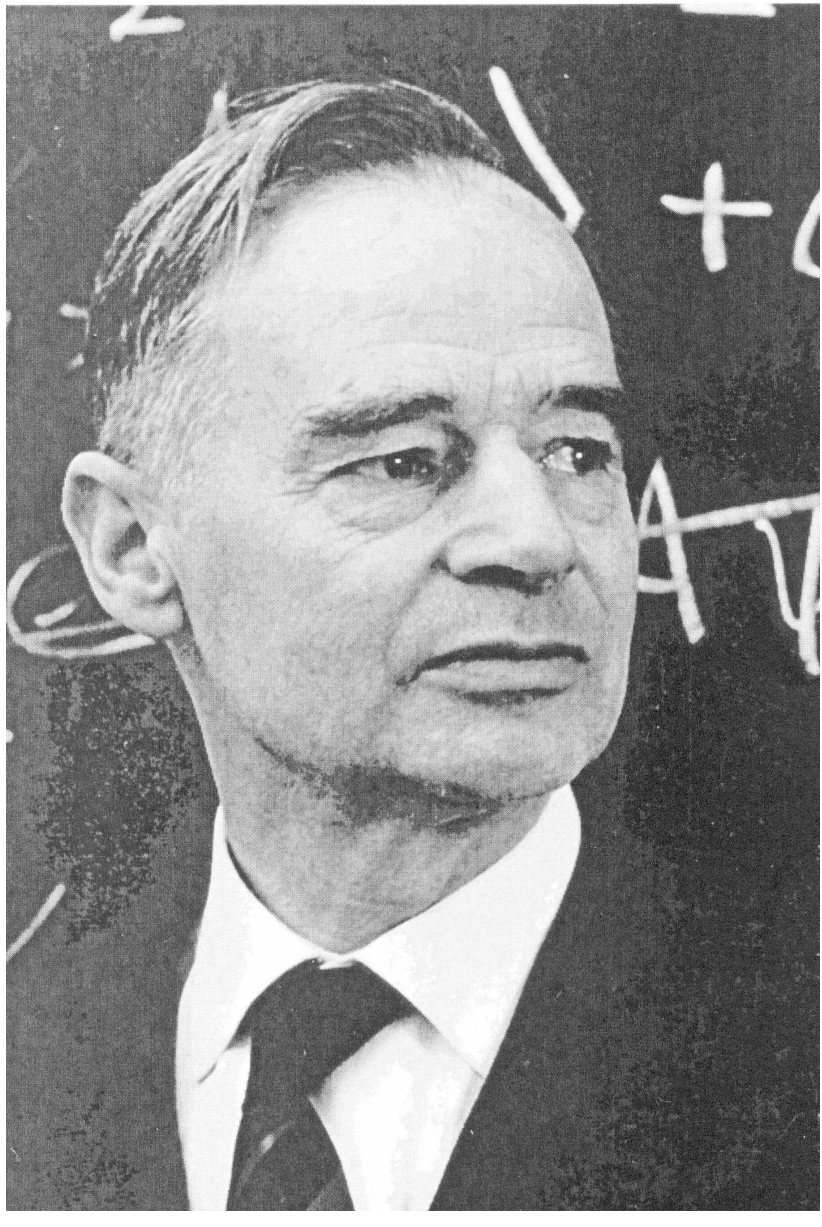
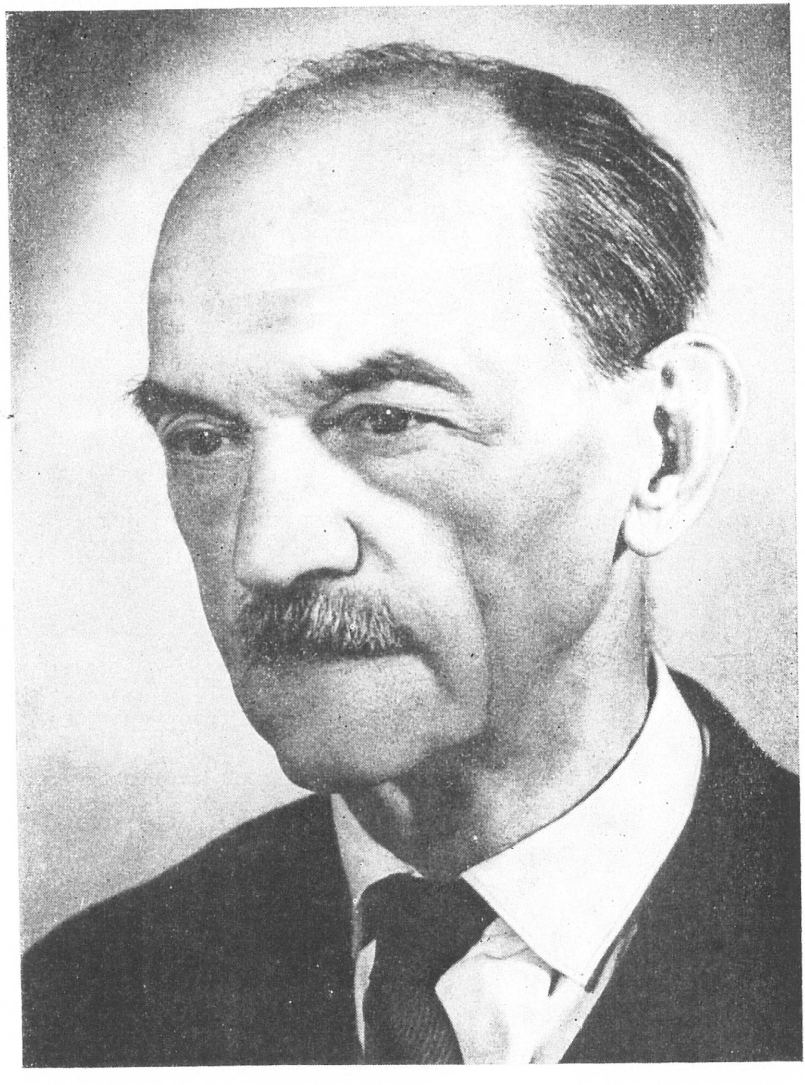
Jarník's Notes of the Lecture Course Allgemeine Idealtheorie by B. L. van der Waerden (Göttingen 1927/1928)

