BULL. AUSTRAL. MATH. SOC. 16A66, 16A02
VOL. 14 (1976), 37-61.

The ideals of the hurwitzean polynomial ring

Margaret J. Morton

In 1919, Adolf Hurwitz formed the quaternion ring R composed of elements whose coordinates were either all integers or halves of odd integers. The objective of this paper is to examine the (two-sided) ideal structure in the hurwitzean polynomial ring $R[x]$, formed by taking all polynomials with coefficients in R. The maximal and prime ideals of $R[x]$ will be characterized with results surprisingly analogous to those in $Z[x]$. In addition, a canonical basis, of the type developed by G. Szekeres, 1952, for polynomial domains, will be developed for the ideals of $R[x]$.

A. Preliminaries

The hurwitzean ring of quaternions (R) is formed of all quaternions $\alpha = a_0 + a_1i + a_2j + a_3k$ where

(i) the coordinates a_0, a_1, a_2, a_3 are either all integers or are all halves of odd integers,

(ii) the units i, j, k satisfy the relations

$$i^2 = j^2 = k^2 = -1 \ , \quad ij = k = -ji \ , \quad jk = i = -kj \ , \quad ki = j = -ik \ .$$

The *conjugate* of α is $\bar{\alpha} = a_0 - a_1i - a_2j - a_3k$. The *norm* of α is $N(\alpha) = \alpha\bar{\alpha} = \bar{\alpha}\alpha = a_0^2 + a_1^2 + a_2^2 + a_3^2$. For all α and β in R, $N(\alpha)$ is in Z and $N(\alpha\beta) = N(\alpha)N(\beta)$. The *trace* of α is $\mathrm{tr}(\alpha) = \alpha + \bar{\alpha}$.

Received 29 October 1975.

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

$tr(\alpha)$ is in Z for all α in R. R is the maximal quaternion ring with the property that if α is in R, then $N(\alpha)$ and $tr(\alpha)$ are in Z.

If α is in R, then α is a *unit*, if and only if $N(\alpha) = 1$. The group of units of R consists of the twenty-four quaternions $\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.

The center of R is Z. Closely related are elements in R of norm two. Any such element which is a right divisor of an element in R is also a left divisor and vice versa.

Rédei [2] showed:

THEOREM 1. *All the distinct ideals of* R, *different from zero, are the principal ideals* $(m\lambda^t)$, *where* $m = 1, 2, \ldots$, $t = 0, 1$, $\lambda = 1 + i$.

From this theorem it follows quite readily that all ideals in R generated by elements of norm two are equal and that all ideals in R commute. The ideals of R will be denoted by $A, B, C, \ldots$.

It can also be shown that:

THEOREM 2. *The following are equivalent:*

(i) P *is a proper prime ideal in* R;

(ii) P *is a proper maximal ideal in* R;

(iii) $P = (p)$, *where* $p \neq 1$ *is an odd prime in* Z, *or* $P = (\lambda)$.

Let $K[x]$ be the quaternion polynomial ring composed of all elements $\rho(x) = r_0(x) + r_1(x)i + r_2(x)j + r_3(x)k$, where $r_0(x), r_1(x), r_2(x), r_3(x)$ are in $Q[x]$. Then $K[x]$ is a non-commutative integral domain with the obvious multiplication and addition. For an element $\rho(x)$ in $K[x]$, conjugate, norm and trace are defined as in R. In addition the symbol ∂ will be used to denote the degree of a polynomial. For any elements

$$\rho(x) = r_0(x) + r_1(x)i + r_2(x)j + r_3(x)k$$

and

$$\tau(x) = t_0(x) + t_1(x)i + t_2(x)j + t_3(x)k$$

in $K[x]$ the following results are easily verified.

(i) If $q(x)$ is in $Q[x]$, then $q(x)\rho(x) = \rho(x)q(x)$ (that is, $Q[x]$ is the center of $K[x]$).

(ii) $N(\rho(x)\tau(x)) = N(\rho(x))N(\tau(x))$.

(iii) $\partial N(\rho(x)\tau(x)) = \partial N(\rho(x)) + \partial N(\tau(x))$.

(iv) $\partial N(\rho(x)+\tau(x)) \leq \max\{\partial N(\rho(x)), \partial N(\tau(x))\}$.

(v) $\partial N(\rho(x)) = 0$, if and only if, $r_0(x), \ldots, r_3(x)$ are in Q .

Such elements $\rho(x)$ are in the quaternion ring.

DEFINITION. $\rho(x)$ is a *unit* in $K[x]$ if there exists $\sigma(x)$ in $K[x]$ such that either $\rho(x)\sigma(x) = 1$ or $\sigma(x)\rho(x) = 1$.

It is not necessary to distinguish between left and right units in $K[x]$. For if $\rho(x)\sigma(x) = 1$, then $\overline{\rho(x)} = \overline{\rho(x)}\rho(x)\sigma(x) = \sigma(x)\rho(x)\overline{\rho(x)}$, so $1 = \sigma(x)\rho(x)$.

THEOREM 3 (Division Algorithm). *Given* $\rho(x)$ *and* $\sigma(x)$ *not units in* $K[x]$, *there exist* $\tau(x)$ *and* $\mu(x)$ *in* $K[x]$ *such that* $\rho(x) = \tau(x)\sigma(x) + \mu(x)$, *where* $\partial\mu(x) < \partial\sigma(x)$. (As stated this is a right division algorithm. Similarly, there is a left division algorithm.)

THEOREM 4 (Existence of a greatest common divisor). *Any two elements* $\rho(x)$ *and* $\sigma(x)$ *in* $K[x]$, *which are not both zero, have a greatest common right divisor* $\phi(x)$ *which is uniquely determined up to a unit.*

Furthermore, there exist $\psi(x)$ *and* $\omega(x)$ *in* $K[x]$ *such that* $\phi(x) = \rho(x)\psi(x) + \sigma(x)\omega(x)$. (A similar result holds for a greatest common left divisor.)

DEFINITION. Let $\rho(x) = r_0(x) + r_1(x)i + r_2(x)j + r_3(x)k$ be in $K[x]$. Then $\rho(x)$ is *primitive* in $K[x]$ if the greatest common divisor of $r_0(x), \ldots, r_3(x)$ in $Q[x]$ is a unit.

The ideals of $K[x]$ will be denoted by $S(x), T(x), \ldots$.

THEOREM 5. *All the distinct ideals of* $K[x]$, *different from zero, are the principal ideals* $(a(x))$, *where* $a(x)$ *is in* $Z[x]$.

Proof. It follows from Theorem 3 that $K[x]$ is a principal ideal domain.

Let $S(x) = (\sigma(x))$ be an ideal in $K[x]$ where

$$\sigma(x) = s_0(x) + s_1(x)i + s_2(x)j + s_3(x)k$$

is a primitive element in $K[x]$. Then

$$i\sigma(x)i + j\sigma(x)j + k\sigma(x)k = -4s_0(x) + \sigma(x) ,$$

so $4s_0(x)$ is in $S(x)$. Furthermore,

$$2(i\sigma(x)j - j\sigma(x)i) = 4s_3(x) + 4s_0(x) ,$$

hence $4s_3(x)$ is in $S(x)$. Similar calculations show that $4s_1(x)$ and $4s_2(x)$ are in $S(x)$. But $\sigma(x)$ is primitive, so the greatest common divisor in $Q[x]$ of $4s_0(x), \ldots, 4s_3(x)$ must be a unit. By Theorem 4 this greatest common divisor must be in $S(x)$. Hence $S(x)$ contains a unit and must equal $K[x]$.

