Modern algebra and polynomial ideals. By F. S. MACAULAY, M.A., St John's College.

(*Received* 2 October, *read* 27 November 1933.)

1. *Introduction**.

The aim of the following exposition is to give some idea of the scope of modern algebra in the light of the theory of ideals. It consists for the most part of definitions, examples, and the statement of theorems without proof; but the selection is severely restricted even in idealtheory. Thus no reference is made to the highly important matter of homomorphic, or multiply isomorphic, correspondence and its consequences.

The standard work is B. L. v. d. Waerden's *Moderne Algebra* in two volumes, which will be referred to as W. I and W. II†.

In the development of the theory of ideals three clearly marked stages can be discerned, based on Dedekind's original definition of an ideal, Lasker's definition of a primary ideal, and Noether's definition of an irreducible ideal. Special theories which have contributed to the general theory are Dedekind's writings‡, matrices, groups, Peirce's linear associative algebra§, Wedderburn's resolution of hypercomplex number systems‖, Lasker's "Moduln und Ideale"¶, and the general theory of pol. ideals**, framed on the theories of Dedekind and Lasker. These theories, at first apparently diverse and more or less independent, have been combined by E. Noether†† in a wonderful manner as the theory of ideals of rings in general, both commutative and non-commutative.

* The definitions of special terms used in the Introduction are given later. The following contractions are occasionally used: pol. (polynomial), el. (element), coeff. (coefficient), hom. (homogeneous), p.p. (power product), lin. ind. (linearly independent).

† W. I (1930), 243 pp. and W. II (1931), 216 pp. Verlag von Julius Springer, Berlin.

‡ *Gesammelte math. Werke*, Vieweg und Sohn, Brunswick.

§ *American J. of Math.* 4 (1881), 97–229.

‖ *Proc. Lond. Math. Soc.* (2), 6 (1908), 77–118.

¶ *Math. Annalen*, 60 (1905), 20–116.

** T. "Modular Systems", *Cambridge Tracts in Maths. and Math. Physics*, No. 19 (1916), 112 pp. A modular system is now more precisely named a pol. ideal. It consists of the aggregate of pols. $A_1F_1+A_2F_2+\ldots+A_kF_k$, where $F_1,\ldots,F_k$ are given pols. in n unknowns $x_1, x_2\ldots, x_n$ and $A_1, \ldots, A_k$ are arbitrary pols. It is specialised in respect to the coeffs. which are els. of a corpus, and so link it up directly with geometry.

†† N. (i). "Idealtheorie in Ringbereichen", *Math. Annalen*, 83 (1921), 25–66.

N. (ii). "Abstrakter Aufbau der Idealtheorie", *Math. Annalen*, 96 (1926), 26–61.

N. (iii). "Hyperkomplexe Grössen und Darstellungstheorie." *Math. Zeitschrift*, 30 (1929), 641–692; including idealtheory of non-commutative rings.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

In the greater portion of the commutative theory Noether assumes as a postulate that every ideal in a ring has a finite basis, which is true for pol. ideals. But she also expresses it in a different, more subtle, and in some ways more advantageous form. This states that in the ring R any series of ideals $M_1, M_2, \ldots$ in which each *includes* the one before and at least one more el. is finite*. This is to be true even when the extreme ideals are (0) and R, i.e. it is assumed that any *factor chain* of ideals in R, $(0) \subset M_1 \subset M_2 \subset \ldots$ must come to R after a finite number of steps, or is of finite *length*. The postulate does not say, however, that there is a chain whose length cannot be increased by inserting additional terms; in pol. idealtheory no such chain exists, for an additional term M_0 can always be inserted between (0) and M_1, and then another between (0) and M_0, and so on indefinitely†. The same may be true of other successive terms M_r, M_{r+1} in the chain. The property that in a ring R there is no ideal M_1 such that an ideal M_0 cannot be inserted between (0) and M_1, $(0) \subset M_0 \subset M_1$, is expressed by saying that there is no *minimal* ideal M_1 in R. It does, however, follow from the factor chain postulate that there is a *maximal* ideal M in R, between which and R no other ideal can be inserted. If this was not so a factor chain could be continued indefinitely from any term without ever coming to R. In pol. theory the ideal $(x_1, x_2, \ldots, x_n)$ is a maximal (or factorless) ideal, and so also is $(x_1 - a_1, \ldots, x_n - a_n)$, where $a_1, \ldots, a_n$ are els. in the corpus of coeffs.

In a non-commutative ring a *minimal condition* for right ideals is assumed, which then follows for left ideals, viz. that every *chain of multiples* $R \supset M_1 \supset M_2 \ldots \supset (0)$ is finite. From this it follows that R includes a minimal right ideal. By means of this postulate Noether obtains results in N. (iii) precisely analogous to those of the Jordan-Hölder theorem (N. (ii), p. 59) in group theory, which are however quite different in actual content and obtained by quite different reasoning. They are practically identical with Wedderburn's results on hypercomplex numbers, but cover a very much greater field.

One of the results analogous to the Jordan-Hölder theorem is that if the ring R includes no nilpotent ideal (though it may

* The proof that the two forms of the postulate are equivalent is given in W. II, p. 25 f. An ideal M_2 *includes* another M_1 if M_2 includes all the els. of M_1; and $M_1 \subset M_2$ denotes that M_2 includes M_1 and other els. in addition. This is looking at M_1 and M_2 as aggregates. Regarding them as ideals and entities, M_2 is called a *proper factor* of M_1, and M_1 a *proper multiple* of M_2.

† *Example.* In the ring of the natural numbers, and in the case of pols. in one unknown, every ideal has a basis (ϕ) consisting of a single element. Hence $M_1 \equiv (\phi)$, and between (0) and (ϕ) we can insert any number of ideals

$$(0) \subset (\phi\phi_1 \ldots \phi_r) \subset \ldots \subset (\phi\phi_1) \subset (\phi).$$

But only a finite number of ideals can be inserted between (ϕ) and R, viz. if ϕ is the product of k irreducible factors not more than $k-1$ ideals can be inserted in the chain between (ϕ) and R.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

include nilpotent elements) there is no multiple chain from R to (0) of more than a certain definite length l, and every multiple chain can be lengthened up to length l. Thus, when there is no nilpotent ideal in R, the minimal or multiple chain condition includes the maximal or factor chain condition. Either of the chain conditions includes the other if there is a finite limit to the chain length.

There is also a *restricted* multiple chain condition in which the last term (0) of the chain is excluded, and the chain ends with any given ideal $M \not\equiv (0)$. With the restricted condition it no longer follows that R includes a minimal ideal; but certain important results follow, at least for commutative rings, such as that every prime ideal is factorless, and every ideal is the product of its primary components.

In the above the terms maximal and minimal are used with their usual and simple meanings; but in W. II, pp. 27, 151, they are defined in a wider sense, at the cost of some loss in clearness.

2. *Definitions.*

In modern abstract algebra *adding* and *multiplying* are *undefined* processes. Both processes are assumed to be *associative*, i.e. $(ab)\,c = a\,(bc)$ and $(a+b)+c = a+(b+c)$. If either process is *commutative*, $ab = ba$ or $a+b = b+a$, as well as associative, it may be described as *permutative*, since the multiplying or adding of any number of elements can be carried out in any order without affecting the result. The process of adding is generally assumed to be permutative.

The subject-matter is the investigation of the properties of *aggregates*, i.e. classes of *elements*, defined by the laws or *postulates* which they obey. The elements may themselves be classes, or classes of classes, and may involve *unknowns*; but it is best at first to regard them as single individuals or operators.

A *group* is a multiplicative associative aggregate $a, b, c, \ldots$ such that the solution of the equation $ab = c$, where any one of the three elements a, b, c is the unknown and the other two are known, is always possible and unique within the group*.

If the multiplying is commutative as well as associative the group is called a commutative or Abelian group. The els. of a group, whether an Abelian group or not, *admit*† of multiplying and dividing, but not of adding. If adding is admitted some name other than group is used.

* This is more than sufficient for a definition. No attempt is made here or later to analyse a definition.