[Illustrations]





V. Jarník

MATHEMATISCHE ANNALEN

BEGRÜNDET 1868 DURCH

ALFRED CLEBSCH UND CARL NEUMANN

FORTGEFÜHRT DURCH

FELIX KLEIN

GEGENWÄRTIG HERAUSGEGEBEN

VON

DAVID HILBERT

IN GÖTTINGEN

UNTER MITWIRKUNG VON

OTTO BLUMENTHAL
IN AACHEN

ERICH HECKE
IN HAMBURG

BARTEL L. VAN DER WAERDEN
IN LEIPZIG

109. BAND

BERLIN
VERLAG VON JULIUS SPRINGER
1934

Über die fundamentalen Identitäten der Invariantentheorie.

Von

B. L. van der Waerden in Amsterdam.

Einleitung.

Die Invarianten eines endlichen oder unendlichen Systems von Linearformen in kogredienten und kontragredienten Variablen x und u' kann man nach dem „ersten Fundamentalsatz der symbolischen Methode" vollständig angeben: sie bauen sich auf aus „Klammerfaktoren" (Determinanten) und „Linearfaktoren" $(a'\,b) = \sum_1^n a'^{(i)} b^{(i)}$. Zwischen diesen bestehen algebraische Identitäten, und es handelt sich im folgenden um die Angabe eines Fundamentalsystems von Identitäten, aus denen sich alle übrigen durch Addition und Multiplikation mit beliebigen Invarianten ableiten lassen.