Let $T(x)$ be any proper ideal in $K[x]$. Then $T(x) = (\tau(x))$, where $\tau(x)$ is a nonprimitive element in $K[x]$. Let $\tau(x) = q(x)\sigma(x)$, where $q(x)$ is in $Q[x]$ and $\sigma(x)$ is primitive in $K[x]$. Then,

$$T(x) = (\tau(x)) = (q(x))(\sigma(x)) = (q(x)) .$$

Let l be the lowest common multiple of the denominators of $q(x)$, then $q(x) = l^{-1}a(x)$, where $a(x)$ is in $Z[x]$. Since l is a unit in $K[x]$ it now follows that $T(x) = (a(x))$.

THEOREM 6. *The following are equivalent:*

(i) $M(x)$ *is a proper maximal ideal in* $K[x]$ *;*

(ii) $M(x)$ *is a proper prime ideal in* $K[x]$ *;*

(iii) $M(x) = (p(x))$ *, where* $\partial p(x) \geq 1$ *and* $p(x)$ *is irreducible in* $Z[x]$ *.*

B. The quaternion factor rings $R_\lambda[x]$ and $R_p[x]$

Before the quaternion polynomial ring $R[x]$ can be discussed it is necessary to examine the structure of certain quaternion factor rings.

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

Let $\lambda = 1 + i$ and p be an *odd* prime in Z. Then $R_\lambda = \frac{R}{(\lambda)}$, $R_\lambda[x] = \frac{R}{(\lambda)}[x]$, $R_p = \frac{R}{(p)}$, and $R_p[x] = \frac{R}{(p)}[x]$ are all quaternion factor rings.

R_λ is a finite field with four elements. It has a complete set of representatives, namely 0, 1, $\frac{1}{2}(1+i+j+k)$ and $\frac{1}{2}(1-i-j-k)$, in R. Thus $R_\lambda[x]$ is a commutative principal ideal domain with a complete set of representatives in $R[x]$. By the same type of proof used for $Z[x]$ it follows that the proper maximal and prime ideals in $R_\lambda[x]$ are generated by the irreducible elements of $R_\lambda[x]$.

THEOREM 7. *(i)* R_p *is isomorphic to the ring of quaternions with coordinates in* Z_p *and consequently has* p^4 *elements.*

(ii) $R_p[x]$ *is isomorphic to the ring of quaternions with coordinates in* $Z_p[x]$.

(iii) R_p *is isomorphic to the full ring of two by two matrices with entries in* Z_p.

(iv) $R_p[x]$ *is isomorphic to the full ring of two by two matrices with entries in* $Z_p[x]$.

(v) $R_p[x]$ *is a principal ideal ring.*

Proof. *(i)* Clearly $Z_p \subseteq R_p$. Since $p \neq 2$, 2^{-1} is in Z_p and the desired result follows.

(ii) Immediate from *(i)*.

(iii) By Theorem 2, (p) is a proper maximal ideal in R. By *(i)*, R_p has only a finite number of elements, thus it can have only a finite number of maximal ideals and must be simple. Therefore, by the Wedderburn-Artin structure theorem, R_p must be isomorphic to a full matrix ring over a division ring. But by Theorem 1 this full matrix ring must have p^4 elements, thus the matrices must be two by two. Moreover the division ring

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

must contain p elements, so, without loss of generality, it can be taken as Z_p.

(iv) Follows from *(iii)*.

(v) Let $A(x)$ be an ideal in $R_p[x]$ and $\alpha(x) = \begin{bmatrix} a_{11}(x) & a_{12}(x) \\ a_{21}(x) & a_{22}(x) \end{bmatrix}$, where $a_{mn}(x)$ is in $Z_p[x]$ for $n = 1, 2$, $m = 1, 2$, be any element in $A(x)$. Using the fact that $A(x)$ is a two-sided ideal it follows that the matrices $\begin{bmatrix} a_{mn}(x) & 0 \\ 0 & 0 \end{bmatrix}$, $n = 1, 2$, $m = 1, 2$, are in $A(x)$.

Let $L(x) = \left\{k(x) \text{ in } Z_p[x] \mid \begin{bmatrix} k(x) & 0 \\ 0 & 0 \end{bmatrix} \text{ in } A(x)\right\}$. Then $L(x)$ is a non-trivial ideal in $Z_p[x]$. But $Z_p[x]$ is a principal ideal ring, hence $L(x) = (l(x))$ for some $l(x)$ in $L(x)$. Thus $\left(\begin{bmatrix} l(x) & 0 \\ 0 & 0 \end{bmatrix}\right)$ is contained in $A(x)$.

Conversely, since $a_{mn}(x)$, $m = 1, 2$, $n = 1, 2$, are in $L(x)$ it follows that in $Z_p[x]$, $a_{mn}(x) = l(x)b_{mn}(x)$ for $m = 1, 2$, $n = 1, 2$. Thus

$$\alpha(x) = \begin{bmatrix} l(x) & 0 \\ 0 & l(x) \end{bmatrix} \begin{bmatrix} b_{11}(x) & b_{12}(x) \\ b_{21}(x) & b_{22}(x) \end{bmatrix},$$

so $A(x)$ is contained in $\left(\begin{bmatrix} l(x) & 0 \\ 0 & l(x) \end{bmatrix}\right)$.

It is clear from this Theorem that R_p has a complete set of representatives in R and $R_p[x]$ has a complete set of representatives in $R_p[x]$.

DEFINITION. Let $\alpha(x) = a_0(x) + a_1(x)i + a_2(x)j + a_3(x)k$ be an element in $R_p[x]$. Then $\alpha(x)$ is *primitive* if the greatest common divisor of the $a_l(x)$, $0 \le l \le 3$, in $Z_p[x]$ is a unit.

THEOREM 8. *(i) The only proper ideals in* $R_p[x]$ *are of the form* $(a(x))$ *, where* $a(x) \not\equiv 1 \bmod p$ *is in* $Z_p[x]$.

(ii) The proper prime and maximal ideals in $R_p[x]$ *are* $(p(x))$ *, where* $p(x) \not\equiv 1 \bmod p$ *is irreducible in* $Z_p[x]$.

Proof. *(i)* This follows by the same type of argument that was used in Theorem 5.

(ii) By *(i)* the proper ideals in $R_p[x]$ commute, so the desired result follows by the standard method.

C. The quaternion polynomial ring $R[x]$

The ring $R[x]$ is clearly a subring of $K[x]$. Thus the definitions made for $K[x]$ are applicable for $R[x]$. However, the structure of $R[x]$ is more complicated than that of $K[x]$. $R[x]$ does not have a division algorithm and is not a principal ideal domain. It can be verified that it is a noetherian ring. The ideals of $R[x]$ will be denoted by $A(x), B(x), C(x), \ldots$.

In R ideals other than those generated by a unit were equal to the whole ring. The same type of situation arises in $R[x]$ as will be shown in Theorem 9.

Let ϕ_λ denote the natural epimorphism from $R[x]$ to $R_\lambda[x]$, where $\lambda = 1 + i$. Let ϕ_p denote the natural epimorphism from $R[x]$ to $R_p[x]$, where p is again an odd prime in Z .

THEOREM 9. *Let* $B(x)$ *be an ideal in* $R[x]$ *. Then* $B(x) = R[x]$ *, if and only if either*

(i) $B(x) = (\alpha(x), p)$ *, where* $\phi_p(\alpha(x))$ *is primitive in* $R_p[x]$ *; or*

(ii) $B(x) = (\alpha(x), \lambda)$ *, where* $\phi_\lambda(\alpha(x)) \equiv 1 \bmod \lambda$ *in* $R_\lambda[x]$.

Proof. Case 1: $B(x)$ contains prime $p \ne 2$. Now (p) is in the

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

kernel of ϕ_p and $(p) \subseteq B(x)$, thus $R[x]/B(x) \cong R_p[x]/\phi_p(B(x))$.

