BULL. AUSTRAL. MATH. SOC. 12A20, 13F05
VOL. 29 (1984), 167-175.

POLYNOMIALS DETERMINING DEDEKIND DOMAINS

JONATHAN A. HILLMAN

If A is a Dedekind domain and f generates a prime ideal of $A[X]$ which is not maximal, then the domain $A[X]/(f)$ is Dedekind if and only if f is not contained in the square of any maximal ideal of $A[X]$. This criterion is used to find the ring of integers of a cyclotomic field, and to determine when a plane curve is normal.

If f is an irreducible monic polynomial in $\mathbb{Z}[X]$ then the ring $K = Q[X]/(f)$ is an algebraic number field (and conversely every algebraic number field may be thus realised, by the Primitive Element Theorem [2, page 185]). The ring $\mathbb{Z}[X]/(f)$ is then contained in the ring of integers of K and so we may ask "when is $\mathbb{Z}[X]/(f)$ the full ring of integers of $Q[X]/(f)$?" The related question "if f in $k[T, X]$ determines an irreducible plane curve $V(f)$ over a perfect field k , when is $V(f)$ normal?" was answered by Zariski, who showed in [4] that this is so if and only if the ideal $(f, \partial f/\partial T, \partial f/\partial X)$ is the unit ideal. If k is algebraically closed, then by the Nullstellensatz this is equivalent to "f is not in m^2 for any maximal ideal m of $k[T, X]$ ", and it is this last criterion which suggests the answer to our question. As a consequence of our main theorem we shall show that the ring of integers of a cyclotomic field may be determined without first computing the discriminant of the

Received 14 October 1983. This work was begun under a grant from the UK Science Research Council at the University of Durham.

field, and we shall reprove Zariski's result (in the case of plane curves). Our method shall be to localize, so as to use Nakayama's lemma and the characterization of a Dedekind domain as a Noetherian domain which is everywhere locally a principal ideal domain.

We recall first some basic facts about localization and integral closure. If R is an integral domain, with field of fractions K, and p is a prime ideal of R, then the localization of R at p is the subring $R_p = \{r/s \text{ in } K \mid r \text{ in } R,\ s \text{ in } R\backslash p\}$ of K. It is a local ring, that is, has an unique maximal ideal, generated by the image of p. The ring R is integrally closed (or normal) if every element of K which is a root of a monic polynomial with coefficients in R is in R itself. An integral domain is 1-dimensional if every nonzero prime ideal is maximal; a Noetherian domain S is Dedekind (integrally closed and 1-dimensional) if and only if for each maximal ideal n of S the maximal ideal of the localization S_n is principal [1, page 95]. (A local domain with maximal ideal principal is called a discrete valuation ring.) If K is an algebraic number field (a finite algebraic extension of Q), the ring of integers of K is

$$O_K = \{\alpha \text{ in } K \mid f(\alpha) = 0 \text{ for some monic polynomial } f \text{ in } \mathbb{Z}[X]\} .$$

The ring O_K has field of fractions K and is Dedekind, and is contained in every such subring of K [1, page 96].

The following lemma is a special case of Nakayama's lemma [1, page 21].

LEMMA. *Let R be a local ring with maximal ideal m generated by 2 elements, $m = (r, s)$ say. Suppose that I is an ideal of R such that $m = m^2 + I$. Then $I = m$.*

Proof. Since $m = m^2 + I$, we may find m, n, p, q in m and i, j in I such that $r = mr + ns + i$ and $s = pr + qs + j$. Since the determinant $(1-m)(1-q) - (-n)(-p)$ is not in m, it is invertible in R, and so we may solve these two linear equations for r and s in terms of i and j. Hence $m \subseteq I$, and so $I = m$. //

In anticipation of our main result (Theorem 2), we shall determine when a polynomial with coefficients in a Dedekind domain generates a prime ideal or a maximal ideal. It is a familiar consequence of Gauss' Content Lemma that a nonconstant polynomial f with coefficients in a P.I.D. A generates a prime ideal of $A[X]$ if and only if it is irreducible in $A_0[X]$ and $c(f) = (1)$, where $c(f)$ is the ideal generated by the coefficients of f (that is, essentially their highest common factor) and A_0 is the field of fractions of A [2, page 127]. The Content Lemma, and hence this result, may be proved for A any Dedekind domain, by localizing at maximal ideals of A. (In fact it works also for A any Krull domain, if we define $c(f)$ as the intersection of all divisorial ideals of A which contain the coefficients of f, and localize at height one prime ideals of A.)