† We say that the els. of an aggregate *admit* of multiplying or adding when any product or sum of its els. is also an el. If $ab=c$ then $a=cb^{-1}$ and $b=a^{-1}c$.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

The following properties are easily proved from the definition. (i) If $ab = ac$ (or if $ba = ca$) then $b = c$; for, regarding b as the unknown in $ab = ac$, the *unique* solution is $b = c$. (ii) If $ae = a$, then $aec = ac$, $c = ec$ by (i), and $bae = ba$ or $ce = c$, i.e. $c = ec = ce$, where c is any el. of the group. The el. e is unique (for if e' has the same properties, $e' = ee' = e$) and is called the identity el. or the *unit-element*. (iii) If $ab = e$, then $aba = ea = a = ae$, i.e. $ba = e$. This el. b is called the *inverse* of a and is written a^{-1}; $aa^{-1} = a^{-1}a = e$. Conversely these properties (i), (ii), (iii) are more than sufficient to define a group.

A *module* is an additive permutative aggregate such that the solution of the equation $a + b = c$, where any one of the elements a, b, c is the unknown and the other two are known, is always possible and unique within the module.

In other words, a module is an Abelian group written additively. The properties corresponding to (i), (ii), (iii) for groups are: (i) If $a + b = a + c$, then $b = c$; (ii) if $a + 0 = a$, then $c = 0 + c = c + 0$, the el. 0 is unique and is called the *zero-element*; (iii) if $a + b = 0$, b is called the negative of a and a the negative of b, written $b = -a$ and $a = -b$.

The zero-el. is sometimes regarded as representing "nothingness", and if so regarded, is an el. common to all modules. It is nearly always written the same as the 0 of ordinary arithmetic. Similarly e in groups may be regarded as the 1 in arithmetic; but aggregates which are not groups may have differing unit-els. The definitions of 0 and e for any aggregate are that the adding of 0 or the multiplying by e leaves every el. unchanged.

A *ring* is a *module* whose elements admit of multiplying in accordance with the associative and distributive rules, i.e.

$$a(bc) = (ab)c, \quad (a + b)c = ac + bc, \quad c(a + b) = ca + cb.$$

If the multiplying is also commutative the ring is called a commutative ring. The reasoning in the theory of non-commutative rings, so far as it has been yet developed, is in marked contrast with the theory of commutative rings, being based on different assumptions (Introduction). In what follows we shall *consider only commutative rings.*

Since a ring is a module its els. admit of adding and subtracting. They also admit of multiplying, but not in general of dividing. *A ring may or may not include* (i) a unit-element e; (ii) *idempotent els.* e, $e^2 = e \neq 0$; (iii) *nilpotent els.* a, some finite power of which is zero but the el. a itself is not zero; (iv) *null-els.* (zero factors) a, b such that $ab = 0$, $a \neq 0$, $b \neq 0$.

A ring is an *integrity-domain* if it includes no null-els. In such a ring $ab = ac$, $a \neq 0$, always requires $b = c$; for $a(b - c) = 0$, $a \neq 0$, so that $b - c = 0$; and there is no idempotent el. e other than the unit; for $e(ea - a) = 0 = (ae - a)e$.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

A *corpus* (or *field*) is an integrity-domain-ring whose els. admit of dividing, excluding division by 0. From any integrity-domain-ring R, a corpus K can be constructed which includes a ring isomorphic to R. The older term *corpus* is much to be preferred to *field* since any aggregate can be named a field.

Ring-extension. If a ring R is enlarged by adding to it an el. x not in R we get an *extension ring*, written $R[x]$. It includes as els. all polynomials

$$(a_0 + c_0)\, x^m + (a_1 + c_1)\, x^{m-1} + \ldots + (a_{m-1} + c_{m-1})\, x + a_m,$$

where $a_0, a_1, \ldots, a_m$ are els. of R and $c_0, c_1, \ldots, c_{m-1}$ are ordinary integers ($c_0 x^m$ means $\pm x^m$ added to itself $\pm c_0$ times). If however R includes a unit-el. e which is also a unit-el. for x ($ex = x$), the part $c_0 x^m + c_1 x^{m-1} + \ldots + c_{m-1} x$, which is derived from x alone, can be omitted, being equal to $ec_0 x^m + ec_1 x^{m-1} + \ldots + ec_{m-1} x$, where $ec_0, ec_1, \ldots, ec_{m-1}$ are els. of R.

$R[x]$ is called an *algebraic extension* of R if x satisfies any equation $(a_0 + c_0)\, x^m + \ldots + (a_{m-1} + c_{m-1})\, x + a_m = 0$, and a *transcendental* extension if it does not satisfy any such equation. In the latter case each el. of $R[x]$ is a *unique* pol. of the form above. If x is an unknown the ring $R[x]$ is isomorphic with any transcendental extension $R[t]$, t known, viz. $f(x) \rightleftarrows f(t)$. *Since x is an unknown,* neither a variable nor an indeterminate, *it is to be regarded as an el. of $R[x]$.*

In a sense $R[x]$, whether x is known or unknown, is no more general than R. Both are rings and R could include unknown els. The general theory of rings holds in the same way for $R[x]$ as for R; and the only kind of question that can arise is whether a specified property of R, not true for all rings, holds for $R[x]$ or not. There are some such properties, notably the property that if each ideal in R has a finite basis, and R has a unit-el. e, and $x = ex$, then the same is true of $R[x]$; *Hilbert's theorem* (W. II, p. 23).

The most important case is when the ring R is a corpus K which is extended by the addition of a finite number of new els. $x_1, x_2, \ldots, x_n$. We assume that the unit-el. e, or 1, of K is also a unit-el. for each of $x_1, \ldots, x_n$. Then $K[x_1, x_2, \ldots, x_n]$ denotes the ring of all pols. in $x_1, \ldots, x_n$ with coeffs. in K; $K(x_1, \ldots, x_n)$ the corpus of all rational functions of $x_1, \ldots, x_n$ with coeffs. in K; and $K(x_{r+1}, \ldots, x_n)[x_1, \ldots, x_r]$ the ring of all pols. in $x_1, \ldots, x_r$ with coeffs. in the corpus $K(x_{r+1}, \ldots, x_n)$. It is clear that

$$K[x_1, \ldots, x_n] \equiv K[x_{r+1}, \ldots, x_n][x_1, \ldots, x_r] \equiv K[x_1][x_2]\ldots[x_n].$$

$K[t_1, t_2, \ldots, t_n]$ is a pure transcendental extension of K if there is no pol. $f(t_1, t_2, \ldots, t_n)$ with coeffs. in K which vanishes. If $x_1, \ldots, x_n$ are unknowns the ring $K[x_1, \ldots, x_n]$ is isomorphic with the ring $K[t_1, \ldots, t_n]$.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

3. *General idealtheory.*

An *ideal* in a ring R is a module M in R whose els. admit of multiplying by all the els. of R; i.e. if $\alpha_1, \alpha_2, \ldots$ are els. of M so also are $r_1\alpha_1$, $r_2\alpha_2$, and $r_1\alpha_1 + r_2\alpha_2 + \ldots$, where $r_1, r_2, \ldots$ are any els. of R. If R does not include a unit-el. $(r_i + m_i)\alpha_i$ must be written in the place of $r_i\alpha_i$, where m_i is an ordinary integer. If M can be generated from a finite number of fixed els. $\alpha_1, \alpha_2, \ldots, \alpha_k$ it is said to have a finite *basis*, and we write $M \equiv (\alpha_1, \alpha_2, \ldots, \alpha_k)$. Only such rings R will be considered as satisfy the finite basis postulate for all ideals in it.

A finite *ring-module*, or R-module, $M \equiv (\alpha_1, \ldots, \alpha_k)$ is defined in the same way as an ideal except that M need not be in R. If the R-module M is not an ideal in R the basic els. $\alpha_1, \alpha_2, \ldots, \alpha_k$ cannot all be in R.

Some of the simpler properties of ideals are independent of the finite basis postulate (W. II, p. 32), but it is not necessary here to separate them out. An ideal (α) with a basis consisting of a single el. α is called a *principal ideal*.

Although an ideal is defined as an aggregate it is also regarded as a single entity. As a consequence of this, terms applied to aggregates become transformed for ideals, *sum* to H.C.F., *intersection* to L.C.M., and so on. Thus in the ring of integers the ideal (6) is a multiple of (2), and (2) a factor of (6); but the aggregate $(2) \supset (6)$, and $(6) \subset (2)$, since (2) includes all the els. of (6) and more.

There are two extreme ideals in R, viz. (0) which has only one el., and R which includes all els., and is the same as (1) if R has a unit-el. 1. The only ideals in a corpus K are (0) and (1).