If $R[x] = B(x)$, then $R_p[x] = \phi_p(B(x))$, so by Theorem 8, $\phi_p(B(x)) = (\alpha_p(x))$, where $\alpha_p(x)$ is primitive in $R_p[x]$. But ϕ_p is an epimorphism, hence there must be $\alpha(x)$ in $B(x)$ such that $\phi_p(\alpha(x)) = \alpha_p(x)$. Hence $B(x) \subseteq (\alpha(x), p)$ and it is then immediate that $B(x) = (\alpha(x), p)$.

Conversely, suppose $B(x) = (\alpha(x), p)$ where $\phi_p(\alpha(x))$ is primitive in $R_p[x]$. Then, by Theorem 8, $\phi_p(B(x)) = R_p[x]$, hence $R[x] = B(x)$.

Case 2. $B(x)$ contains λ . Then, as in Case 1, $R[x]/b(x) \simeq R_\lambda[x]/\phi_\lambda(b(x))$. Since $R_\lambda[x]$ is commutative, any ideal in $R_\lambda[x]$ which equals $R_\lambda[x]$ must be generated by an element which is congruent to 1 . The remainder of the proof now follows as in Case 1.

Theorem 9 is non-trivial. One example of an ideal equal to $R[x]$ is $(x+i, 3)$.

Theorem 9 indicates that the maximal ideals of $R[x]$ might not have the prime elements of $R[x]$ among their generators. This is indeed the case as will be shown in the following discussion which characterizes the maximal ideals of $R[x]$.

LEMMA 1. *Let $g(x)$, not a unit, be in $Z[x]$. Then $(g(x))$ is not a maximal ideal in $R[x]$.*

Proof. Since $Z[x]$ is noetherian it must contain a maximal ideal $(f(x), p)$, where $f(x)$ is irreducible mod p and p is prime in Z , such that $(g(x))_{Z[x]} \subsetneqq (f(x), p)_{Z[x]}$. Let $\alpha(x)$ be any element in $(g(x))_{R[x]}$. Then, since $g(x)$ is in the center of $R[x]$, $\alpha(x) = g(x)\beta(x)$ for some $\beta(x)$ in $R[x]$. But $g(x) = f(x)g_1(x) + ph(x)$, where $g_1(x)$, $h(x)$ are in $Z[x]$. Hence $\alpha(x) = f(x)g_1(x)\beta(x) + ph(x)\beta(x)$ and $\alpha(x)$ is in $(f(x), p)_{R[x]}$. Thus $(g(x))_{R[x]} \subsetneqq (f(x), p)_{R[x]}$.

Case 1. $p \neq 2$. It suffices to show that $(f(x), p)_{R[x]} \neq R[x]$. Now the natural epimorphism ϕ_p will map $R[x]/(f(x), p)$ onto

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

$R_p[x]/(\phi_p(f(x)))$. By Theorem 8, since $f(x)$ is in $Z[x]$, $(\phi_p(f(x))$ is a proper ideal in $R_p[x]$. Therefore $(f(x), p)$ must be a proper ideal in $R[x]$.

Case 2. $p = 2$. Now $(f(x), 2)_{R[x]} \subseteq (f(x), \lambda)_{R[x]}$. Then, as in Case 1, it follows that $(f(x), \lambda) \neq R[x]$.

LEMMA 2. *Let* $A(x) = (\alpha_1(x), \ldots, \alpha_r(x))$ *be a proper maximal ideal in* $R[x]$. *Then* $A(x)$ *contains a non-zero integer from* Z .

Proof. Let $\alpha_l(x) = a_0^{(l)}(x) + a_1^{(l)}(x)i + a_2^{(l)}(x)j + a_3^{(l)}(x)k$, for $1 \le l \le r$. Then, by the same argument that was used in Theorem 5, $4a_0^{(l)}(x)$, $4a_1^{(l)}(x)$, $4a_2^{(l)}(x)$, $4a_3^{(l)}(x)$ are in $A(x)$ for $1 \le l \le r$. Thus $2a_0^{(l)}(x)$, $2a_1^{(l)}(x)$, $2a_2^{(l)}(x)$, $2a_3^{(l)}(x)$ are in $Z[x]$, for $1 \le l \le r$, and their greatest common divisor in $Z[x]$ must be 1 or 2 . Suppose not. Then there exists $g(x)$, not a unit, in $Z[x]$ such that $g(x)$ divides $a_m^{(l)}(x)$ for $0 \le m \le 3$ and $1 \le l \le 3$. Hence $g(x)$ divides $\alpha_l(x)$ for $1 \le l \le r$. But then $A(x) \subseteq (g(x)) \subsetneqq R[x]$. Since $A(x)$ is maximal it now follows that $A(x) = (g(x))_{R[x]}$, which is false by Lemma 1.

Since the greatest common divisor in $Z[x]$ of the $2a_m^{(l)}(x)$ is 1 or 2 , there exists $t_m^{(l)}(x)$, $1 \le l \le r$, $0 \le m \le 3$, in $Q[x]$ such that

$$2 \sum_l \sum_m a_m^{(l)}(x) t_m^{(l)}(x) = 1 \text{ or } 2 .$$

Clearing denominators in the preceeding immediately gives the desired result.

LEMMA 3. *Let* $A(x) = (\alpha_1(x), \ldots, \alpha_r(x))$ *be a proper maximal ideal in* $R[x]$. *Then* $A(x)$ *contains either*

(i) a prime integer $p \neq 2$ *from* Z *, or*

(ii) an element from R *of norm two.*

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

Proof *(i)* (showing that $A(x)$ contains some prime integer p). By Lemma 2, $A(x)$ contains a non-zero integer n . Let the prime decomposition of n in Z be $p_1 \ldots p_m$.

If p_1 is in $A(x)$ the proof is finished.

Suppose p_1 is not in $A(x)$. Since $A(x)$ is maximal it follows that $(A(x), p_1) = R[x]$. Hence there exists $\alpha(x)$ in $A(x)$ and $\beta(x)$ in $B(x)$ such that $\alpha(x) + \beta(x)p_1 = 1$. Thus

$$\alpha(x)p_2 \ldots p_m + \beta(x)n = p_2 \ldots p_m ,$$

so $p_2 \ldots p_m$ is in $A(x)$. If p_2 is in $A(x)$, the proof is finished. If not, by the same arguments as above, $p_3 \ldots p_m$ is in $A(x)$. Repeating the above argument, it must eventually follow that p_m is in $A(x)$ if $p_1, \ldots, p_{m-1}$ are not.

(ii) If the prime integer obtained in *(i)* is odd the proof is finished.

Suppose the prime integer obtained in *(i)* is 2 . Note that $2 = \lambda\bar{\lambda}$. Suppose λ is not in $A(x)$; then since $A(x)$ is maximal, $(A(x), \lambda) = R[x]$. Recalling that if λ is a left divisor it is a right divisor and vice versa, there must exist $\alpha(x)$ in $A(x)$ and $\beta(x)$ in $R[x]$ such that $\alpha(x) + \beta(x)\lambda = 1$. Thus $\alpha(x)\bar{\lambda} + \beta(x)2 = \bar{\lambda}$, so $\bar{\lambda}$ is in $A(x)$.

COROLLARY. *Let* $A(x)$ *be a proper maximal ideal in* $R[x]$. *Then* $A(x)$ *must contain a proper maximal ideal from* R .

Proof. This is immediate from Lemma 3.

Since all ideals in R generated by elements of norm two are equal it follows from this corollary that $\lambda = 1 + i$ must be in $A(x)$.

LEMMA 4. *Let* $M(x)$ *be a proper maximal ideal in* $R[x]$. *Then either*

(i) $M(x) = (a(x), p)$ *, where* p *is an odd prime in* Z *and* $a(x) \not\equiv 1 \bmod p$ *is in* $Z[x]$ *and irreducible* $\bmod p$ *; or*

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

(ii) $M(x) = (\alpha(x), \lambda)$ *, where* $N(\lambda) = 2$ *and* $\alpha(x) \not\equiv 1 \bmod \lambda$ *is irreducible* $\bmod \lambda$.