If A is a P.I.D. then $A[X]$ is factorial, and so f is irreducible in $A[X]$ if and only if (f) is a prime ideal of $A[X]$, and hence if and only if f is irreducible in $A_0[X]$ and $c(f) = (1)$. If A is integrally closed (in particular if A is Dedekind) then a monic polynomial f in $A[X]$ is irreducible in $A[X]$ if and only if it is irreducible in $A_0[X]$, for any monic factor in $A_0[X]$ must have coefficients which are sums of products of roots of f and so integral over A. On the other hand $A = \mathbb{Z}[\sqrt{-6}]$ is Dedekind but not a P.I.D. and $f = -\sqrt{-6}.X^2 + 5X + \sqrt{-6}$ is irreducible in $A[X]$ (and $c(f) = 1$) but $f = (\sqrt{-6})^{-1}(2X+\sqrt{-6})(3X+\sqrt{-6})$ in $A_0[X]$.

If the domain A has only finitely many prime ideals then $A[X]$ has principal maximal ideals. In fact A must then be a P.I.D. [3, page 24] and if $(p_1), \ldots, (p_r)$ are the nonzero prime ideals of A, any irreducible polynomial of the form $f = p_1 \ldots p_r Xg - 1$ (with g in $A[X]$) generates a maximal ideal of $A[X]$. However it follows from the next result that these are essentially the only such examples.

THEOREM 1. *Let A be a Dedekind domain with infinitely many prime ideals, and let m be a maximal ideal of $A[X]$. Then $m \cap A \neq 0$.*

Proof. If $m \cap A = 0$ then $m_0 = mA_0$ is a (proper) maximal ideal of $A_0[X]$, and so is principal. Therefore after localizing away from finitely

https://doi.org/10.1017/S0004972700021420 Published online by Cambridge University Press

many primes of A , we may assume $m = (f)$ for some nonconstant polynomial f . Let p be a nonzero prime of A , and let p in A generate the maximal ideal of A_p . Then p maps to a nonzero element of the field $A[X]/(f)$, so $p.g - 1 = h.f$ for some g, h in $A[X]$. Therefore f maps to a unit in $\left(A_p/(p)\right)[X]$ and so the constant term of f is a unit in $A_p/(p)$ and all the other coefficients of f are in p . At least one of these coefficients is nonzero and so is contained in only finitely many prime ideals of the Dedekind domain A . This contraducts our hypothesis and so we must have $m \cap A \neq 0$. //

COROLLARY 1. *No maximal ideal of A is principal.* //

COROLLARY 2 (Nullstellensatz for two variables). *Let F be an algebraically closed field, and let m be a maximal ideal of $F[T, X]$. Then $m = (T-\alpha, X-\beta)$ for some α, β in F .*

Proof. Since $F[T]$ has infinitely many primes, $m \cap F[T]$ is a non-zero prime ideal and so $T - \alpha$ is in m for some α . Similarly $X - \beta$ is in m for some β , and so $(T-\alpha, X-\beta) = m$. //

THEOREM 2. *Let A be a Dedekind domain and $(f) \subset A[X]$ a principal prime ideal which is not maximal. Then the domain $S = A[X]/(f)$ is Dedekind if and only if f is not in m^2 for any maximal ideal m of $A[X]$.*

Proof. The maximal ideals m of $A[X]$ which contain f correspond bijectively to the maximal ideals n of S under the surjection of $A[X]$ onto S . Thus it will suffice to show that for such an n , the localization S_n is a discrete valuation ring if and only if f is not in m^2 . Let $q = m \cap A$, $B = A_q$ and $R = A[X]_m$. Since $0 \subset f.R \subset m.R$ is a chain of distinct prime ideals, mR cannot be principal. Therefore q is a nonzero prime ideal of A , for otherwise B would be a field and R would be a principal ideal domain, as it is a localization of $B[X]$. Hence B is a discrete valuation ring, with maximal ideal qB generated by q say, and R is a local ring with maximal ideal mR generated by q and g , for some g representing an irreducible factor of the image of f in $(A/q)[X] = \left(B/(q)\right)[X]$. Since mR is not principal, the quotient mR/mR^2 has dimension 2 as a vector space over the field R/mR , by

https://doi.org/10.1017/S0004972700021420 Published online by Cambridge University Press

Nakayama's lemma. The maximal ideal of S_n is $mR/(f)$ and so is principal if and only if there is some t in R such that $mR = (f, t)$. In this case the images of f and t in mR/mR^2 would form a basis, so f is not in m^2. Conversely if f is not in m^2 then there is some t in R such that the images of f and t generate mR/mR^2, and hence $mR = (f, t)$ by Nakayama's lemma again. The theorem follows. //