Any el. α of an ideal M is called a multiple of M since the ideal (α) is a multiple of M. This is denoted by $\alpha = 0\,(M)$. Also $M_1 = 0\,(M)$ has the same meaning as $M_1 \subseteq M$.

The H.C.F. $(M_1, M_2, \ldots)$ of any number of ideals $M_1, M_2, \ldots$ is the ideal consisting of all sums $\alpha_1 + \alpha_2 + \ldots$, where $\alpha_1 = 0\,(M_1)$, $\alpha_2 = 0\,(M_2)$, ...

The L.C.M. $[M_1, M_2, \ldots]$ is the ideal consisting of all els. α common to $M_1, M_2, \ldots$, i.e. $\alpha = 0\,(M_1)$, $\alpha = 0\,(M_2)$, ... It is the intersection of the aggregates $M_1, M_2, \ldots$.

The *product* $M_1 M_2 \ldots M_k$ is the ideal consisting of all products $\alpha_1\alpha_2\ldots\alpha_k$, where $\alpha_1 = 0\,(M_1)$, $\alpha_2 = 0\,(M_2)$, ... and *all sums of such products*. It is a multiple of the L.C.M. and is equal to the L.C.M. if the ring R has a unit-el. e which is included in the H.C.F. (M_i, M_j) of each and every pair of the ideals; i.e. $(M_i, M_j) \equiv (e) \equiv R$.

The *quotient* (or residual) of M by M', written $M : M'$, is the ideal consisting of all els. α such that $\alpha M' = 0\,(M)$. Ideal factors and quotients are to be distinguished from factors and quotients in ordinary arithmetic. If $M : M' \equiv M''$ it does not follow that $M \equiv M'M''$,

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

or that $M:M'' \equiv M'$. In a quotient $M:M'$ it may generally be assumed that M' is a factor of M; for $M:M' \equiv M:(M, M')$, and (M, M') is a factor of M. A quotient of M is a factor of M; but not all factors are quotients. There may be many factors M' of M for all of which the quotient $M:M'$ is the same; but there is one and only one quotient of M among them; this is the quotient $M:(M:M')$ and the H.C.F. of all the factors M' (T. § 26). *When, and only when, M' is a quotient of M does it follow from $M:M' \equiv M''$ that $M:M'' \equiv M'$.*

A *prime* ideal P in R is an ideal such that if $\alpha_1\alpha_2 = 0\,(P)$, $\alpha_1 \neq 0\,(P)$, then $\alpha_2 = 0\,(P)$; or, what comes to the same thing, if $M_1M_2 = 0\,(P)$, $M_1 \neq 0\,(P)$, then $M_2 = 0\,(P)$. The ring R is a prime ideal in R although it is not possible that $\alpha_1 \neq 0\,(R)$. The ideal (0) is not prime unless R is an integrity-domain (p. 30).

A *primary* ideal Q in R is an ideal such that if $\alpha_1\alpha_2 = 0\,(Q)$, $\alpha_1 \neq 0\,(Q)$, then some finite power of α_2 is $0\,(Q)$* It follows that if $M_1M_2 = 0\,(Q)$, $M_1 \neq 0\,(Q)$, then $M_2^\rho = 0\,(Q)$. For, taking $\alpha_1 = 0\,(M_1)$, but $\alpha_1 \neq 0\,(Q)$, since $M_1 \neq 0\,(Q)$, and supposing that

$$M_2 \equiv (\alpha_2, \alpha_3, \ldots, \alpha_k),$$

we have $\alpha_1\alpha_i = 0\,(Q)$, $\alpha_1 \neq 0\,(Q)$; so that, $\alpha_i^{\rho_i} = 0\,(Q)$, and $M_2^\rho = 0\,(Q)$, where $\rho = (\rho_2 - 1) + \ldots + (\rho_k - 1) + 1$.

To a primary ideal Q corresponds a prime ideal P which is the aggregate of all els. in R of which some finite power is $0\,(Q)$. It is easily proved that this aggregate is an ideal and that it is prime and a factor of Q (W. II, p. 32). P is called the prime ideal *belonging* to Q and Q a primary ideal belonging to P. Further, some finite power of P is $0\,(Q)$, and the least value of ρ such that $P^\rho = 0\,(Q)$ is called the *index* of Q. If Q is primary with prime P and $M \neq 0\,(Q)$ is any ideal, *$Q:M$ is primary with prime P*; also $Q:M \equiv Q$ if $M \neq 0\,(P)$ and $Q:M \supset Q$ if $M = 0\,(P)$.

An *irreducible ideal* M in R (N. (i), p. 25) is such an ideal that if $M \equiv [M_1, M_2]$, one of the two ideals M_1, M_2 must be M; i.e. M is not the L.C.M. of any two of its *proper* factors; such as a power of a prime number in arithmetic. This may be called the L.C.M. irreducibility test. The *product* irreducibility test is only satisfied by a prime ideal.

The following are some of the principal theorems in general idealtheory (W. II, p. 34).

A prime ideal is irreducible.

An irreducible ideal is primary.

* Noether's definition (N. (i), p. 25), avoiding any reference to a prime ideal. Lasker's definition for pol. ideals was dependent on the manifold of Q and the prime P determined by it.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

Every primary factor of an irreducible ideal with the same belonging prime is a quotient of the same (Noether, not proved in W.).

The L.C.M. of any number of primary ideals with the same prime P is a primary ideal with prime P.

Any given ideal M is the L.C.M. *of a finite number of irreducible ideals.* All those with the same prime P can be collected into a single primary ideal with prime P; and all which are superfluous can be omitted. Hence *any ideal M is the* L.C.M. *of a finite number of primary ideals with different primes such that no one of the primary ideals is a factor of the* L.C.M. *of all the rest* (Lasker's theorem, extended by Noether to general ideals). Each of these primary ideals is called a *primary component* of M.

Let $Q_1, Q_2, \ldots, Q_k$ be the primary components of M, and let $P_1, P_2, \ldots, P_k$ be their belonging primes. *Then if $M' \neq 0\,(M)$ is any other ideal, having one or more of the primes $P_1, P_2, \ldots, P_k$ as a factor, $M : M'$ is a proper quotient of M; but if M' has no one of $P_1, P_2, \ldots, P_k$ as a factor, then $M : M' \equiv M$.*

The primes $P_1, P_2, \ldots P_k$ belonging to the primary components of M are all unique. Hence each P_i is also called a prime *belonging* to M. If P_i is not a factor of any $P_j\,(j \neq i)$, P_i is said to be *isolated*; otherwise it is said to be *imbedded*. These terms isolated and imbedded are also applied to the corresponding primary components of M. *Any isolated primary component of M is unique, an imbedded one is not unique; but the* L.C.M. *of any imbedded one and all the primary components with respect to which it is imbedded is unique.*

4. *Polynomial ideals.*

In this and the following sections an ideal M will mean a pol. ideal, i.e. an ideal in the ring $K[x_1, x_2, \ldots, x_n]$, where K is a corpus. All theorems in general idealtheory are true for ideals in this ring. Also the finite basis postulate for ideals is no longer a postulate, but a theorem, resulting from Hilbert's theorem (p. 31). Another theorem is that the ring $K[x_1, x_2, \ldots, x_n]$ is an integrity-domain* (p. 30). The most distinctive feature of pol. idealtheory is the existence of the manifold of an ideal, and the unique correspondence between a prime ideal and its manifold.

The *manifold* of an ideal M is the totality of points $(\xi_1, \xi_2, \ldots, \xi_n)$ which, when substituted for $(x_1, x_2, \ldots, x_n)$, make every el. of the ideal vanish. It is sufficient for this that the els. of any one basis of M should vanish. The coordinates $\xi_1, \xi_2, \ldots, \xi_n$ are not restricted to belong to K. The manifold of a power of an ideal M is the manifold of M; for if $\alpha = 0\,(M)$ then $\alpha^\rho = 0\,(M^\rho)$, i.e. α vanishes for all the points of M^ρ. The manifold of a primary ideal Q is the manifold

* Assuming that no pol. in the ring vanishes unless all its coeffs. vanish.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

of its prime P, since $P^\rho = 0 (Q)$. The complete manifold of any ideal M consists of the manifolds of all the prime ideals belonging to the isolated primary components of M.

