettensatz.

II. Ganz-abgeschlossen im Quotientenkörper P.

[167] See MA-II, p. 90, where a more general definition is given: *Ein Ring* $\mathfrak{S}$ *heißt ganz-abgeschlossen in einem Oberring* $\mathfrak{T}$*, wenn jede in bezug auf* $\mathfrak{S}$ *ganze Größe von* $\mathfrak{T}$ *zu* $\mathfrak{S}$ *gehört.*

Etwa: Polynombereich von n Variablen; oder der Ring der ganzen Zahlen.

Da das Einheitselement des Quotientenkörpers der Gleichung $e^2 = e$ genügt, so ist es ganz, liegt somit in $\mathcal{R}$.

Sei $\Sigma = P(s)$ ein einfacher algebraischer separabler Erweiterungskörper von $\mathcal{R}$; $\mathcal{S}$ ein Ring in Σ, der $\mathcal{R}$ umfasst.

Behauptungen:

1.) Wenn $\mathcal{S}$ endlicher $\mathcal{R}$-Modul ist, so sind alle Elemente von $\mathcal{S}$ ganz.

2.) Sind alle Elemente von $\mathcal{S}$ ganz, so ist $\mathcal{S}$ endlicher $\mathcal{R}$-Modul.

Beweis. 1.) Sei $\mathcal{S} = (g_1, g_2, \ldots, g_r)$, a ein Element aus $\mathcal{S}$. Nach dem Kriterium ist a ganz.

2.) Das erzeugende Element s kann ganz gewählt werden. Dann sind auch die zu s konjugierten Grössen $s_1, \ldots, s_n$ in einem Galoisschen Erweiterungskörper von Σ ganz. Die symmetrische Funktion

$$D = \left| 1\, s_i\, \ldots\, s_i^{n-1} \right|^2 = \prod_{i<k} (s_i - s_k)^2$$

ist rational, d.h. Element von P. Ist nun u irgend eine ganze Grösse von $\mathcal{S}$, so ist $u = \sum_0^{n-1} a_j s^j$ mit rationalen a_i.

Die konjugierten zu u sind

$$u_i = \sum_0^{n-1} a_j s_i^j.$$

Auflösung der a_j ergibt $a_j D =$ ganze Grösse b_j. b_j ist zugleich rational also in $\mathcal{R}$.

$$u = \sum_0^{n-1} b_j \frac{s^j}{D}.$$

Also ist der Ring $\mathcal{S}$, der aus lauter ganzen Grössen u besteht, enthalten im $\mathcal{R}$-Modul $(\frac{1}{D}, \frac{s}{D}, \ldots, \frac{s^{n-1}}{D})$.

Da dieser Modul endlich ist, so ist es $\mathcal{S}$ auch (vgl. § 29; in $\mathcal{R}$ gilt der Teilerkettensatz). Durch sukzessive Adjunktionen ist dies auf alle endlichen separ. Erweiterungen auszudehnen.

Für die Ausdehnung dieses Satzes auf inseparable Erweiterungen siehe Artin – v. d. Waerden, Gött. Nachr. 1926.[168]

[168] E. Artin, B.L. van der Waerden: *Die Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Körpererweiterungen*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen 1926, pp. 23–27.

Erweiterungsringe von $\mathcal{R}$ mit endlicher $\mathcal{R}$-Modulbasis bezeichnet man als $\mathcal{R}$-Ordnungen; der Satz lässt sich auch so fassen: Der Ring aller ganzen Grössen in Σ ist maximale $\mathcal{R}$-Ordnung (umfasst jede andere $\mathcal{R}$-Ordnung) in Σ. Man nennt sie die Hauptordnung.

Beispiele: Ganze algebr. Zahlen, ganze algebr. Funktionen von n Variablen in einem festen Körper.

Aus den Sätzen des § 29 folgt:

In jeder $\mathcal{R}$-Ordnung $\mathcal{S}$ gilt der Teilerkettensatz für $\mathcal{R}$-Moduln, also um so mehr für $\mathcal{S}$-Moduln, d.h. Ideale.

Gilt in $\mathcal{R}$ der Vielfachenkettensatz für die Teiler eines Ideals $\mathfrak{c}$, so gilt auch in $\mathcal{S}$ für die Modulteiler, also um so mehr für die Idealteiler von $\mathfrak{c}$, der Vielfachenkettensatz.

Jedes Ideal $\mathfrak{a} \neq 0$ in $\mathcal{S}$ enthält eine Zahl $a \neq 0$, deren Norm

$$Na \equiv 0 \ (a) \equiv 0 \ (\mathfrak{a})$$

ist. (Na) ist ein Ideal in $\mathcal{R}$, von dem $\mathfrak{a}$ Teiler ist. Jedes Ideal in $\mathcal{S}$ ist also Teiler eines Ideals in $\mathcal{R}$. Gilt also für die Teiler eines jeden Ideals $\neq 0$ in $\mathcal{R}$ der Vielfachenkettensatz, so gilt dasselbe für $\mathcal{S}$.