Proof. By Lemma 3, $M(x)$ contains either a prime $p \neq 2$ or $\lambda = 1 + i$.

Case 1. $M(x)$ contains a prime $p \neq 2$. Let $M(x) = (p, \alpha_1(x), \ldots, \alpha_r(x))$. Then since $(p)_{R[x]} \subseteq M(x)$, it follows that $R[x]/M(x) \cong R_p[x]/\phi_p(M(x))$, where ϕ_p is again the natural epimorphism from $R[x]$ to $R_p[x]$. Thus $\phi_p(M(x))$ is a proper ideal in $R_p[x]$. By Theorem 8, $\phi_p(M(x)) \subseteq (a_p(x))$, for some $a_p(x)$ which is irreducible in $Z_p[x]$. Hence $\phi_p(\alpha_l(x)) = a_p(x)\beta_p(x)$ for some $\beta_p(x)$ in $R_p[x]$, where $1 \leq l \leq r$. Therefore $\alpha_l(x) - a(x)\beta(x)$ must be in $(p)_{R[x]}$, $1 \leq l \leq r$, for some $\beta(x)$ in $R[x]$ and $a(x)$ irreducible in $Z_p[x]$. Thus $\alpha_l(x)$ is in $(a(x), p)$ for $1 \leq l \leq r$, and consequently $M(x) \subseteq (a(x), p) \subseteq R[x]$. But

$$R[x]/(a(x), p) \cong R_p[x]/(\phi_p(a(x))) = R_p[x]/(a_p(x)) ,$$

and $(a_p(x)) \neq R_p[x]$ so $(a(x), p) \neq R[x]$. Then, since $M(x)$ is maximal it must be that $M(x) = (a(x), p)$.

Case 2. $M(x)$ contains λ . Let $M(x) = (\lambda, \alpha_1(x), \ldots, \alpha_r(x))$. Then, as in Case 1, $\phi_\lambda(M(x)) \subseteq (\alpha_\lambda(x))$ for some $\alpha_\lambda(x)$ irreducible in $R_\lambda[x]$. Thus, since $R_\lambda[x]$ is commutative, for some $\beta_\lambda(x)$ in $R_\lambda[x]$, $\phi_\lambda(\alpha_l(x)) = \alpha_l(x)\beta_\lambda(x)$ where $1 \leq l \leq r$. The argument is now completed in a similar fashion to Case 1.

LEMMA 5. *(i) Let* p *be an odd prime and* $a(x) \not\equiv 1 \bmod p$ *be in* $Z[x]$ *and irreducible* $\bmod p$ *. Then* $M(x) = (a(x), p)$ *is a proper maximal ideal in* $R[x]$.

(ii) Let $\lambda = 1 + i$ *and* $\alpha(x) \not\equiv 1 \bmod \lambda$ *in* $R[x]$ *be irreducible* $\bmod \lambda$ *. Then* $M(x) = (\alpha(x), \lambda)$ *is a proper maximal ideal in* $R[x]$.

Proof. *(i)* Suppose $(a(x), p)$ is not a maximal ideal in $R[x]$. Since $R[x]$ is noetherian there must exist a maximal ideal $N_1(x)$ in

$R[x]$ such that $(p, a(x)) \subsetneqq N_1(x) \subsetneqq R[x]$. By Lemma 3, $N_1(x)$ must contain either an odd prime or λ . Since $N_1(x) \neq R[x]$ it is clear that $N_1(x)$ can not contain λ or any odd prime except p . Thus, by Lemma 4, $N_1(x) = (b(x), p)$, where $b(x)$, not a unit, is in $Z[x]$ and irreducible mod p.

Since $a(x)$ is in $(b(x), p) = N_1(x)$, there must exist $\alpha(x)$ and $\beta(x)$ in $R[x]$ such that $a(x) = b(x)\beta(x) + p\alpha(x)$. Hence $\phi_p(a(x)) = \phi_p(b(x)\phi_p(\beta(x)))$ in $R_p[x]$. But $a(x)$ is irreducible mod p , hence $\phi_p(a(x))$ must be irreducible in $R_p[x]$; thus $\phi_p(\beta(x))$ must be a unit in $R_p[x]$. Let $\gamma_p(x)$ be its inverse in $R_p[x]$; then since ϕ_p is an epimorphism there must be a $\gamma(x)$ in $R[x]$ such that $\phi_p(\gamma(x)) = \gamma_p(x)$. Hence $\gamma(x)a(x) - b(x)$ is in (p) in $R[x]$. Thus $b(x)$ is in $(a(x), p)$. But then $(a(x), p) = N_1(x)$, which is a contradiction.

(ii) Suppose $(a(x), \lambda)$ is not a maximal ideal in $R[x]$. Then it must be contained in a maximal ideal $N_1(x)$. By Lemma 3, $N_1(x)$ must contain either an odd prime from Z or λ . Since $N_1(x) \neq R[x]$ it is clear that $N_1(x)$ can not contain an odd prime p . Thus $N_1(x)$ must be of the form $(\beta(x), \lambda)$ where $\beta(x) \not\equiv 1 \bmod \lambda$ and $\beta(x)$ is irreducible mod λ . Hence $(\alpha(x), \lambda) \subseteq (\beta(x), \lambda)$; so $(\phi_\lambda(\alpha(x))) \subseteq (\phi_\lambda(\beta(x)))$ in $R_p[x]$. But $\alpha(x)$ is irreducible mod λ , so $(\phi_\lambda(\alpha(x)))$ is a maximal ideal in $R_\lambda[x]$; hence $(\phi_\lambda(\alpha(x))) = (\phi_\lambda(\beta(x)))$. Returning to $R[x]$ it follows that $(\alpha(x), \lambda) = (\beta(x), \lambda) = N_1(x)$, which is a contradiction.

THEOREM 10. *$M(x)$ is a proper maximal ideal in $R[x]$, if, and only if, either*

(i) $M(x) = (a(x), p)$ *, where* p *is an odd prime in* Z *and* $a(x) \not\equiv 1 \bmod p$ *in* $Z[x]$ *is irreducible* mod p *; or*

(ii) $M(x) = (\alpha(x), \lambda)$ *, where* $N(\lambda) = 2$ *and* $\alpha(x) \not\equiv 1 \bmod \lambda$ *is irreducible* mod λ .

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

Proof. Immediate by Lemmas 4 and 5.

The preceding discussion showed that the maximal ideals were not, as might be expected, generated by the prime elements of $R[x]$. The following discussion will show that the unexpected also happens in the characterization of the prime ideals. Again, as for the maximal ideals, a characterization surprisingly analogous to the situation in $Z[x]$ will be shown to occur.

LEMMA 6. *Let* $P(x)$ *be a prime ideal in* $R[x]$ *. Then* $P(x) \cap R$ *is a prime ideal in* R *.*

Proof. Suppose $P(x) \cap R$ is not a prime ideal in R . Then there exist ideals A and B in R such that $AB \subseteq P(x) \cap R$, but neither A nor B is in this intersection. Now raise the ideals A and B to $R[x]$ forming the ideals $A(x)$ and $B(x)$. Then $A(x) = (\alpha)$ and $B(x) = (\beta)$ for some α and β in R .

Let $\gamma(x)$ be any element in $A(x)B(x)$. Then

$$\gamma(x) = \left[\sum_{l=1}^{n} \gamma_l^{(1)}(x)\alpha\gamma_l^{(2)}(x)\right]\left[\sum_{h=1}^{m} \gamma_h^{(3)}(x)\beta\gamma_h^{(4)}(x)\right] ,$$

where $\gamma_l^{(1)}(x)$, $\gamma_l^{(2)}(x)$, $\gamma_h^{(3)}(x)$, $\gamma_h^{(4)}(x)$, $1 \le l \le n$, $1 \le h \le m$, are in $R[x]$. Thus $\gamma(x)$ is a polynomial with coefficients in AB . Hence $A(x)B(x) \subseteq P(x)$, which is prime. Without loss of generality, suppose $A(x) \subseteq P(x)$; then $A \subseteq A(x) \cap R \subseteq P(x) \cap R$, which is a contradiction.