Um das Problem schärfer zu fassen, bilden wir einen Polynombereich Ω von endlich oder unendlich vielen Unbestimmten, denen später die oben charakterisierten einfachsten Invarianten zugeordnet werden. Diejenigen Polynome aus Ω, die identisch (in den Formenkoeffizienten als Unbestimmte) verschwinden, wenn man für die erstgenannten Unbestimmten diese Invarianten einsetzt, bilden ein Ideal in Ω, und es handelt sich um eine Basis für dieses Ideal [1]). Beschränkt man sich auf endlichviele Unbestimmte, so hat das Ideal nach dem Hilbertschen Basissatz eine endliche Basis; die Anzahl der Elemente dieser Basis ist bei wachsender Anzahl der Unbestimmten zwar nicht beschränkt, aber E. Pascal hat bewiesen [2]),

[1]) Diese Auffassung hat E. Noether vertreten (Die Endlichkeit des Systems der ganzzahligen Invarianten binärer Formen, Gött. Nachr. 1919). Sie gestattet eine präzise und einfache Ausdrucksweise.

[2]) E. Pascal, Memorie d. R. A. d. Lincei (4) 5 (1888). Für das binäre Gebiet siehe Gordan-Kerschensteiner, Vorlesungen über Invariantentheorie II, S. 132; für das ternäre E. Study, Methoden zur Theorie der ternären Formen, Leipzig 1889, S. 75.

MODERNE ALGEBRA

VON

DR. B. L. VAN DER WAERDEN
O. PROFESSOR AN DER UNIVERSITÄT
GRONINGEN

UNTER BENUTZUNG VON VORLESUNGEN
VON
E. ARTIN UND E. NOETHER

ERSTER TEIL

BERLIN
VERLAG VON JULIUS SPRINGER
1930

Springer-Verlag in Berlin W 9. — Verantwortlich für den Anzeigenteil: Albert Meyer, Berlin-Steglitz, Kühlebornweg 5. — Druck von Friedr. Vieweg & Sohn in Braunschweig
Printed in Germany

Pl. 3.

Van der Waerden

Allgemeine Idealtheorie

Göttingen, Wintersem. 1927-28.

4. XI.

§ 1. Einleitung.

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

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

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

$$(1) \qquad N\alpha = |\alpha|^2 = a^2 + 5b^2;$$

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.

Der Begriff des Ideals läßt sich aber auch auf algebraische Funktionen einer Veränderlichen anwenden: es sei $P(x)$ ~~der~~ Körper der rationalen Funktionen von x über P, $P[x]$ der zugehörige ~~Funktionenkörper~~ Polynombereich, $P(x, y_1, y_2, \dots, y_r)$ ist ein Erweiterungskörper, in welchem $y_1, \dots y_r$ algebraische Funktionen sind.

Man definiert ganze algebraische Funktionen und Ideale und findet eine Eindeutigkeit Zerlegbarkeit von Idealen in Primideale. Die Primideale entsprechen dann eineindeutig den Punkten der Riemannschen Fläche.

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

Einen vierten Ausgangspunkt bildete die Theorie der hyperkomplexen Zahlen

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

wo $a_\varkappa$ Zahlen eines reellen Körpers sind. (Frobenius, E. Noether).

Wenn eine Menge M so beschaffen ist, dass mit α, β auch $\alpha \pm \beta, \alpha\beta$ zu M gehören, heisst 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 es 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 Dirichlets Vorlesungen über Zahlentheorie.
Hilbert, Zahlbericht. Landau, Hecke.

2.) Modulsysteme:
F. S. Macaulay, Modular Systems, Cambr. Tracts 19.
V. d. Waerden, Nullstellentheorie..., Math. Ann. 96

3.) Funktionenkörper
Dedekind-Weber, Algebr. Funkt. einer Veränderlichen, Crelle's J. 92.