Die auf Teilerkettensatz und Einheitselement mit oder ohne eingeschr. Vielfachenkettensatz basierte Idealtheorie überträgt sich demnach auf jede $\mathcal{R}$-Ordnung $\mathcal{S}$. Für die Hauptordnung gilt darüber hinaus noch die Idealtheorie des nächsten §, da die Hauptordnung ganz-abgeschlossen im Quotientenkörper P ist.

Ist $\mathcal{R}$ der Ring der ganzen Zahlen, $\Sigma = P(\sqrt{-3})$, so ist $(1, \sqrt{-3})$ eine $\mathcal{R}$-Ordnung, und $\left(1, \frac{1+\sqrt{-3}}{2}\right)$ die Hauptordnung.

§ 31. Idealtheorie der ganz-abgeschlossenen Ringe

Sei $\mathcal{R}$ ein Integritätsbereich mit folgenden Eigenschaften:[169]

I. Teilerkettensatz.

II. Eingeschr. Vielfachenkettensatz.[170]

III. Ganz-abgeschlossen im Quotientenkörper.

Auf Grund von I, II ist jedes Ideal Produkt von teilerfremden Primäridealen.[171]

[169] The material in MA-II, pp. 97–103, is presented in a quite different way.

[170] In MA-II, p. 97, at this place it is required: *Alle vom Nullideal verschiedenen Primideale sind teilerlos.* This is a corollary of the condition II. – see Section 28.

[171] See Section 23 and Section 28.

Wir wollen zeigen, dass jedes Primärideal Primidealpotenz ist. Hilfsmittel: $\mathcal{R}$-Moduln im Quotientenkörper. (Man nennt diese, wenn sie endlich sind, auch „gebrochene Ideale“.) Alle Quotienten sind Modulquotienten in Σ.

‖ Ist $\mathfrak{p} \neq (0), (1)$ ein Primideal, so gibt es in $\mathcal{R} : \mathfrak{p}$ ein nichtganzes Element.

Beweis.[172] Sei $p \neq 0$ Element von $\mathfrak{p}$, und $(p) = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$. Ein $\mathfrak{q}_i$ muss $\mathfrak{p}$ als zugehöriges Primideal haben, wir nennen es $\mathfrak{q}$:

$$(p) = [\mathfrak{q}, \mathfrak{d}] \quad \text{(wo } \mathfrak{d} \text{ der Durchschnitt der übrigen ist).}$$

$$\mathfrak{p}^h \equiv 0 \ (\mathfrak{q})$$

$$\mathfrak{p}^h \mathfrak{d} \equiv 0 \ (p)$$

Sei h die niedrigste Zahl, für die diese Gleichung gilt, also

$$\mathfrak{p}^{h-1} \mathfrak{d} \not\equiv 0 \ (p).$$

Sei b ein Element von $\mathfrak{p}^{h-1}\mathfrak{d}$, nicht durch p teilbar. Dann

$$b\mathfrak{p} \equiv 0 \ (\mathfrak{p}^h \mathfrak{d}) \equiv 0 \ (p),$$

also $\frac{b}{p}$ Element von $\mathcal{R} : \mathfrak{p}$, aber nicht ganz.

Ist $\mathfrak{p} \neq (0), (1)$ ein Primideal, so ist $\mathfrak{p} \cdot (\mathcal{R} : \mathfrak{p}) = \mathcal{R}$ (schreibe daher $\mathcal{R} : \mathfrak{p} = \mathfrak{p}^{-1}$).[173]

Beweis. $\mathfrak{p} \cdot (\mathcal{R} : \mathfrak{p})$ ist ein ganzes Ideal, Teiler von $\mathfrak{p}$ (da es $\mathfrak{p} \cdot 1$ umfasst). Also entweder $\mathfrak{p} \cdot (\mathcal{R} : \mathfrak{p}) = \mathcal{R}$ oder $\mathfrak{p} \cdot (\mathcal{R} : \mathfrak{p}) = \mathfrak{p}$. Im letzten Fall sei a ein Element von $\mathcal{R} : \mathfrak{p}$ und

$$\mathfrak{p} = (p_1, \ldots, p_r).$$

$$a p_i = \sum c_{ik} p_k \quad (c_{ik} \text{ ganz})$$

Elimination der p_i ergibt

$$\begin{vmatrix} c_{11} - a & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} - a & \ldots & c_{2n} \\ & & \ldots & \\ c_{n1} & c_{n2} & \ldots & c_{nn} - a \end{vmatrix} = 0,$$

also a ganz. Also alle Elemente von $\mathcal{R} : \mathfrak{p}$ ganz, entgegen dem vorigen Satz.

‖ Jedes Primärideal ist Primidealpotenz.