In any prime ideal P a maximum number $n-r$ of the unknowns, say $x_{r+1}, \ldots, x_n$, can be chosen such that no pol. in $K[x_{r+1}, \ldots, x_n]$ can be an el. of P. If these unknowns are given arbitrary values the manifold of P will still include some points, but only a finite number. In fact, if we put $x = u_1 x_1 + \ldots + u_r x_r$ and equate the basic els. of P to zero, we can eliminate $x_1, x_2, \ldots, x_r$ and obtain an irreducible equation for x with coeffs. in $K[u_1, \ldots, u_r, x_{r+1}, \ldots, x_n]$. If this equation is of degree d its d solutions are linear functions of $u_1, u_2, \ldots, u_r$, viz. $x = u_1 \xi_{1i} + \ldots + u_r \xi_{ri}$, $(i = 1, 2, \ldots, d)$. The *general* point of the manifold of P is $(\xi_{1i}, \ldots, \xi_{ri}, x_{r+1}, \ldots, x_n)$, where $\xi_{1i}, \ldots, \xi_{ri}$ are algebraic functions of $x_{r+1}, \ldots, x_n$, i.e. each ξ_{ij} satisfies an equation with coeffs. in $K[x_{r+1}, \ldots, x_n]$. In order that a pol. in $K[x_1, x_2, \ldots, x_n]$ may vanish for this general point it is necessary and sufficient that the pol. should be an el. of P.

The number $n-r$ of the independent unknowns $x_{r+1}, \ldots, x_n$ is the *dimension* of P and its manifold, while the number r of the dependent unknowns $x_1, \ldots, x_r$ is called the *rank* of P; and the same definitions apply to the (highest) dimension and (lowest) rank of any ideal M, viz. these are the dimension and rank of the primary components of M of highest dimension. The rank of M does not alter when any or all of $x_{r+1}, \ldots, x_n$ are supposed to have arbitrary (i.e. non-special) known values; nor does it alter when M is replaced by its equivalent H-ideal (p. 36); and again it is never ambiguous. For all of these reasons it seems of advantage to use the term *rank* for an ideal rather than *dimension*.

If M is of rank r its primary components of rank r are necessarily isolated and are consequently unique. Components of rank greater than r (dimension less than $n-r$) may be isolated or imbedded. If all the primary components of M are of the same rank M is called an *unmixed*, and otherwise a *mixed*, ideal. *The following are unmixed ideals:*

(i) An ideal M of rank r such that no one of the ideals

$$M, (M, u_n), \ldots, (M, u_n, \ldots, u_{r+2})$$

has a primary component of rank n, where $u_n, u_{n-1}, \ldots, u_{r+2}$ are non-special linear non-hom. functions of $x_1, x_2, \ldots, x_n$. The converse also is true that M is a mixed ideal if this set of conditions does not hold.

(ii) An ideal M of rank r which has a basis consisting of r els. only.

(iii) Any power of the ideal M in (ii). A power of a prime ideal may be mixed.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

(iv) An ideal of rank r whose basis consists of all the determinants of a matrix of pols. with $r-1$ more columns than rows. Both (ii) and (iii) are particular cases, since

$$M^\rho \equiv (F_1, F_2, \ldots, F_r)^\rho \equiv \begin{pmatrix} F_1, & F_2, & \ldots, & F_r, & 0, & 0, & \ldots \\ 0, & F_1, & \ldots, & F_{r-1}, & F_r, & 0, & \ldots \\ \ldots\ldots & & & & & & \end{pmatrix} \rho \text{ rows.}$$

There could be no better example of method than Krull's proof of Lasker's extension of M. Noether's "fundamental theorem", which has not been published as far as I am aware*. Lasker's statement (Satz XXVII) can be expressed in a modified but equivalent form, viz. "If $M \equiv (F_1, F_2, \ldots, F_k)$, $P \equiv (x_1, x_2, \ldots, x_n)$, and $F = 0\,(M, P^l)$ for all values of l greater than 0, there exists a pol. ϕ with non-vanishing constant term such that $F\phi = 0\,(M)$". It is clear that the aggregate of pols. F is an ideal, viz. $M_P \equiv (F_1', F_2', \ldots, F_{k'}')$. The first part of the proof is to show that $M_P \equiv (M, P^h M_P)$, where h has any given numerical value. By the definition of a quotient,

$$(M, P^h M_P) : P^h \supseteq P^h M_P : P^h \supseteq M_P,$$

i.e. $M_P = 0\,((M, P^h M_P) : P^h)$. But $(M, P^h M_P) : P^h$ only differs from $(M, P^h M_P)$ in respect to the primary component whose prime is P; and of this component M, $P^h M_P$, P^l are all multiples, and therefore also (M, P^l) and M_P. Hence $M_P = 0\,(M, P^h M_P)$; also

$$(M, P^h M_P) = 0\,(M_P);$$

therefore $M_P \equiv (M, P^h M_P)$.

Now $M_P \equiv (F_1', F_2', \ldots, F_{k'}')$; hence

$$F_i' = 0\,(P^h M_P, M) = u_{i1} F_1' + u_{i2} F_2' + \ldots + u_{ik'} F_{k'}'\,(M),$$

where $u_{ij} = 0\,(P^h)$. Solving the k' equations of this kind we have $DF_i' = 0\,(M)$, where D is the determinant whose diagonal els. are $u_{11} - 1, \ldots, u_{k'k'} - 1$ and the other els. are $u_{ij}\,(i \neq j)$. Then, since

$$F = 0\,(F_1', \ldots, F_{k'}'),$$

it follows that $DF = 0\,(M)$, where D is a pol. with constant term ± 1.

H-ideals. A linear combination of any given set of pols. in $K[x_1, x_2, \ldots, x_n]$ means the sum of any number of the set with multipliers which are els. of K. If no one of the set is a linear combination of the rest the set is called a *linearly independent* set. Consider a *complete* lin. ind. set of els. of an ideal M of degrees less than or equal to l. Such a set exists in which all the els. of any the same degree k are not only lin. ind. in themselves, but also as regards their highest terms, those namely which are hom. of degree k; for, so long as this was not so, one or more els. of degree k could be replaced by els. of lower degree. When the els. of M of degrees

* The proofs by Lasker and in T. § 56 are both unsatisfactory.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

less than or equal to l have been thus arranged they can all be made hom. by means of an additional unknown x_0 of homogeneity. In this way we arrive at the els. of what is called an *H-ideal* M_0 in $K[x_0, x_1, \ldots, x_n]$ *equivalent* to M in $K[x_1, x_2, \ldots, x_n]$; in fact $M \equiv (M_0)_{x_0=1}$. An *H-ideal* in general is an ideal having a basis of hom. pols. in which only hom. els. are taken into account, every other el. being a linear combination of hom. els.

To every el. F_0 of M_0 corresponds a unique el. F of M, viz. $F \equiv (F_0)_{x_0=1}$; but to each el. F of M of degree l corresponds one el. F_0 of M_0 of degree l and one el. of every degree greater than l, viz. $x_0F_0, x_0^2F_0, \ldots$. *There is however a one-one correspondence between the els. of* M_0 *of degree* l *and the els. of* M *of all degrees less than or equal to* l.

Another important point to notice is that M_0 is not a general H-ideal; for if $x_0F_0 = 0\,(M_0)$ then $F_0 = 0\,(M_0)$, i.e., $M_0 : (x_0) \equiv M_0$. Expressed in words: *No power of* x_0 *is an el. of any primary component of* M_0; *and, in particular,* M_0 *has no primary component of dimension* 0 *or rank* $n+1$. An H-ideal M in $K[x_1, \ldots, x_n]$, other than (0) or (1), has or has not an equivalent non-H-ideal according as $M : (x_1, \ldots, x_n) \equiv M$ or not. If

$$M : (x_1, \ldots, x_n) \equiv M$$

we can choose a linear function $u \equiv c_1x_1 + \ldots + c_nx_n$ which is not an el. of any belonging prime of M, so that $M : (u) \equiv M$, and M is equivalent to the non-H-ideal $(M)_{u=1}$.

In the theory of H-ideals the most important point is the origin (0, 0, ..., 0); for there the supreme singularity of the manifold of the H-ideal is situated and all other singularities are reflected. In employing hom. coordinates in geometry this point is excluded, and can only be restored by replacing points by radiating lines from the origin.

5. *The inverse system.*

The explanation of the inverse system given in T. is rather difficult, but can be presented in a simpler way from the broadened outlook of modern algebra. It is sufficient at first to consider H-ideals, since a non-H-ideal can be replaced by its equivalent H-ideal.