If f is in m^2, then f' is in m, so f and f' map to 0 in the field $A[X]/m$. (Here f' denotes the derivative of f.) Thus, writing $m = (q, g)$ as in the theorem, the images of f and f' in $(A/q)[X]$ have a common root in an extension field of A/q. When this is the case may be determined readily by computing the resultant of f and f'. Recall that if C is an integral domain and f, g are in $C[X]$, the resultant of f and g is an element $R(f, g)$ in C (expressible as the determinant of a matrix whose entries are the coefficients of f and g and zeros) which is 0 if and only if f and g have a common root in a field containing C [2, page 135]. In particular $R(f, f') = 0$ if and only if f has a repeated root. Moreover, if p is a prime ideal of C and $\bar{f}$ and $\bar{g}$ denote the images of f and g in $(C/p)[X]$, then $R(\bar{f}, \bar{g})$ is the image of $R(f, g)$ in C/p (as is clear from the definition of the resultant in [2]). Thus the condition "f is not in m^2" in the theorem is satisfied automatically unless $m = (q, g)$ with q containing $R(f, f')$. Since A is assumed Dedekind, there are only finitely many such q (and hence only finitely many such m), provided that $R(f, f') \neq 0$. (An example in which $f' = 0$ although f is non-constant is given below.)

A similar argument using that a local Noetherian domain R with maximal ideal m is regular if and only if Krull $\dim R = \dim_{R/m} m/m^2$ [1, page 123], gives the following generalization: "if R is a regular Noetherian domain and $f_1, \ldots, f_h$ in R are such that $p_i = (f_1, \ldots, f_i)$ for $1 \leq i \leq h$ defines a chain of h distinct prime ideals, then R/p_h is regular if and only if the images of $f_1, \ldots, f_h$ in m/m^2 are linearly independent over R/m, for each maximal ideal m

of R which contains p_h ." (In the 1-dimensional Noetherian case "regular" is equivalent to "integrally closed".) However the two most interesting cases, namely $A = \mathbb{Z}$ or $A = k[T]$ with k a field, fall within the scope of the theorem as stated.

We shall now consider some examples. If $A = \mathbb{Z}$ and f is monic then $S = \mathbb{Z}[X]/(f)$ is contained in the ring of integers O_K of the algebraic numberfield $K = Q[X]/(f)$ and Theorem 1 gives an effective method of determining when S is all of O_K . In this case O_K is generated as an abelian group by the powers of a single element, for if ξ is the image of X in S then $S = \mathbb{Z}[\xi]$. For instance, let $K_n = \mathbb{Q}[X]/(\Phi_n)$ be the field of nth roots of unity, where Φ_n is the nth cyclotomic polynomial. Since $X^n - 1$ (and hence Φ_n) has distinct roots over any field of characteristic prime to n , the only primes dividing $R(\Phi_n, \Phi'_n)$ are factors of n . If $n = mq$ with $q = p^r$ and $(m, p) = 1$ then $\Phi_n(X) = \Phi_m(X^q)/\Phi_m(X^{q/p})$ so $\Phi_n \equiv \Phi_m^{\phi(q)}$ modulo (p) . Let ζ_m be a primitive mth root of unity. Then $\Phi_n(X)$ divides $\Phi_p(X^{n/p})$ and so $\Phi_n(\zeta_m)$ divides $\Phi_p(1) = p$. Therefore Φ_n is not in $(\theta, p)^2$ for any θ which is an irreducible factor of Φ_m modulo (p) , and so $\mathbb{Z}[\zeta_n] = \mathbb{Z}[X]/(\Phi_n)$ is the full ring of integers of K_n .

In general however it is not so easy to decide when the ring of integers of an algebraic number field has such a "primitive" basis. Although it is possible in principle to list the finitely many irreducible monic polynomials in $\mathbb{Z}[X]$ with the same degree and smaller discriminant than a given one f , and hence to decide whether there is one determining the full ring of integers of the field $Q[X]/(f)$, it is already an arduous task for a pure cubic, $f = X^3 - m$. Nevertheless the criterion of Theorem 1 suffices to show that if m is square free and neither of $m - 1$ nor $m + 1$ is divisible by 9 , then $\mathbb{Z}[X]/(X^3-m)$ is Dedekind. (Note also that $X^3 - m^2$ determines the same number field, but does not satisfy the

https://doi.org/10.1017/S0004972700021420 Published online by Cambridge University Press

criterion of the theorem.)

One might ask instead what is the minimum number of elements needed to generate O_K as a ring. In particular do two suffice? See [5] and [6] for methods of effectively determining O_K.

The case $A = k[T]$ corresponds to the geometric question: "when is a plane curve $V(f) = \{(a, b) \text{ in } k^2 \mid f(a, b) = 0\}$ nonsingular?". The word "nonsingular" is here open to several interpretations. The classical one is that f, $\partial f/\partial T$ and $\partial f/\partial X$ should generate the unit ideal, and thus have no common zeros (with coefficients in any extension field of k), so that the curve has everywhere a well defined tangent line, while the one more amenable to algebra is that the coordinate ring $S = k[T, X]/(f)$ should be a Dedekind domain. The latter is the more intrinsic notion, in that it depends only on the coordinate ring of the curve, and not the planar embedding. A curve $V(f)$ whose coordinate ring is Dedekind is said to be normal (over k).