---

[172] In MA-II, p. 99, the previous proposition is labeled as *Hilfssatz 3*: *Ist* $\mathfrak{p} \neq \mathfrak{o}$, *so liegt in* $\mathfrak{p}^{-1}$ *ein nichtganzes Element.*

[173] See MA-II, p. 99, *Satz 1*: *Ist* $\mathfrak{p} \neq \mathfrak{o}$, *so ist* $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{o}$.

Beweis. Sei $\mathfrak{q}$ primär, h der Exponent. Für Exponenten $< h$ sei der Satz schon bewiesen.

$$\mathfrak{p}^h \equiv 0\ (\mathfrak{q}) \equiv 0\ (\mathfrak{p})$$

Multiplikation mit $\mathfrak{p}^{-1}$:

$$\mathfrak{p}^{h-1} \equiv 0\ (\mathfrak{p}^{-1}\mathfrak{q}) \equiv 0\ (\mathcal{R}).$$

$\mathfrak{p}^{-1}\mathfrak{q}$ ist primär, da es keinen anderen Primteiler als $\mathfrak{p}$ haben kann. Also nach Induktionsvoraussetzung $\mathfrak{p}^{-1}\mathfrak{q} = \mathfrak{p}^k$, $\mathfrak{q} = \mathfrak{p}^{k+1}$, q.e.d.[174]

Also ist jedes Ideal Produkt von Primidealpotenzen.

Insbesondere gültig: für Hauptordnungen in Zahlkörpern und Funktionenkörpern einer Variablen.[175]

Die Darstellung ist eindeutig: aus $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r = \mathfrak{p}'_1\mathfrak{p}'_2\ldots\mathfrak{p}'_{r'}$ folgt $r = r'$, $\mathfrak{p}_i = \mathfrak{p}'_i$ bei passender Anordnung.

Beweis. Jedes $\mathfrak{p}_1$ links muss auch rechts vorkommen (denn wenn ein Produkt durch $\mathfrak{p}_1$ teilbar ist, so ein Faktor). Multiplikation mit $\mathfrak{p}_1^{-1}$ führt den Fall r auf $r-1$ zurück.

Umkehrsatz: Gilt in einem Integritätsbereich $\mathcal{R}$ mit Einheit die eindeutige Zerlegung in Primideale so ist der Ring ganz-abgeschlossen im Quotientenkörper.

Beweis.[176] Aus $\mathfrak{ab} = \mathfrak{ac}$ folgt $\mathfrak{b} = \mathfrak{c}$. Das gilt auch, wenn $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ nicht Ideale, sondern endliche $\mathcal{R}$-Moduln in P sind, da diese sich durch Multiplikation mit einer Zahl ganz machen lassen.

Sei nun a ganz in bezug auf $\mathcal{R}$ und Element des Quotientenkörpers P:

$$a^n \equiv 0\ (1, a, \ldots, a^{n-1})$$

Der Modul $A = (1, a, a^2, \ldots, a^{n-1})$ ist endlich und hat die Eigenschaft $\mathfrak{a}^2 = \mathfrak{a}$ oder $\mathfrak{a}^2 = \mathfrak{a}\mathcal{R}$. Daraus $\mathfrak{a} = \mathcal{R}$, mithin a in $\mathcal{R}$.

(Es ist demnach z.B. in Zahlkörpern notwendig, zur Hauptordnung überzugehen, um die Primidealzerlegung zu erzwingen: eine andere Ordnung tut es nicht.)

---

[174] For the following statement, see MA-II, p. 99, *Satz 2*: *Jedes Ideal* $\mathfrak{a}$ *ist Produkt von Primidealen.*

[175] For the following two statements, see MA-II, pp. 100–101.

[176] Correctly, in the spirit of the lecture, the term *Einheitselement* should be used in the previous proposition.

Ringe	Typische Beispiele	Idealtheorie
Ringe mit Teilerkettensatz	Polynombereich von n Var. ü endl. Erweiterungen davon	Jedes Ideal Durchschn. v. Primärid. Zugehörige Primideale eindeutig Isolierte Komponenten eindeutig
Ringe m. Teilerkettens. ü beschr. Vielfachenkettens.	Polynombereich einer Var. Ring der ganzen, der geraden Zahlen ü deren endl. Erweit. („Ordnungen“)	Jedes Ideal Durchschn. v. teilerfremden Primäridealen
ohne Einheitselement … Ring der geraden Zahlen		Alle Primärkomponenten, die nicht zu 0 gehören, eindeutig bestimmt
mit Einheitselement … Ring der ganzen Zahlen		Alle Primärkomponenten, eindeutig Durchschnitt = Produkt
ganz-abgeschl. in Quotientenkörper „s-Axiom-Ring“	Hauptordnung eines Zahlkörpers od. Funktionenkörpers einer Var.	Jedes Ideal Produkt v. Primid. Eindeutig
Euklidische Ringe … (Jedes Ideal Hauptideal)	Ring der ganzen Zahlen Polynombereich einer Var. Gaußsche Zahlen $a + bi$	Jede Zahl Produkt v. Primzahlen Bis auf Einheiten eindeutig
Körper		Nur die Ideale (0) und (1).