The *inverse system* of an H-ideal M in $K[x_1, x_2, \ldots, x_n]$ is the aggregate M^{-1} of hom. pols. E in $K[x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}]$ such that each el. E of M^{-1} vanishes for each el. F of M when for the p.p. ω^{-1} in E is substituted the coeff. of ω in F; i.e. if $E \equiv \Sigma c\omega^{-1}$ and $F \equiv \Sigma a\omega$ then $\Sigma ca = 0$. Clearly F must be of the same degree as E in order that Σca may not vanish identically.

Hence the equating of the els. of M^{-1} to zero gives the equations which are identically satisfied by the coeffs. of any and every element of M.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

The aggregate M stands in the same relation to M^{-1} as M^{-1} does to M, $\Sigma ca = \Sigma ac = 0$, i.e. M is the inverse of M^{-1}, $M \equiv (M^{-1})^{-1}$. The arrays of the coeffs. of a complete lin. ind. set of els. F of M and a like set of els. E of M^{-1} of any the same degree are conjugate arrays, and the two arrays combined form a square array. Also M^{-1} is a module in the same sense as M, viz. the els. of M^{-1} of the same degree admit of adding and subtracting.

If E is an el. of M^{-1} so also is $\omega_1 E$, where ω_1 is any p.p. of $x_1, x_2, \ldots, x_n$; this is on the understanding that all terms in the product $\omega_1 E$ which are not in the ring $K[x_1^{-1}, \ldots, x_n^{-1}]$ are to be neglected; i.e. $\omega_1 c \omega^{-1}$ is to be assumed to vanish if any one of the indices in the p.p. ω_1 exceeds the corresponding index in the p.p. ω or ω^{-1}. That $\omega_1 E$ is an el. of M^{-1} follows from the corresponding property that $\omega_1 F$ is an el. of M if F is an el. of M. The derived el. $\omega_1 F$ is of higher degree than F whereas the degree of $\omega_1 E$ in $x_1^{-1}, \ldots, x_n^{-1}$ is less than the degree of E. It follows that if $E_1, E_2, \ldots, E_k$ are els. of M^{-1} then $A_1 E_1 + A_2 E_2 + \ldots + A_k E_k$ is an el., where $A_1, A_2, \ldots, A_k$ are arbitrary pols. in $K[x_1, \ldots, x_n]$ such that $A_1 E_1, \ldots, A_k E_k$ are hom. of the same degree; and *M, M^{-1} are both H-ring-modules with the same multiplying ring $K[x_1, \ldots, x_n]$.*

Example. If $M \equiv (x_1^{l_1}, x_2^{l_2}, \ldots, x_n^{l_n})$, then $M^{-1} \equiv (\omega^{-1})$, where $\omega \equiv x_1^{l_1-1} x_2^{l_2-1} \ldots x_n^{l_n-1}$, and (ω^{-1}) denotes* the inverse system whose els. are ω^{-1} and all derived els. $\omega_1 \omega^{-1}$.

If $F = 0(M) = A_1 x_1^{l_1} + \ldots + A_n x_n^{l_n}$, the coeffs. in F of ω and all p.ps. which are factors of the same are zeros; and this is also sufficient that we may have $F = 0(M)$. Hence the els. E of M^{-1} are ω^{-1} and $\omega_1 \omega^{-1}$, since these vanish for every el. F of M; i.e. $M^{-1} \equiv (\omega^{-1})$.

A system M^{-1} which has a basis (E) consisting of a single el. is called a *principal system* and the same name is given to the ideal M. A *principal ideal* is an ideal (F).

If M is any ideal such that $M^{-1} \equiv (E_1, \ldots, E_k)$, where the degrees of $E_1, \ldots, E_k$ are all less than a definite finite number l, then all els. of M^{-1} vanish for each of $x_1^l, x_2^l, \ldots, x_n^l$. Hence these are all els. of M, and M is a primary ideal with prime $(x_1, x_2, \ldots, x_n)$, whose manifold is a single point, the origin. This system M^{-1} and ideal M are of a very special and simple kind; if M is an H-ideal it has no equivalent non-H-ideal.

A general el. $E \equiv \Sigma c_{p_1, \ldots p_n} (x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n})^{-1}$ of the inverse system M^{-1} of a general H-ideal M must therefore be of *indefinite*

* In T. square brackets are used for the basis of M^{-1} but here round brackets are used, just as for M. While $(E_1, \ldots, E_k)$ denotes the sum or H.C.F. of $(E_1), \ldots, (E_k)$, $(E_1, \ldots, E_k)^{-1}$ is the L.C.M. of $(E_1)^{-1}, \ldots, (E_k)^{-1}$, viz.

$$M \equiv (E_1, \ldots, E_k)^{-1} \equiv [(E_1)^{-1}, \ldots, (E_k)^{-1}].$$

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

degree l so that a value as high as we please can be assigned to l, and $c_{p_1, \ldots, p_n}$ must be a function of $p_1, \ldots, p_n$. The derived el. $x_1^{l_1} \ldots x_n^{l_n} E \equiv \Sigma c_{p_1 \ldots p_n} (x_1^{p_1 - l_1} \ldots x_n^{p_n - l_n})^{-1}$ is also of *indefinite* degree and can be written

$$\Sigma c_{q_1 + l_1, \ldots q_n + l_n} (x_1^{q_1} \ldots x_n^{q_n})^{-1},$$

where $q_1, \ldots, q_n$ may be changed to $p_1, \ldots, p_n$. Hence

$$\Sigma c_{p_1 + l_1, \ldots, p_n + l_n} (x_1^{p_1} \ldots x_n^{p_n})^{-1}$$

is an el. of M^{-1} of the same degree as E, where $c_{p_1 + l_1, \ldots, p_n + l_n}$ is the same function of $p_1 + l_1, \ldots, p_n + l_n$ as $c_{p_1, \ldots, p_n}$ is of $p_1, \ldots p_n$. As before, if $M^{-1} \equiv (E) . M^{-1}$ and also M, is called a principal system.

Inverse system M^{-1} of a non-H-ideal M. This is defined in the same way as for an H-ideal except that the els. E of M^{-1} are now *non-hom. pols.* in $x_1^{-1}, \ldots, x_n^{-1}$ of indefinitely high degree, which are indistinguishable from infinite power series. There may be some els. E which are terminating power series or finite pols. This happens when (and only when) the manifold of M includes the origin, which is always the case for an H-ideal $\not\equiv (1)$. Not all factors of M have inverse systems which can be derived from M^{-1}, but all the latter are inverse systems of factors of M (cf. (ii) below).

If all the els. E of M^{-1} are broken off at degree l the resulting *truncated* els. will vanish for all els. of M of degrees less than or equal to l. A complete lin. ind. set of these truncated els. can be obtained by considering only the els. of M of degrees less than or equal to l. They correspond to the els. of M_0^{-1} of degree l.

Properties of the inverse system M^{-1}.

(i) If $M \equiv (F_1, F_2, \ldots, F_k)$ necessary and sufficient conditions that E may be an el. of M^{-1} are that each $F_i E$ should vanish identically. Hence every FE vanishes when

$$F = 0 (M) \text{ and } E = 0 (M^{-1}).$$

(ii) $(E_1, \ldots, E_h)^{-1}$: $(F_1, \ldots, F_k) \equiv (\ldots, F_i E_j, \ldots)^{-1}$.

(iii) If M is of rank n (dimension 0), M^{-1} has only a finite number of lin. ind. els.

The following ideals are principal systems.

(iv) *A prime ideal.*

(v) *An irreducible ideal. Conversely an ideal which is primary and a principal system is irreducible.* Since every ideal resolves into a finite number of irreducible ideals or principal systems, every inverse system has a finite basis.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

(vi) *Any ideal whose primary components are all principal systems and isolated, and only such.* The primes belonging to any ideal are all different but not necessarily isolated (p. 34).

From (v) and (vi) a principal system may be defined in general idealtheory as an ideal whose primary components are all irreducible and isolated; it may be mixed or unmixed.

(vii) *The quotient of a principal system with respect to a principal ideal*, by (ii) above.