4.) Allgemeine Theorie:
E. Noether, Idealtheorie in Ringbereichen, Math. Ann. 83
Abstrakter Aufbau ... Math. Ann. 96.

§ 3. Ringe.

Zahlenringe hat zuerst Hilbert betrachtet, abstrakt bei E. Noether, Math. Ann. 83, einfacher bei Hasse, höher Algebra I.

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 ~~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 ~~von~~ $-b+a = a-b$ von $b+x=a$. Dann ist weiter

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

$(nm)\cdot a = n\cdot(ma)$ (m, n ganze rationale Zahlen); das ist eine direkte Folge unserer Gruppenergebnisse.

Im Produkt darf man ausklammern und beliebig vertauschen, endlich Potenzen mit positiven Exponenten definieren (denn dies folgte in § 2 nur aus den assoziativen und kommutativen Gesetz): $a^1 = a$, $a^{n+1} = a^n \cdot a$;

$a^n a^m = a^{n+m}$, $(a^n)^m = a^{nm}$,

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

Auch für Differenzen gilt freilich das distributive Gesetz

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

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

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

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

auch so:

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

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

Man kann es so aussprechen:
"Maximale" (im mengentheoretischen Sinn)
"Ideale in $\mathfrak{O}$ (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 Einheits-
element, wo jedes Ideal Hauptideal ist.

Z.B. 1.) Ring der ganzen rationalen
Zahlen

2.) Polynombereich $\Sigma'[x]$, wo
Σ Körper.

3.) Der Ring der ganzen Gaussschen
Zahlen $a+bi$ (a,b ganz rational)

Beweis zu 3.) Wenn $\alpha = a+bi$, $\gamma = c+di$
$\neq 0$ (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: $\frac{\alpha}{\gamma} = g+ih$, g, h rational.
Ich finde die zu g, h nächsten ganzen rat.
Zahlen e, f:

$$\frac{\alpha}{\gamma} = e+if+r+is, \text{ wo } |r| \leqq \tfrac{1}{2}, |s| \leqq \tfrac{1}{2}$$
$$= \varepsilon + r+is \quad (\varepsilon \text{ ganze G. Zahl})$$
$$\alpha = \varepsilon\gamma + \varrho, \text{ wo}$$
$$N(\varrho) = N\left(\gamma\cdot(r+is)\right) \leqq N(\gamma)\cdot\tfrac{1}{2} < N(\gamma)$$

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

Weil der Restklassen~~körper~~ring bei Primidealen keine Nullteiler hat, so folgt: falls p Primzahl,

$$ab \equiv 0 (p)\,,$$ so ist entweder

$a \equiv 0(p)$ oder $b \equiv 0(p)$.

28/XI

Jedem Element n eines euklidischen Ringes entspricht ein Ideal, nämlich das Ideal (n); und zwar entsprechen denjenigen Zahlen, die sich nur um Einheiten 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, und zusammengesetzten Zahlen entsprechen keine Primideale, denn wenn $n = ac$, (a, c keine Einheiten) so ist

Wenn $\sum$ ein Körper, so sind z. B. die Primzahlen von $\sum[x]$ 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.

Satz. Jedes Element eines Euklidischen Ringes lässt sich eindeutig in die Form bringen $a = \underset{\text{Einheit}}{\varepsilon}\, p_1 p_2 \cdots p_r$,

wo $p_1, p_2 \cdots p_r$ keine Einheiten und Primzahlen sind. Das soll bedeuten: in jeder analogen Zerlegung $a = \varepsilon' p_1' p_2' \cdots p_{r'}'$ ist ~~r~~ $r' = r$ und bis auf Anordnung

$p_i' = p_i \xi_i$, ξ_i Einheit.

Beweis: 1.) Eindeutigkeit beweist man so:

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 $p_1' \cdots p_{r'}'$, also mindestens einen Faktor; z. B. p_1'; weil p_1' Primzahl, so ist $p_1' = \xi p_1$, ξ Einheit. Durch Kürzen:

$\varepsilon p_2 p_3 \cdots p_r = \varepsilon' \xi p_2' \cdots p_{r'}'$; und nun ist für diese Zahlen ($r-1$ statt r) schon alles bewiesen.