If $V(f)$ is nonsingular in the classical sense, then it is certainly normal. For otherwise, by the theorem there would be some maximal ideal m of $k[T, X]$ such that f is in m^2, and hence $(f, \partial f/\partial T, \partial f/\partial X)$ would be contained in m and so not be the unit ideal. Zariski showed that if k is a perfect field (that is, if $\operatorname{char} k = 0$, or $\operatorname{char} k = p$ and the map : $x \to x^p$ for all x in k is surjective) the two interpretations are equivalent [4]. This may be seen as follows. If m is a maximal ideal of $k[T, X]$, then a variation of the argument of Corollary 2 shows that $m = (\phi(T), \psi(T, X))$ for some ϕ and ψ, and so if $L = k[T, X]/m$ the extension L/k is finite. If k is perfect, L/k must be separable, and so if $\bar{k}$ is an algebraic closure of k the ring $\bar{k}[T, X]/\bar{k} = \bar{k} \otimes L$ is a direct sum of copies of $\bar{k}$, indexed by the $n = [L : k]$ imbeddings of L in $\bar{k}$ [2, page 435]. Hence $\bar{k}m = \bigcap_{1 \le i \le n} m_i$ where m_i is a maximal ideal of $\bar{k}[T, X]$, and the map from $\bar{k} \otimes L$ to $\bigoplus_{1 \le i \le n} (\bar{k}[T, X]/m_i)$ sending $\kappa \otimes (g+m)$ to $(\kappa g+m_i)$ is an isomorphism. Therefore the map from $\bar{k} \otimes (m/m^2)$ to $\bigoplus_{1 \le i \le n} \left(m_i/m_i^2\right)$ sending $\kappa \otimes (g\phi+h\psi+m^2)$ to $\left(\kappa g\phi+\kappa h\psi+m_i^2\right)$ is onto, and so also an isomorphism, by a dimension count. Now if f is

https://doi.org/10.1017/S0004972700021420 Published online by Cambridge University Press

in $k[T, X]$ and $I = (f, \partial f/\partial T, \partial f/\partial X) \subseteq m$, then $\bar{k}I \subseteq m_i$ for each $1 \le i \le n$. By the Nullstellensatz $m_i = (T-t_i, X-x_i)$ for some t_i, x_i in $\bar{k}$ and on considering the Taylor expansions of f at (t_i, x_i) we see that f must be in m_i^2 for each $1 \le i \le n$. Hence f is in m^2. Thus if $V(f)$ is normal, $(f, \partial f/\partial T, \partial f/\partial X)$ is contained in no maximal ideal and so must be the unit ideal.

Zariski gave the following example to show that the assumption that k be perfect is in general necessary. Suppose that k is not perfect and that b is not a pth power in k (where $p = \text{char } k$). Let $f = T^p - b$. Then $\partial f/\partial T = \partial f/\partial X = 0$ and so $V(f)$ is singular everywhere from the classical point of view, but $T^p - b$ is irreducible in $k[T]$ [2, page 222], so $K = k[T]/(T^p-b)$ is a field and $k[T, X]/(f) = K[X]$ is a principal ideal domain, and so $V(f)$ is normal.

References

[1] Michael F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra* (Addison-Wesley, Reading, Massachusetts; London; Don Mills, Ontario; 1969).

[2] Serge Lang, *Algebra* (Addison-Wesley, Reading, Massachusetts, 1965).

[3] Jean-Pierre Serre, *Corps locaux* (Actualitiés Scientifiques et Industrielles, 1296. Hermann, Paris, 1962).

[4] Oscar Zariski, "The concept of a simple point of an abstract algebraic variety", *Trans. Amer. Math. Soc.* 62 (1947), 1-52.

[5] Hans J. Zassenhaus, "On Hensel factorization. II", *Symposia Mathematica*, 15, 499-513 (Convengo di Strutture in Corpi Algebrici, INDAM, Rome, 1973. Academic Press, London, 1975).

https://doi.org/10.1017/S0004972700021420 Published online by Cambridge University Press

[6] Horst G. Zimmer, *Computational problems, methods, and results in algebraic number theory* (Lecture Notes in Mathematics, **262**. Springer-Verlag, Berlin, Heidelberg, New York, 1972).

Department of Mathematics,
The Faculties,
Australian National University,
GPO Box 4,
Canberra, ACT 2601,
Australia.

https://doi.org/10.1017/S0004972700021420 Published online by Cambridge University Press