(viii) *Any ideal M of rank r having a basis consisting of r els. only* $(F_1, F_2, \ldots, F_r)$. In fact $(M, x_{r+1}^{l+1}, \ldots, x_n^{l+1})^{-1}$ has a single basic el. ((vi) and T. § 71) from which all the els. of M^{-1} of degrees less than or equal to l can be derived. The converse is not true; e.g. if

$$M^{-1} \equiv (x_1^{-2} + x_2^{-2} + x_3^{-2}) \text{ in } K[x_1^{-1}, x_2^{-1}, x_3^{-1}],$$

then $$M \equiv (x_1^2 - x_3^2, x_2^2 - x_3^2, x_2x_3, x_3x_1, x_1x_2).$$

(ix) *An unmixed ideal M of rank r when $M^{(r)}$ is a principal system.* $M^{(r)}$ denotes the ideal M regarded as being in the ring

$$K(x_{r+1}, \ldots, x_n)[x_1, \ldots, x_r], \text{ having } K(x_{r+1}, \ldots, x_n)$$

as its coeff. domain. It is desirable to have a simpler proof than that given in T. § 82.

(x) *A superperfect ideal* (p. 43); and more generally an unmixed ideal M of rank r when $M^{(r)}$ is superperfect.

To prove (vi), suppose that $M \equiv [Q_1, Q_2, \ldots, Q_k]$, where $Q_1, Q_2, \ldots, Q_k$ are all irreducible and isolated. Then

$$M^{-1} \equiv (Q_1^{-1}, \ldots, Q_k^{-1}) \equiv (E_1, \ldots, E_k).$$

Choose a pol. $F = 0\,[Q_2, \ldots, Q_k]$, but $F \neq 0\,(P_1)$, where P_1 is the prime of Q_1. This can be done because P_1 is isolated.

Now $F(E_1 + \ldots + E_k) = FE_1$, since $FE_i = 0\,(i > 1)$.

But $$(FE_1)^{-1} \equiv (E_1)^{-1} : (F) \equiv Q_1 : (F) \equiv Q_1,$$

since $F \neq 0\,(P_1)$; hence $(FE_1) \equiv Q_1^{-1} \equiv (E_1)$. Thus all els. $E_1, \ldots, E_k$ can be derived from the single el. $E_1 + E_2 + \ldots + E_k$, i.e.

$$M \equiv (E_1 + \ldots + E_k)^{-1}.$$

The fundamental property of a principal system M is that every factor M' all of whose belonging primes are primes belonging to M is a quotient of M with respect to another such factor M'' and M', M'' are reciprocal quotients; $M' \equiv M : M''$ and $M'' \equiv M : M'$. This theorem, if I am not mistaken, is one of Noether's in general idealtheory. Gröbner has used it for proving some important properties of ideals.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

6. *Perfect ideals.*

An H-ideal M of rank r in $K[x_1, \ldots, x_n]$ is a *perfect ideal* if the H-ideal $(M)_{x_{r+1}=\ldots=x_n=0}$ is of rank r (a condition which can always be fulfilled by a preliminary substitution) *and has as many lin. ind. els. up to any degree as the non-H-ideal* $M^{(r)}$ *has* (*v.* def. in (ix), p. 40). A non-H-ideal is perfect when its equivalent H-ideal is perfect.

A perfect ideal is unmixed. The proof is sketched here for an H-ideal M. Let $f_1, f_2, \ldots, f_\rho$ be a complete lin. ind. set of els. of $(M)_{x_{r+1}=\ldots=x_n=0}$ up to a definite finite degree l, and let $F_1, F_2, \ldots, F_\rho$ be a set of els. of M of the same degrees as $f_1, f_2, \ldots, f_\rho$, such that $(F_i)_{x_{r+1}=\ldots=x_n=0} = f_i$. Then the $F_1, F_2, \ldots, F_\rho$ form a complete lin. ind. set of els. of $M^{(r)}$ up to degree l. Let $\phi F = 0\,(M)$, where ϕ is a pol. in $K[x_{r+1}, \ldots, x_n]$ and F a pol. of degree less than or equal to l in $K[x_1, x_2, \ldots, x_n]$. Then

$$F = 0\,(M^{(r)}) = \lambda_1 F_1 + \lambda_2 F_2 + \ldots \lambda_\rho F_\rho,$$

where $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ are unique els. of $K(x_{r+1}, \ldots, x_n)$; and from the fact that $f_1, f_2, \ldots, f_\rho$ are lin. ind. it can be proved that

$$\lambda_1, \lambda_2, \ldots, \lambda_\rho$$

are pols. in $K[x_{r+1}, \ldots, x_n]$. Hence $F = 0\,(M)$: i.e. $\phi F = 0\,(M)$ requires that $F = 0\,(M)$. Hence M has no belonging prime of which any ϕ could be an el., and consequently no primary component of rank greater than r. Hence M is unmixed.

Example (i). $M \equiv (x_1^2, x_2 + x_1 x_3)$. This is a primary and irreducible ideal of rank 2 with prime (x_1, x_2), and with a basis consisting of two els. only; but it is not perfect. Multiplying $x_2 + x_1 x_3$ by x_1 and x_2, we see that x_1^2, $x_1 x_2$, x_2^2 are all els. of M; hence the equivalent H-ideal is

$$M_0 \equiv (x_1^2, x_1 x_2, x_2^2, x_0 x_2 + x_3 x_1).$$

Hence $(M_0)_{x_0=x_3=0} \equiv (x_1^2, x_1 x_2, x_2^2)$ is of rank 2, and has no el. of degree 1; but $M_0^{(2)}$ in

$$K(x_0, x_3)[x_1, x_2]$$

has an el. $x_0 x_2 + x_3 x_1$ of degree 1. Hence M_0 and M are not perfect. It may be noticed that $(M)_{x_3=0}$ has the same number of lin. ind. els. as $M^{(2)}$ in $K(x_3)[x_1, x_2]$ up to any degree. Hence the definition of a perfect H-ideal is insufficient if applied to a non-H-ideal.

Ex. (ii). $M \equiv (x x_4 - x_1 x_3, x_1^3 - x^2 x_3, x_1^2 x_4 - x x_3^2, x_1 x_4^2 - x_3^3)$. This is a prime H-ideal of rank 2 in $K[x, x_1, x_3, x_4]$ whose manifold

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

$(x = \lambda x_1 = \lambda^3 x_3 = \lambda^4 x_4)$ is a well-known quartic curve in hom. coordinates, and a quartic cone in 4-space.

$$(M)_{x=x_4=0} \equiv (x_1 x_3,\ x_1^3,\ x_3^3)$$

is of rank 2 and has only one el. of degree 2. But $M^{(2)}$ in

$$K(x, x_4)[x_1, x_3]$$

has two els. $x x_4 - x_1 x_3$, $x_4 x_1^2 - x x_3^2$ of degree 2. Hence M is not perfect. A general hyperplane u cuts the quartic cone in a quartic 3-space curve; but a hyperplane u_0 through the vertex of the cone cuts it in 4 lines and apparently an extra point at the vertex; for the ideal (M, u_0) imposes one more condition on its included els.* than (M, u) does. (M, u) includes all pols. which contain its manifold, but the same is not true of (M, u_0). If

$$u_0 \equiv c_4 x + c_3 x_1 + c_1 x_3 + c x_4,$$

the pol. $c_4 x_1^2 + c_3 x x_3 + c_1 x_1 x_4 + c x_3^2$ contains the manifold of (M, u_0), but is not an el. of (M, u_0). (M, u_0) is a mixed ideal and (M, u) unmixed. This illustrates the effects which singularities and projection may have.

Ex. (iii). *Any ideal M of rank n in $K[x_1, \ldots, x_n]$ is perfect.* This is true for an H-ideal by definition. Suppose then that M is a non-H-ideal and that M_0 is its equivalent H-ideal. Arrange a complete lin. ind. set of els. F of M up to degree l, as explained on p. 36, so that the hom. pols. formed by the terms of highest degree are also lin. ind. These form a lin. ind. set of els. of $(M_0)_{x_0=0}$ up to degree l. The els. F of M, after inserting x_0, form a lin. ind. set of els. F_0 of M_0 and of $M_0^{(m)}$. There are other els. of M_0 up to the degree l, viz. such els. as $x_0^p F_0$ of degrees less than or equal to l, where F_0 is one of the set already found ($x_1^{p_1} \ldots x_n^{p_n} F_0$ is itself an F_0); but these give no additional els. for $(M_0)_{x_0=0}$ or $M_0^{(m)}$. Hence M, $(M_0)_{x_0=0}$, $M_0^{(m)}$ all have the same number of lin. ind. els. up to any degree; i.e. M_0 is perfect and therefore also M. All this follows from the fact that $M_0 : (x_0) \equiv M_0$.