Wir haben nebenbei noch bewiesen: Wenn $f(x)$ in $S[x]$ 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.

Folgerung: Wenn Σ ein Körper, so folgt durch Induktion sofort aus unserem Satz:

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

2/XII

Kapitel II.
Körpertheorie.

§1. Primkörper.

Ein Körper, der keinen echten Unterkörper enthält, heißt Primkörper.

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 $\mathfrak{p}$, denn $ne + me = (n+m)e$, $ne \cdot me = nme^2 = nme$. Der Quotientenkörper Π von $\mathfrak{p}$ 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 $\neq \Omega$.

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

$$n \longleftrightarrow ne$$

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

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

$$w = \sum \alpha_i v_i \quad (\alpha_i \text{ aus } \Sigma)$$
$$= \sum\sum \beta_{ik} u_k v_i \quad (\beta_{ik} \text{ aus } K).$$

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

$\sum \beta_{ik} u_k v_i = 0$ folgt

$\sum_k \beta_{ik} u_k = 0$, also $\beta_{ik} = 0$;

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

9/XII Es sei $K \subseteq \Sigma \subseteq \Omega$; Ω algebraisch über Σ, Σ algebraisch über K. Behauptung: Ω ist algebraisch über K.

Beweis: Es sei $w \in \Omega$; dann ist

$$w^n + \sigma_{n-1} w^{n-1} + \dots + \sigma_0 = 0,$$

wo $\sigma_i \in \Sigma$. Der Körper $K(\sigma_0)$ ist einfache alg. Erw. von K, also endliche Erweiterung; $K(\sigma_0, \sigma_1)$ 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 $K(\sigma_0 \sigma_1 \dots \sigma_{n-1})$ eine endliche Erweiterung von K; $K(\sigma_0, \sigma_1, \dots, \sigma_{n-1}, w)$ eine einfache algebr., also endliche Erweiterung von $K(\sigma_0 \dots \sigma_{n-1})$, also eine endliche Erweiterung von K; daher ist w algebraisch über K, w.z.b.w.

§6. Algebraisch abgeschlossene Körper.

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

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

Beweis: es sei ξ algebraisch über Ω; dann ist auch ξ algebr. über 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.

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 der 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 $K_1 \cong \overline{K_1}$, $K_2 \cong \overline{K_2}$ …, 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.

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.

§ 18 Der Hilbertsche Basissatz.

Wenn in einem Ring R jedes Ideal eine endliche Basis hat, so sagt man: in R gilt der Basissatz. In Körpern, im Euklidischen Ringen gilt der Basissatz.

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

Beweis: Sei A ein Ideal in $R[x]$, und A_0 die Gesamtheit der Koeffizienten der höchsten Potenzen von x in allen Polynomen von A. A_0 ist ein Ideal, hat also eine endliche Basis $(a_1 \dots a_r)$, gehörig zu Polynomen $(f_1 \dots f_r)$. Ist n der höchste Grad der Polynome f_i, so kann man modulo $(f_1, \dots, f_r)$ den Grad eines jeden Polynoms erniedrigen bis auf $n-1$. Sei nun A_1 das Ideal der Koeffizienten von x^{n-1} in diesen Polynomen vom Grad $\leqq n-1$.

W. Jarnik, Göttingen, Bühlstr. 28.

2. Heft.

Van der Waerden: Allgemeine Idealtheorie
Göttingen Wintersemester 1927-28

§ 20. Nullstellentheorie der Primideale

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

Beweis: Klar.

2.) Ist P dieses Primideal, so ist Ω dem Quotientenkörper des Restklassenringes R/P isomorph, und zwar entsprechen den Restklassen von $x_1, \cdots, x_n$ die Elemente $\xi_1 \cdots \xi_n$.