LEMMA 7. *Let* m *be in* Z *,* $a(x)$ *be in* $Z[x]$ *, and* $\alpha(x)$, $\beta(x)$ *be in* $R[x]$ *. If* $m\alpha(x) = a(x)\beta(x)$ *and* $a(x)$ *is irreducible in* $Z[x]$ *, then* m *divides* $\beta(x)$ *.*

Proof. Let $a(x) = a_0 + a_1x + \ldots + a_{n_1}x^{n_1}$ in $Z[x]$, $\beta(x) = \beta_0 + \ldots + \beta_{n_2}x^{n_2}$ in $R[x]$ and $p_1 \ldots p_q$ be the prime factorization of m in Z . Since $a(x)$ is irreducible in $Z[x]$, there must exist a first coefficient, say a_s , such that p_1 does not divide a_s in Z .

Suppose p_1 does not divide $\beta(x)$ in $R[x]$. Then there exists a first coefficient, say β_t, such that p_1 does not divide β_t in R. Now the coefficient of x^{s+t} in $a(x)\beta(x)$ is

$$a_0\beta_{s+t} + a_1\beta_{s+t-1} + \dots + a_s\beta_t + \dots + a_{s+t}\beta_0 .$$

Since this coefficient is divisible by p_1 and $a_0, \dots, a_{s-1}$, $\beta_{t-1}, \dots, \beta_0$ are divisible by p_1 it follows that p_1 divides $a_s\beta_t$ in R. But since p_1 is prime and p_1 does not divide a_s, there exist c_1 and c_2 in Z such that $c_1p_1 + c_2a_s = 1$. Hence $c_1p_1\beta_t + c_2a_s\beta_t = \beta_t$, so that p divides β_t in R, which is a contradiction. Hence p_1 divides $\beta(x)$ in $R[x]$.

Suppose $\beta(x) = p_1\beta_1(x)$; then $p_2 \dots p_q\alpha(x) = a(x)\beta_1(x)$, so by the same argument as above p_2 must divide $\beta_1(x)$. Continuing in this fashion it follows that m divides $\beta(x)$.

COROLLARY. *Let p be prime in Z, $a(x)$ be in $Z[x]$ and $\alpha(x)$, $\beta(x)$ be in $R[x]$. If $p\alpha(x) = a(x)\beta(x)$ in $R[x]$ and p does not divide $a(x)$, then p divides $\beta(x)$.*

Proof. Let $a(x) = a_0 + a_1x + \dots + a_nx^n$ in $Z[x]$ and $\beta(x) = \beta_0 + \dots + \beta_mx^m$ in $R[x]$. Since p does not divide $a(x)$ there must exist a first coefficient, say a_s, such that p does not divide a_s in Z.

Now suppose p does not divide $\beta(x)$ in $R[x]$ and obtain a contradiction as in Lemma 7.

LEMMA 8. *Let $P(x)$ be a proper prime ideal in $R[x]$. Then $P(x)$ must have one of the following forms:*

(i) $(p(x))$, *where $p(x)$ is irreducible in $Z[x]$;*

(ii) (P), *where P is a prime ideal in R;*

(iii) $(a(x), p)$, *where p is an odd prime in Z and $a(x) \not\equiv 1 \bmod p$ in $Z[x]$ is irreducible* $\bmod p$;

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

(iv) $(a(x), \lambda)$ *, where* $N(\lambda) = 2$ *and* $\alpha(x) \not\equiv 1 \bmod \lambda$ *is irreducible* $\bmod \lambda$.

Proof. By Lemma 6, $P(x) \cap R$ is a prime ideal in R . Thus, by Theorem 2, there are three cases to consider.

Case 1. $P(x) \cap R = \{0\}$. First raise $P(x)$ to be an ideal in $K[x]$. Since $P(x) \cap R = \{0\}$ this must be a proper ideal in $K[x]$; so, by Theorem 5, $P(x)_{K[x]} = (a(x))$ for some $a(x)$ in $Z[x]$. Hence $a(x)$ can be written as a $K[x]$ linear combination of generators for $P(x)$. But then there exists a d in Z such that $da(x)$ can be written as an $R[x]$ linear combination of generators for $P(x)$, so that $da(x)$ is in $P(x)$. Since d and $a(x)$ are in the center of $R[x]$ it follows that the ideal product $(d)(a(x))$ is in $P(x)$. But $P(x)$ is prime and $P(x) \cap R = \{0\}$; therefore $(a(x)) \subseteq P(x)$.

Let $a_1(x) \ldots a_n(x)$ be the prime factorization of $a(x)$ in $Z[x]$. Then one of the ideals $(a_l(x))$, $1 \le l \le n$, must be in $P(x)$. Without loss of generality, suppose $(a_1(x)) \subseteq P(x)$. Then it remains to show that $P(x) \subseteq (a_1(x))$. Suppose the generators of $P(x)$ are $\alpha_1(x), \ldots, \alpha_r(x)$. Since $P(x)_{K[x]} = (a(x)) = (a_1(x) \ldots a_n(x))_{K[x]}$ it follows that there exist integers $m_1, \ldots, m_r$ in Z such that $m_h\alpha_h(x) = a_1(x)\beta_h(x)$, $1 \le h \le r$, where $\beta_h(x)$ is in $R[x]$ and $a_1(x)$ is irreducible in $Z[x]$. By Lemma 7, m_l divides $\beta_h(x)$ in $R[x]$ for $1 \le h \le r$. Thus $\alpha_h(x)$, $1 \le h \le r$, is in the ideal $(a_1(x))$ in $R[x]$; so $P(x) \subseteq (a_1(x))$.

Hence $P(x) = (a_1(x))$, where $a_1(x)$ is irreducible in $Z[x]$.

Case 2. $P(x) \cap R = P$, where $P \ne \{0\}$ is a proper prime ideal in R .

(i) $P = (p)$ where p is an odd prime in Z . The first step is to show that $\phi_p(P(x))$ is a prime ideal in $R_p[x]$. Let $(a_p(x))$ and $(b_p(x))$ be proper ideals in $R_p[x]$ such that $(a_p(x))(b_p(x)) \subseteq \phi_p(P(x))$. Then $a_p(x)b_p(x)$ is in $\phi_p(P(x))$, so that $a_p(x)b_p(x) + \alpha(x)p$ is in

$P(x)$ for some $\alpha(x)$ in $R[x]$. But p is in $P(x)$, so $a_p(x)b_p(x)$ must be in $P(x)$. Since $a_p(x)$ and $b_p(x)$ are both in the center of $R[x]$ and $P(x)$ is prime it must be that $a_p(x)$ or $b_p(x)$ is in $P(x)$. Hence $(a_p(x))$ or $(b_p(x))$ must be in $\phi_p(P(x))$ and thus $\phi_p(P(x))$ is a prime ideal in $R_p[x]$.

By the above the prime ideals in $R[x]$ containing p must lie among the inverse images with respect to ϕ_p of the prime ideals in $R_p[x]$. But the only ideals in $R[x]$ which contain p and are among these inverse images are (p) and $(a(x), p)$, where $a(x)$ is in $Z[x]$ and irreducible mod p.