An unmixed H-ideal M of rank $n-1$ in $K[x_1, \ldots, x_n]$ is perfect. M has no primary component of rank n, i.e. $(x_1, x_2, \ldots, x_n)$ is not a prime belonging to it. Hence, if $M : (x_n) \not\equiv M$, we can substitute

$$x_n + c_1 x_1 + \ldots + c_{n-1} x_{n-1}$$

for x_n such that $M : (x_n) \equiv M$. Hence M is perfect.

It can also be proved, with the help of certain other theorems, that *an H-ideal of rank r in $K[x_1, \ldots, x_n]$ is perfect if the ideal $(M)_{x_{r+2}=\ldots=x_n=0}$ is of rank r and unmixed; and conversely.* Thus the

* Also the els. of (M, u_0, u_1) are subject to five or four conditions, according as u_1 passes through the vertex of M or not; i.e. the apparent extra point of (M, u_0) is retained, or not, in (M, u_0, u_1) in the two cases.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

ideals stated to be unmixed in (ii), (iii), (iv), pp. 35, 36, *are also perfect when they are H-ideals* (cf. Ex. (i), p. 41).

Perfect ideals have simpler properties than other ideals; and the same is specially true of their inverse systems. When M is a perfect H-ideal of rank r, $M^{(r)}$ has a complete set of lin. ind. els. up to any degree which *end* with a complete lin. ind. set of els. of $(M)_{x_{r+1}=\ldots=x_n=0}$ in $K[x_1, x_2, \ldots, x_r]$. Correspondingly the inverse system $(M^{(r)})^{-1}$ has a complete set of lin. ind. els. (finite in number) which *begin with the els. of* $(M)^{-1}_{x_{r+1}=\ldots=x_n=0}$ in $K[x_1^{-1}, \ldots x_r^{-1}]$ and proceed indefinitely in ascending p.p.'s of $x_1^{-1}, \ldots, x_r^{-1}$, the degrees of the coeffs. in $K[x_{r+1}, \ldots, x_n]$ also ascending at the same time and to the same extent from 0 onwards, so that the complete el. (or power series in $x_1^{-1}, \ldots, x_r^{-1}$) is homogeneous in all of $x_1, \ldots, x_n$ combined. The *total degree* in $x_1, x_2, \ldots, x_n$ of each of these els. of $(M^{(r)})^{-1}$ is the degree of the commencing terms reversed in sign, and is negative, with the exception of one el. of *total* zero degree.

A perfect H-ideal M of rank r such that $(M)_{x_{r+1}=\ldots=x_n=0}$ is a principal system is a *superperfect ideal**. Under these conditions M is a principal system and perfect, but the latter are not sufficient conditions for M to be superperfect (Ex. (iii), p. 44). *An H-ideal of rank r with a basis consisting of r els. only is superperfect*, and the only ideal so far discussed which is superperfect*. When M is superperfect of rank r, $(M^{(r)})^{-1}$ has a *whole* basis $(E^{(r)})$ such that any *whole*† el. of $(M^{(r)})^{-1}$ is $AE^{(r)}$, where A is a pol. in $K[x_1, x_2, \ldots, x_n]$ and $E^{(r)}$ begins with the single basic el. of $(M)^{-1}_{x_{r+1}=\ldots=x_n=0}$. Similarly, if M is perfect but not superperfect, $(M^{(r)})^{-1}$ has a whole basis $(E_1^{(r)}, \ldots, E_k^{(r)})$ whose els. begin with any set of basic els. of $(M)^{-1}_{x_{r+1}=\ldots=x_n=0}$.

Let M' be now any unmixed (perfect or non-perfect) H-ideal of rank r such that $(M')_{x_{r+1}=\ldots=x_n=0}$ is of rank r. Take any superperfect H-ideal M of rank r such that $M = 0\,(M')$. It would suffice, for example, to choose any r els. of M' as the basis of M provided that they are such that $(M)_{x_{r+1}=\ldots=x_n=0}$ is of rank r. Finally take $M'' \equiv M : M' \equiv (M, F_1'', \ldots, F_k'')$, where no F_i'' is superfluous. *Then $(M'^{(r)})^{-1}$ has a whole basis $(F_1'', \ldots, F_k'')\,E^{(r)}$, where $(E^{(r)})$ is the whole basis of $(M^{(r)})^{-1}$. Also $M'^{-1} \equiv (F_1'', \ldots, F_k'')\,E$, where $(E) \equiv M^{-1}$. Also the two ideals M', M'', which are reciprocal quotients with respect to the superperfect ideal M, are both perfect if one is.*

* Also a non-H-ideal is superperfect if its equivalent H-ideal is superperfect. An H-ideal of rank n which is a principal system is superperfect. $M \equiv (x_1^{-1} + x_2^{-2})^{-1}$ is not; for $M_0 \equiv (x_0 x_1 - x_2^2, x_1^2, x_1 x_2)$ and $(M_0)_{x_0=0} \equiv (x_1^{-1}, x_2^{-1})^{-1}$.

† A *whole el.* of $M^{(r)}$ or $(M^{(r)})^{-1}$ is, as the name indicates, an el. whose coeffs. are whole instead of fractional as regards $x_{r+1}, \ldots, x_n$. A whole el. or basis of $M^{(r)}$ is simply an el. or basis of M when M is unmixed. A whole basis of $(M^{(r)})^{-1}$ is a basis $(E_1^{(r)}, \ldots, E_k^{(r)})$ of whole els. such that any whole el. of $(M^{(r)})^{-1}$ is of the form $A_1 E_1^{(r)} + \ldots + A_k E_k^{(r)}$, where $A_1, \ldots, A_k$ are pols. in $K[x_1, \ldots, x_n]$.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

The number k of the els. in the basis of $(M'^{(r)})^{-1}$ above is the least number that will suffice for a *whole* basis*; though a much smaller number might suffice for a basis not a whole basis. All that can be said of the k els. in the basis of M'^{-1} is that no one of them is superfluous although a smaller number might suffice. In the following examples, except in Ex. (i), M', M, and $M'' \equiv M : M'$, have the meanings assigned them above; in particular M' is *any given unmixed H-ideal* of rank r. If M is not given, the easiest way of choosing it is that described above.

Ex. (i). The inverse system of the ideal $(x_1 - a_1, \ldots, x_n - a_n)$ has only one el., viz. $E \equiv \Sigma\, a_1^{p_1} \ldots a_n^{p_n} (x_1^{p_1} \ldots x_n^{p_n})^{-1}$. This begins with the constant term $(x_1^0 x_2^0 \ldots x_n^0)^{-1}$, which may be written 1. The derived el. $x_1^{l_1} \ldots x_n^{l_n} E$ is equal to $a_1^{l_1} \ldots a_n^{l_n} E$. If an ideal is the L.C.M. of k such simple ideals its inverse system will have k corresponding els. $E_1, \ldots, E_k$, which can be combined into one principal or basic el. $E_1 + E_2 + \ldots + E_k$.

The principal or basic els. of the inverse system of the most general ideal whose manifold is a single point $(a_1, \ldots, a_n)$ consist of a number of power series $\Sigma f a_1^{p_1} \ldots a_n^{p_n} (x_1^{p_1} \ldots x_n^{p_n})^{-1}$, where f is a pol. in $K[p_1, p_2, \ldots, p_n]$. To this basic el. corresponds a *polynomial* ϕ in $K[x_1^{-1}, \ldots, x_n^{-1}]$ if the origin is moved to the point $(a_1, \ldots, a_n)$. The two pols. f, ϕ do not have the same coeffs. but are of the same degree.

Ex. (ii). $M' \equiv (x_1^2, x_1 x_2, x_2^2, x_0 x_2 + x_3 x_1)$. We can choose

$$M \equiv (x_1^2, x_2^2);$$ then $$M'' \equiv M : M' \equiv (x_1^2, x_1 x_2, x_2^2, x_0 x_2 - x_3 x_1),$$

$$F_1'' = x_1 x_2,\ F_2'' \doteq x_0 x_2 - x_3 x_1,\ E^{(2)} \equiv (M^{(2)})^{-1} \equiv (x_1 x_2)^{-1},$$

and

$$(M'^{(2)})^{-1} \equiv (F_1'', F_2'')\, E^{(2)} \equiv (x_1^{-0} x_2^{-0},\ x_0 x_1^{-1} - x_3 x_2^{-1}).$$

Here $x_1^{-0} x_2^{-0}$, or 1, is only needed for a *whole* basis.