Beweis: Durch $f(x_1, x_2, \cdots, x_n) \to f(\xi_1, \xi_2, \cdots, \xi_n)$ wird R auf $K[\xi_1, \xi_2, \cdots \xi_n]$ meromorph abgebildet. Also ist $K[\xi_1 \cdots \xi_n]$ isomorph dem Restklassenring von R nach dem Ideal der Polynome f, denen die Null zugeordnet wird, dieses Ideal ist aber P. Dann müssen aber auch die Quotientenkörper isomorph sein.

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

Beweis: Den Polynomen f aus R ordnen

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 Flächen (Polynomen) des Ideals und gewissen irreduziblen Mannigfaltigkeiten.

Abstrahiert man 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.

Kap V. Ganze algebraische Größen.

Literatur: E. Noether, Abstrakter Aufbau ..., Math. Annalen 96 (1926).

§ 29. Moduln in bezug auf einen Ring.

Ein Modul war eine additiv geschriebene Abelsche Gruppe M (§ 2). Ist in einem Modul ein Multiplikationsring R gegeben, und eine Multiplikation $r \cdot m = m'$ der Elemente von M mit den Elementen von R erklärt, mit den Eigenschaften

1.) $r \cdot m$ ist Element von M

2.) $r(m_1 + m_2) = r m_1 + r m_2$

3.) $rs \cdot m = r \cdot sm$

4.) $(r+s)m = rm + sm$,

so nennt man M einen R-Modul. Untermoduln eines R-Moduls sind Untergruppen, die wieder R-Moduln sind; also die mit m auch rm enthalten, wo $r \in R$, 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).

Beispiele: Alle Ringe, die R umfassen, sind R-Moduln. Die Ideale in R sind R-Moduln.

Ein R-Modul heißt endlich, wenn er eine endliche Basis $m_1, \dots, m_s$ 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 R-Modul M besagt die Unmöglichkeit einer unendlichen Kette von Untermoduln

$$M_1 \subset M_2 \subset \dots$$

Ist insbesondere $M = R$, so hat man den Teilerkettensatz für Ideale.

Wie früher ist der Teilerkettensatz äquivalent mit dem Basissatz: Jeder Untermodul von M (und insbesondere M selbst) ist endlich.

$$\begin{vmatrix} a & r_1 & \cdots & r_n \\ 0 & r_{11}-a & \cdots & r_{1n} \\ \cdot & \cdot & \cdots & \cdot \\ 0 & r_{n1} & \cdots & r_{nn}-a \end{vmatrix} = 0 .$$

Folgen 1.) Summe und Produkt zweier ganzen Grössen b, c sind wieder ganz.
Beweis: Sei $b^h \equiv 0 (R, b, \cdots, b^{h-1})$
und $c^k \equiv 0 (R, c, \cdots, c^{k-1})$,
Man wähle für $g_1 \cdots g_n$ 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