(ii) $P = (\lambda)$ where $N(\lambda) = 2$. Then, since λ is in $P(x)$, the isomorphism $R[x]/P(x) \cong R_\lambda[x]/\phi_\lambda(P(x))$ holds. But $R_\lambda[x]$ is a commutative ring; thus $P(x)$ is a prime ideal in $R[x]$, if, and only if, $\phi_\lambda(P(x))$ is a prime ideal in $R_p[x]$. Thus the prime ideals in $R[x]$ containing λ must be among the inverse images with respect to ϕ_λ of the prime ideals in $R_\lambda[x]$. Consequently, the only possibilities are (λ) and $(\alpha(x), \lambda)$, where $\alpha(x)$ in $R[x]$ is irreducible mod λ.

Case 3. $P(x) \cap R = R$. If this is true, then 1 is in $P(x)$ which is impossible.

LEMMA 9. *(i) Let p be an odd prime in Z and $a(x) \not\equiv 1 \bmod p$ in $Z[x]$ be irreducible* mod p. *Then $(a(x), p)$ is a proper prime ideal in* $R[x]$.

(ii) Let $N(\lambda) = 2$ and $\alpha(x)$ in $R[x]$ be irreducible mod λ. *Then $(\alpha(x), \lambda)$ is a proper prime ideal in $R[x]$.*

Proof. *(i)* Let $C(x)$ and $B(x)$ be two ideals in $R[x]$ such that $C(x)B(x) \subseteq (a(x), p)$. Then

$$\phi_p(C(x))\phi_p(B(x)) \subseteq \phi_p(a(x), p) = \phi_p(a(x)) = A_p(x),$$

say. By Theorem 8, $A_p(x)$ is a prime ideal in $R_p[x]$. Without loss of generality $\phi_p(B(x)) \subseteq A_p(x)$. Then

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

$$B(x) \subseteq \phi_p^{-1}\phi_p\big(B(x)\big) \subseteq \phi_p^{-1}\big(A_p(x)\big) \subseteq \big(a(x), p\big) ,$$

for, by Theorem 10, $\big(a(x), p\big)$ is a maximal ideal. Thus $\big(a(x), p\big)$ is a prime ideal.

(ii) Follows by the same argument as was used in *(i)*.

LEMMA 10. *(i) Let* p *be an odd prime in* Z *. Then* (p) *is a proper prime ideal in* $R[x]$ *.*

(ii) Let $N(\lambda) = 2$ *. Then* (λ) *is a proper prime ideal in* $R[x]$ *.*

Proof. *(i)* Let $A(x)$ and $B(x)$ be two ideals in $R[x]$ such that $A(x)B(x) \subseteq (p)$. Then, in $R_p[x]$, $\phi_p\big(A(x)\big)\phi_p\big(B(x)\big) \subseteq (0)$.

Case 1. At least one of $\phi_p\big(A(x)\big)$ or $\phi_p\big(B(x)\big)$ is (0) . Without loss of generality suppose it is $\phi_p\big(A(x)\big)$. Then

$A(x) \subseteq \phi_p^{-1}\big(\phi_p\big(A(x)\big)\big) \subseteq (p)$ and the proof is complete.

Case 2. $\phi_p\big(A(x)\big)$ and $\phi_p\big(B(x)\big)$ are both proper ideals in $R_p[x]$. By Theorem 8, there exist $a_p(x)$ and $b_p(x)$ in $Z_p[x]$ such that $\phi_p\big(A(x)\big) = \big(a_p(x)\big)$ and $\phi_p\big(B(x)\big) = \big(b_p(x)\big)$. Then, since $\big(a_p(x)\big)\big(b_p(x)\big) \subseteq (0)$, p must divide $a_p(x)b_p(x)$ in $Z[x]$. Consequently, without loss of generality, p divides $a_p(x)$ in $Z[x]$. Thus $\big(a_p(x)\big) = (0)$; so $A(x) \subseteq \phi_p^{-1}\big(\phi_p\big(A(x)\big)\big) \subseteq (p)$ and the proof is complete.

Case 3. Either $\phi_p\big(A(x)\big)$ or $\phi_p\big(B(x)\big)$ is $R_p[x]$. Without loss of generality, suppose $\phi_p\big(A(x)\big) = R_p[x]$. Then, by Theorem 8, it must be generated by a primitive element in $R_p[x]$. Thus the generator of $\phi_p\big(B(x)\big)$ must be divisible by p ; so $\phi_p\big(B(x)\big) = (0)$, and again the proof is complete.

(ii) Let $A(x)$ and $B(x)$ be two ideals in $R[x]$ such that $A(x)B(x) \subseteq (\lambda)$. Then $\phi_\lambda\big(A(x)\big)\phi_\lambda\big(B(x)\big) \subseteq (0)$ in $R_\lambda[x]$. Since $R_\lambda[x]$ is a commutative integral domain it follows, without loss of generality,

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

that $\phi_\lambda(A(x)) \subseteq (0)$. Thus $A(x) \subseteq \phi_\lambda^{-1}\phi_\lambda(A(x)) \subseteq (\lambda)$, and the proof is complete.

LEMMA 11. *Let* $p(x)$ *, not equal to a constant, be irreducible in* $Z[x]$ *. Then* $(p(x))$ *is a prime ideal in* $R[x]$ *.*

Proof. Let $A(x)$ and $B(x)$ be ideals in $R[x]$ such that $A(x)B(x) \subseteq (p(x))$. Then, lifting each of these ideals to $K[x]$, it follows that $A(x)_{K[x]}B(x)_{K[x]} \subseteq (p(x))_{K[x]}$. By Theorem 6, $(p(x))_{K[x]}$ is a prime ideal in $K[x]$. Without loss of generality, suppose $A(x)_{K[x]} \subseteq (p(x))_{K[x]}$.

Let $\alpha_1(x), \ldots, \alpha_r(x)$ be the generators of $A(x)$ in $R[x]$. Then $\alpha_l(x) = p(x)\rho_l(x)$, $1 \le l \le r$, $\rho_l(x)$ in $K[x]$; so $m_l\alpha_l(x) = p(x)\beta_l(x)$, $1 \le l \le r$, $\beta_l(x)$ in $R[x]$, and m_l in Z . Hence, by Lemma 7, m_l divides $\beta_l(x)$ in $R[x]$ for $1 \le l \le r$. Thus $\alpha_l(x)$ is in $(p(x))$ for $1 \le l \le r$. Hence $A(x) \subseteq (p(x))$ and $(p(x))$ is a prime ideal in $R[x]$.

THEOREM 11. $P(x)$ *is a proper prime ideal in* $R[x]$ *, if, and only if, one of the following is true:*

(i) $P(x) = (p(x))$ *, where* $p(x)$ *, not a unit, is irreducible in* $Z[x]$ *;*

(ii) $P(x) = (P)$ *, where* P *is a proper prime ideal in* R *;*

(iii) $P(x) = (a(x), p)$ *, where* p *is an odd prime in* Z *and* $a(x) \not\equiv 1 \bmod p$ *in* $Z[x]$ *is irreducible* $\bmod p$ *;*

(iv) $P(x) = (\alpha(x), \lambda)$ *, where* $N(\lambda) = 2$ *and* $\alpha(x) \not\equiv 1 \bmod \lambda$ *is in* $R[x]$ *and irreducible* $\bmod \lambda$ *.*

Proof. This is immediate from Lemmas 8 through 11.

D. A Szekeres type basis for the ideals of $R[x]$

DEFINITION. Let $A(x)$ be an ideal in $R[x]$. $A(x)$ is a *primitive ideal* if there does not exist an ideal $(a(x))$, where $a(x)$ is in $Z[x]$ or $N(a(x)) = 2$, such that $A(x) \subseteq (a(x)) \subsetneq R[x]$.