Ex. (iii). $M' \equiv (x_1 x_2,\ x_1 \overline{x_1 - x_3},\ x_2 \overline{x_2 - x_3})$. We can choose

$$M \equiv (x_1 \overline{x_1 - x_3},\ x_2 \overline{x_2 - x_3}).$$

$(M)_{x_3=0}$ has to be of the same rank 2 as M', and for this a basis $(x_1 x_2, x_1 x_3, x_2 x_3)$ will not serve for M' without making a substitution for x_3, such as $x_1 + x_2 - x_3$. $M'' \equiv (x_1 - x_3,\ x_2 - x_3) \equiv (F_1'', F_2'')$ is superperfect, while M' is perfect but not superperfect. $E^{(2)}$ begins with the principal el. of $(M)^{-1}_{x_3=0}$, viz. $x_1^{-1} x_2^{-1}$, and is of total degree -2. The whole basis of $(M'^{(2)})^{-1} \equiv (F_1'', F_2'')\, E^{(2)}$ has two els., each of

* Hence the least number k of els. which will suffice for a basis of $M'' \equiv M : M'$ (over and above els. of M) is independent of the choice of M, the ideal M' being given.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

total degree -1. Now $M^{(2)}$ is the L.C.M. of 4 simple ideals whose points are $(0, 0)$, $(0, x_3)$, $(x_3, 0)$, (x_3, x_3), and a basis for $(M^{(2)})^{-1}$ is, as in *Ex.* (i), the sum of their inverse systems

$$1, \Sigma x_3^p x_2^{-p}, \quad \Sigma x_3^p x_1^{-p}, \quad \text{and} \quad \Sigma x_3^{p+q} x_1^{-p} x_2^{-q}.$$

By subtracting the sum of the 2nd and 3rd from the sum of the 1st and 4th, and dividing out x_3^2 we have

$$E^{(2)} \equiv \sum_{p, q>0} x_3^{p+q-2} x_1^{-p} x_2^{-q} \equiv (x_1 x_2)^{-1} + \dots,$$

and

$$(M'^{(2)})^{-1} \equiv (x_1 - x_3, x_2 - x_3) E^{(2)} \equiv \left(\sum_{p>0} x_3^{p-1} x_2^{-p}, \sum_{p>0} x_3^{p-1} x_1^{-p} \right).$$

The method applied here to $M^{(2)}$ in order to find $(M^{(2)})^{-1}$ or $E^{(2)}$ might have been applied directly to $M'^{(2)}$ in order to find $(M'^{(2)})^{-1}$.

Ex. (iv). $M' \equiv (xx_4 - x_1 x_3, x_1^3 - x^2 x_3, x_1^2 x_4 - x_3^2 x, x_1 x_4^2 - x_3^3)$. M' is of rank 2 and order 4; $x = \lambda x_1 = \lambda^3 x_3 = \lambda^4 x_4$. But the ideal $(xx_4 - x_1 x_3, x_1^2 x_4 - x_3^2 x)$ regarded as an ideal in $K(x, x_4)[x_1, x_3]$ has only 4 points and may be used as a basis of $M'^{(2)}$ and for finding a basis of $(M'^{(2)})^{-1}$. The coeff. of $x_1^{-p} x_3^{-q}$ in the single el. of this basis is $\Sigma a_1^p a_3^q$ summed over the 4 points; and this is easily found to be $4x^{\frac{1}{4}(3p+q)} x_4^{\frac{1}{4}(p+3q)}$ or 0 according as $p \sim q = 0\,(4)$ or not. Hence $(M'^{(2)})^{-1} \equiv (\Sigma x^{\frac{1}{4}(3p+q)} x_4^{\frac{1}{4}(p+3q)} x_1^{-p} x_3^{-q})$, where $p \sim q = 0\,(4)$. The first few terms are

$$1 + xx_4 x_1^{-1} x_3^{-1} + x^3 x_4 x_1^{-4} + x^2 x_4^2 x_1^{-2} x_3^{-2} + xx_4^3 x_3^{-4} + x^4 x_4^2 x_1^{-5} x_3^{-1} + \dots.$$

Multiplying these by x_1^2, x_3, x_1 we find the els. of the whole basis of $(M'^{(2)})^{-1}$ to be

$$xx_1^{-2} + x_4 x_3^{-2} + x^2 x_4 x_1^{-3} x_3^{-1} + \dots, \quad x_1^{-1} + xx_4 x_1^{-2} x_3^{-1} + x_4^2 x_3^{-3} + \dots, \quad \text{and} \quad x_3^{-1} + x^2 x_1^{-3} + xx_4 x_1^{-1} x_3^{-2} + \dots.$$

They are all of total degree -1; which is what we are led to look for by taking M to be $(xx_4 - x_1 x_3, x_4^2 x_1 + x^2 x_3 - x_1^3 - x_3^3)$; when $M'' \equiv (M, F_1'', F_2'', F_3'')$, and $E^{(2)}$ begins with $x_1^{-3} - x_3^{-3}$.

Ex. (v). The numbers of lin. ind. els. of the ideals M, M', M'' of degree l are denoted by D_l, D_l', D_l''; and the numbers of *whole* els. of $(M^{(r)})^{-1}$, $(M'^{(r)})^{-1}$, $(M''^{(r)})^{-1}$ of total degree l lin. ind. with respect to K, *not* $K(x_{r+1}, \dots, x_n)$, are denoted by G_l, G_l', G_l''. The two series of numbers D_l', G_l' characterise the ideal M' more fully than either one alone; but in a perfect or superperfect ideal each series can be expressed in terms of the other. From the fact that $(M'^{(r)})^{-1} \equiv (F_1'', \dots, F_k'')\, E^{(r)}$ we obtain the relation

$$G'_{l-\gamma+1} = D_l'' - D_l,$$

where $\gamma - 1$ is the negative of the total degree of $E^{(r)}$, or the degree

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press

of the single basic element of $M_{x_{r+1}=\ldots=x_n=0}$. For $D_l'' - D_l$ is the number of els. F'' of $(F_1'', \ldots F_k'')$ of degree l of which no linear combination is an el. of M; for $M'' \equiv (M, F_1'', \ldots, F_k'')$; and

$$F E^{(r)} \equiv 0,$$

where $F = 0\,(F_1'', \ldots, F_k'')$ requires $F = 0\,(M^{(r)}) = 0\,(M)$, since F is a *whole* el. of $M^{(r)}$. Also $F'' E^{(r)}$ is of total degree $l - \gamma + 1$. Hence $G'_{l-\gamma+1} = D_l'' - D_l$; and similarly $G''_{l-\gamma+1} = D_l' - D_l$. These two relations may be regarded as determining the series G_l'', D_l'' in terms of the series D_l', G_l'. If M has only r basic els. of degrees $l_1, l_2, \ldots, l_r$, then $\gamma - 1 = \Sigma\,(l_i - 1)$ and D_l is the coeff. of x^l in $\{1 - (1 - x^{l_1}) \ldots (1 - x^{l_r})\}\,(1 - x)^{-n}$.

Many properties of pol. ideals, not excluding those of the inverse system, have been extended to analogous or identical properties in general idealtheory; and it seems likely that other such extensions may be made. The connecting link between the inverse system and general theory is that a primary principal system is an irreducible ideal. Another relation is the following: If M is an H-ideal then, as a *general* rule, the els. of M^{-1} correspond one-one to the classes of the "Restklassenring" $K[x_1, \ldots, x_n]/M$, the el. $\Sigma c\omega^{-1}$ of M^{-1} corresponding to the class to which $\Sigma c\omega$ belongs. The rule holds when, and only when, the sum of the squares of the determinants of the array of the coeffs. of a complete lin. ind. set of els. of M of degree l does not vanish for any value of l (cf. top of p. 38). Thus the rule does not hold for the principal H-ideal $M \equiv (\Sigma a\omega)$ if $\Sigma a^2 = 0$; but holds for every H-ideal in $K[x_1, \ldots, x_n]$ if there is no Σa^2, $a = 0\,(K) \neq 0$, which vanishes.

https://doi.org/10.1017/S0305004100012354 Published online by Cambridge University Press