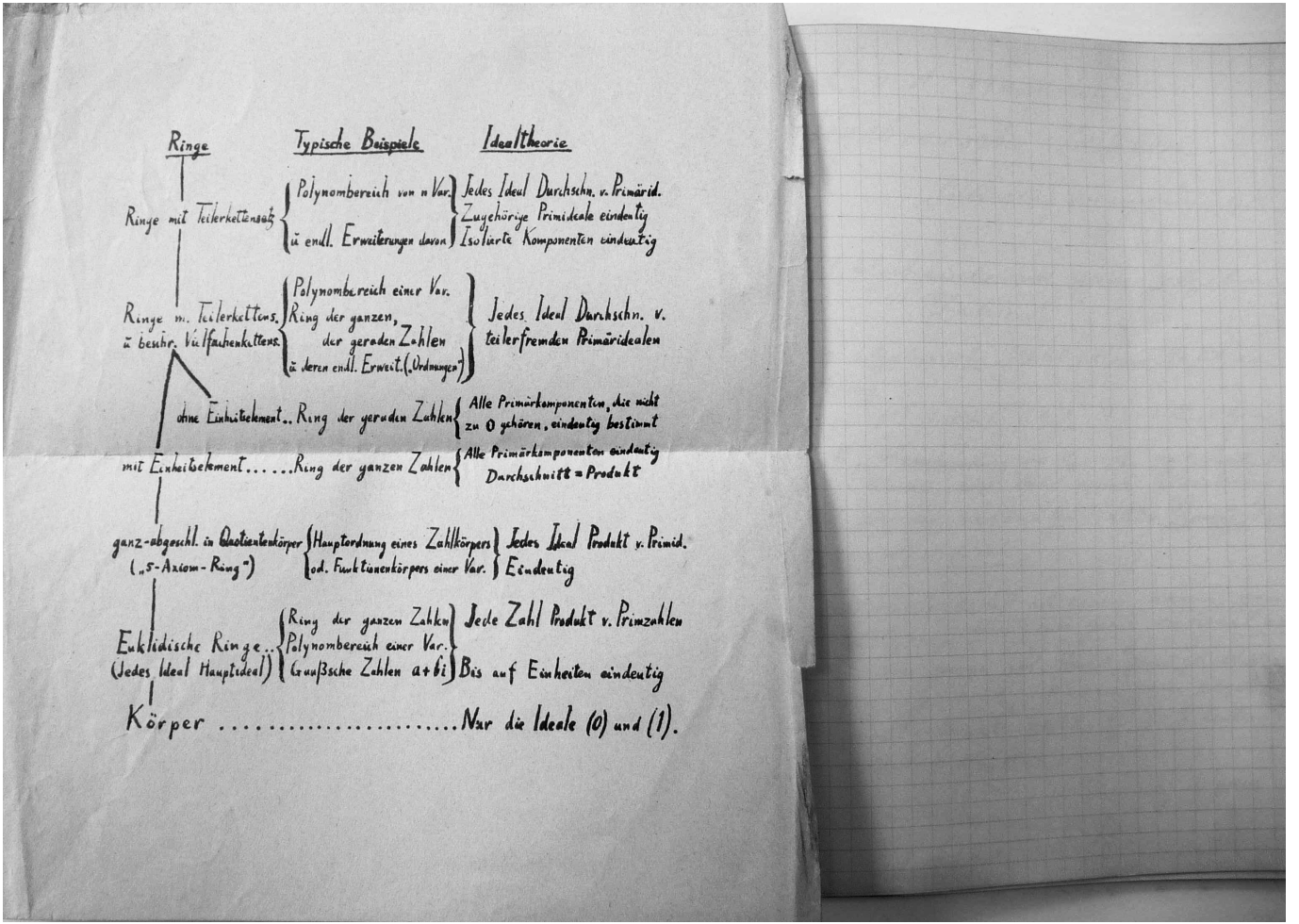
$$a^h + b_1 a^{h-1} + \cdots + b_h = 0$$

ist ganz, wenn die Koeffizienten $b_1, b_2, \cdots b_h$ es sind.
Beweis: Sei $b_i^{k_i} \equiv 0 (R, b_1, \cdots, b_i^{k_i-1})$.
Man nehme für $g_1, \cdots g_n$ alle Potenzprodukte $a^i b_1^{j_1} \cdots b_h^{j_h}$ $(i<h, j_1<k_1 \cdots j_h<k_h)$.
Dann ist das Kriterium erfüllt.
Daraus: Sind alle Elemente von S ganz in bezug auf R, und a in bezug auf S, so auch a in bezug auf R.
Ein Integritätsbereich R heisst ganz-abgeschlossen im Quotientenkörper P, wenn jede Größe aus P, die ganz in bezug auf R ist, in R liegt.
Gilt in R die eindeutige Faktorzerlegung, so ist 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 ganz in R.


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 bestnr. 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).