Let $\alpha(x)$ be an element in $R[x]$. Then

$$2\alpha(x) = a_0(x) + a_1(x)i + a_2(x)j + a_3(x)k$$

for some $a_0(x)$, $a_1(x)$, $a_2(x)$, $a_3(x)$ in $Z[x]$. Let $a(x)$ be the greatest common divisor of $a_0(x), \ldots, a_3(x)$ in $Z[x]$. Then

$$2\alpha(x) = a(x)\left(b_0(x)+b_1(x)i+b_2(x)j+b_3(x)k\right) = a(x)\beta(x) ,$$

where $\beta(x)$ is in $R[x]$, its coordinates are in $Z[x]$, and have no common divisor there. Then there are two possibilities:

(i) two divides $a(x)$ in $Z[x]$; then, clearly, $\frac{a(x)}{2}$ is the largest element in $Z[x]$ which divides $\alpha(x)$ in $R[x]$;

(ii) two does not divide $a(x)$ in $Z[x]$; then, by the corollary to Lemma 7, two must divide $\beta(x)$ in $R[x]$. Hence, $a(x)$ is the largest element in $Z[x]$ which divides $\alpha(x)$ in $R[x]$.

Now let $B(x) = \left(\beta_1(x), \ldots, \beta_s(x)\right)$ be any ideal in $R[x]$. By the preceding paragraph, for each $\beta(x)$, $1 \le l \le s$, there is a greatest $a_l(x)$ in $Z[x]$ such that $\beta_l(x) = a_l(x)\gamma_l(x)$, $\gamma_l(x)$ in $R[x]$. Now let $a(x)$ be the greatest common divisor of the $a_l(x)$, $1 \le l \le s$, in $Z[x]$. Then

$$B(x) = \left(a(x)\right)\left(\gamma_1(x), \ldots, \gamma_s(x)\right) .$$

Let $\gamma_l(x) = \gamma_0^{(l)} + \gamma_1^{(l)}x + \ldots + \gamma_{m_l}^{(l)}x^{m_l}$, $1 \le l \le s$. Factor from the $\gamma_h^{(l)}$, $1 \le l \le s$, $0 \le h \le m_l$, all common factors λ in R with norm two. Let $\gamma_l(x) = \lambda_1 \ldots \lambda_t\alpha_l(x)$, $1 \le l \le s$, and $N(\lambda_1) = \ldots = N(\lambda_t) = 2$. Then

$$B(x) = \left(a(x)\right)\left(\lambda_1\right) \ldots \left(\lambda_t\right)\left(\alpha_1(x), \ldots, \alpha_s(x)\right) = \left(a(x)\right)(\lambda)^t A(x) ,$$

where t is a non-negative integer and $A(x) = \left(\alpha_1(x), \ldots, \alpha_s(x)\right)$. Then $A(x)$ is a primitive ideal in $R[x]$.

Thus, in order to characterize all the ideals in the ring $R[x]$, it is sufficient to characterize the primitive ideals. This will be done by adapting a proof by Szekeres [3].

LEMMA 12. *Let* $A(x)$ *be a primitive ideal in* $R[x]$. *Then* $A(x)$ *contains a non zero integer from* Z .

Proof. Let $A(x) = (\alpha_1(x), \ldots, \alpha_r(x))$ where

$$\alpha_l(x) = a_0^{(l)}(x) + a_1^{(l)}(x)i + a_2^{(l)}(x)j + a_3^{(l)}(x)k$$

for $1 \le l \le r$. Then, by the same argument as in Theorem 5, $4a_m^{(l)}(x)$, $1 \le l \le r$, $0 \le m \le 3$, are in $A(x) \cap Z[x]$. Moreover, since $A(x)$ is primitive, the greatest common divisor in $Z[x]$ of these elements must be 2 or 4 . Thus, there exist $h_m^{(l)}(x)$, $1 \le l \le r$, $0 \le m \le 3$, in $Q[x]$ such that $4\sum_l \sum_m a_m^{(l)}(x)h_m^{(l)}(x)$ is 2 or 4 . Clearing denominators, it follows that

$$\sum_l \sum_m 4a_m^{(l)}(x)k_m^{(l)}(x) = k \neq 0$$

in Z , where the $k_m^{(l)}(x)$, $1 \le l \le r$, $0 \le m \le 3$, are in $Z[x]$. Hence k is in $A(x)$.

DEFINITION. Let α and β be in R . Then α is *equivalent* to β $(\alpha \sim \beta)$, if, and only if, $(\alpha) = (\beta)$.

In each equivalence class of R defined above choose a certain element. This will be called a *normed* element of R .

Now the only proper ideals in R are of the form $(m\lambda^t)$ where m is non negative in Z , $N(\lambda) = 2$, and $t = 0$ or 1 . Thus one complete representative set of the normed R is

$$N = \{0, 1, 2, \ldots, \lambda, 2\lambda, 3\lambda, \ldots\} .$$

For convenience let $\overline{N} = \{0, 1, 2, \ldots, \overline{\lambda}, 2\overline{\lambda}, 3\overline{\lambda}, \ldots\}$.

LEMMA 13. *Let* $A \subseteq B$ *be ideals in* R *and* $A = (\gamma_1)$, *where* γ_1 *is given in* $N \cup \overline{N}$. *Then there exists a* γ_2 *in* $N \cup \overline{N}$ *such that* $B = (\gamma_2)$

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

and $\gamma_1 = \alpha\gamma_2$ *where* α *is in* N .

Proof. Clearly γ_2 can be chosen in $N \cup \overline{N}$ so that $B = (\gamma_2)$ and γ_2 can be either of the form $m_2\lambda^{t_2}$ or $m_2\overline{\lambda}^{t_2}$. It just remains to show that given γ_1 and the fact that $\gamma_1 = \alpha_1 m_2\lambda^{t_2} = \alpha_2 m_2\overline{\gamma}^{t_2}$, at least one of the α_1 or α_2 is in N .

Case 1. γ_1 is in N . Let $\gamma_1 = m_1\gamma_1^{t_1} = \alpha_1 m_2\lambda^{t_2} = \alpha_2 m_2\overline{\lambda}^{t_2}$.

(i) $t_1 = t_2 = 0$. Then $m_1 = \alpha_1 m_2$, so $m_1^2 = N(\alpha_1)m_2^2$ in Z and m_2 must divide m_1 . Thus α_1 is in N for $\gamma_2 = m_2$.

(ii) $t_1 = 0$, $t_2 = 1$. Then $m_1 = \alpha_2 m_2\overline{\lambda}$, so $m_1^2 = 2N(\alpha_2)m_2^2$ in A . Thus $m_1 = km_2$ for some k in Z ; hence $k^2 = N(\alpha_2)2$, so k must be even. Let $k = 2k_1$. Then $2k_1 = \alpha_2\overline{\lambda}$, so $k_1\lambda = \alpha_2$; that is, α_2 is in N if $\gamma_2 = m_2\overline{\lambda}$.

(iii) $t_1 = 1$, $t_2 = 0$. Then $m_1\lambda = \alpha_1 m_2$; so $2m_2^2 = N(\alpha_1)m_2^2$ in A . Hence m_2 divides m_1 in Z . Thus α_1 is in N if $\gamma_2 = m_2$.

(iv) $t_1 = t_2 = 1$. Then $m_1\lambda = \alpha_1 m_2\lambda$; so $m_1 = \alpha_1 m_2$ and the proof is as in (i).

Case 2. γ_1 is in $\overline{N}$. Let $\gamma_1 = m_1\overline{\lambda}_1^{t_1}$. Then the same type of argument that was used in Case 1 holds.

Let $R(\alpha)$ be the system of representatives containing the element 0 , of the residue classes mod α , for an element α in N .

THEOREM 12. *Let* $A(x)$ *be a primitive ideal in* $R[x]$. *Then* $A(x) = (\alpha_0(x), \ldots, \alpha_m(x))$, *where*

(i) $\alpha_0(x) = \alpha_1 \ldots \alpha_m$,

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

$$\alpha_l\alpha_l(x) = x\alpha_{l-1} + \sum_{h=1}^{l} \beta_{hl}\alpha_{h-1}(x) , \quad 1 \le l \le m ;$$

(ii) $\alpha_1, \ldots, \alpha_m$ *are in* N *,* $\alpha_l \ne 0$ *, and* $\alpha_m \ne 1$ *;*

(iii) $\beta_{1l}, \ldots, \beta_{ll}$ *are in* $R(\alpha_l)$ *for* $1 \le l \le m$ *.*

Proof I (showing that $\alpha_0(x), \ldots, \alpha_m(x)$ are in $R[x]$). Obviously $\alpha_0(x)$ is in $R[x]$.

(i)
$$\begin{aligned}\alpha_1\alpha_1(x) &= x\alpha_0(x) + \beta_{11}\alpha_0(x)\\ &= (x+\beta_{11})\alpha_1 \ldots \alpha_m\\ &= \alpha_1(x+\beta'_{11})\alpha_2 \ldots \alpha_m ,\end{aligned}$$

where β'_{11} is in R . Thus $\alpha_1(x) = (x+\beta'_{11})\alpha_2 \ldots \alpha_m$ and is in $R[x]$. Moreover $\alpha_1(x)$ has leading coefficient $\alpha_2 \ldots \alpha_m$.

(ii)
$$\begin{aligned}\alpha_2\alpha_2(x) &= x\alpha_1(x) + \beta_{12}\alpha_0(x) + \beta_{22}\alpha_1(x)\\ &= (x+\beta_{22})(x+\beta'_{11})\alpha_2 \ldots \alpha_m + \beta_{12}\alpha_1 \ldots \alpha_m\\ &= \alpha_2(x+\beta'_{22})(x+\beta''_{11})\alpha_3 \ldots \alpha_m + \alpha_2\beta'_{12}\alpha'_1\alpha_3 \ldots \alpha_m ,\end{aligned}$$

where $\beta'_{22}, \beta''_{11}, \beta'_{12}, \alpha'_1$ are in R . Thus $\alpha_2(x)$ is in $R[x]$ and has leading coefficient $\alpha_3 \ldots \alpha_m$.

(iii) Continuing in this fashion it follows that $\alpha_0(x), \ldots, \alpha_m(x)$ are in $R[x]$. The leading coefficient of $\alpha_l(x)$, $1 \le l \le m$, is $\alpha_{l+1} \ldots \alpha_m$ and the leading coefficient of $\alpha_m(x)$ is 1 .

II (showing that $(\alpha_0(x), \ldots, \alpha_m(x))$ is indeed a primitive ideal). Since $\alpha_m(x)$ has leading coefficient 1 and $\alpha_0(x)$ is a constant other than zero it is obvious that for $m > 0$, the ideal $(\alpha_0(x), \ldots, \alpha_m(x))$ is primitive. For $m = 0$, the polynomial sequence $\alpha_0(x), \ldots, \alpha_m(x)$ is reduced to $\alpha_0(x) = 1$; so $(\alpha_0(x), \ldots, \alpha_m(x))$ is again primitive.

III. Let $M_l(x)$ be the two-sided R-module consisting of those elements of $A(x)$ whose degree is at most l . Then

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

$$M_0(x) \subseteq M_1(x) \subseteq M_2(x) \subseteq \ldots .$$

Furthermore, the leading coefficients of the elements of $M_l(x)$ form an ideal $M_l = (\gamma_l)$ in R. By Lemma 12, $M_0 \neq \{0\}$; thus

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

is a non-trivial chain.

IV. Since $R[x]$ is a noetherian ring, $A(x)$ is finitely generated. Consequently, there is a minimal l for which $A(x)$ is generated by the elements of $M_l(x)$. Denote this l by $m(A(x)) = m$.

V. Now choose, in one way or another, from among each of the $M_0(x), \ldots, M_m(x)$ a polynomial $\alpha_l(x) = \gamma_l x^l + \ldots$, $0 \leq l \leq m$. Then, for each element $\alpha(x)$ of $M_l(x)$, $l > 0$, since its leading coefficient is in M_l which is principal, there is an α in R for which $\alpha(x) = \alpha\alpha_l(x)$ lies in $M_{l-1}(x)$. Then, since the degrees of $\alpha_l(x), \ldots, \alpha_0(x)$ are descending, it follows by induction that $\alpha_0(x), \ldots, \alpha_l(x)$ constitute a left R-basis of the R-module $M_l(x)$. Moreover, by definition of m,

$$A(x) = (\alpha_0(x), \ldots, \alpha_m(x)) .$$

VI. By III, $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$. Each of these ideals is principal in R and the generator γ_0 of M_0 can be taken in N. Then, by Lemma 13, there exists γ_1 in $N \cup \overline{N}$ such that $M_1 = (\gamma_1)$ and $\gamma_0 = \alpha_1\gamma_1$ where α_1 is in N. Continuing up this ideal chain applying Lemma 13, it follows that there exist elements $\alpha_1, \ldots, \alpha_m \neq 0$ in N such that

$$\alpha_{l-1} = \alpha_l\gamma_l , \quad 1 \leq l \leq m .$$

VII. By VI, $\alpha_l\gamma = \gamma_{l-1}$ for $1 \leq l \leq m$. Hence $\alpha_{l+1} \cdots \alpha_m = \gamma_l$ for $1 \leq l \leq m$. Thus, $\alpha_l\alpha_l(x) - x\alpha_{l-1}(x)$ is in $M_{l-1}(x)$ for $1 \leq l \leq m$. Hence, there exist β_{hl}, $1 \leq h \leq l$, $1 \leq l \leq m$, in R

such that

$$\alpha_l \alpha_l(x) = x\alpha_{l-1}(x) + \sum_{h=1}^{l} \beta_{hl}\alpha_{h-1}(x) \quad \text{for} \quad 1 \le l \le m ,$$

and $\alpha_0(x) = \alpha_1 \ldots \alpha_m \alpha_m$.

Now, using the formulations for $\alpha_0(x), \ldots, \alpha_m(x)$ in I, it follows that γ_m divides $\alpha_0(x), \ldots, \alpha_m(x)$. But γ_m is in $N \cup \bar{N}$ and $\alpha_0(x), \ldots, \alpha_m(x)$ generate $A(x)$ which is primitive. Thus $\gamma_m = 1$.

VIII (showing that $\alpha_m \ne 1$). If $\alpha_m = 1$ (thus $m > 0$) it would follow from VII that $\alpha_m(x)$ is contained in the ideal generated by $\alpha_0(x), \ldots, \alpha_{m-1}(x)$. But then this ideal would be equal to $A(x)$, contradicting the definition of $m(A(x)) = m$ in IV.

IX (showing that $\beta_{1l}, \ldots, \beta_{ll}$ are in (α_l) for $1 \le l \le m$). Clearly this condition holds for $\alpha_0(x)$. Now continue by induction. Suppose that for some r , $1 \le r \le m$, the $\alpha_0(x), \ldots, \alpha_{r-1}(x)$ have been chosen as in V so that the coefficients β_{hl} , $1 \le h \le l$, $1 \le l \le r-1$, satisfy condition *(iii)*.

Let $\alpha_r^*(x)$ be any polynomial in $A(x)$ which might replace $\alpha_r(x)$. Then $\alpha_r^*(x)$ and $\alpha_r(x)$ have the same leading coefficient $\alpha_{r+1} \ldots \alpha_m$. Thus, since $\alpha_r^*(x)$ is in $M_r(x)$, there exist $\delta_0, \ldots, \delta_{r-1}$ in R such that

$$\alpha_r^*(x) = \alpha_r(x) + \delta_{r-1}\alpha_{r-1}(x) + \ldots + \delta_0\alpha_0(x) .$$

From this it follows that

$$\alpha_r\alpha_r^*(x) = x\alpha_{r-1}(x) + \sum_{l=1}^{r} (\beta_{lr}+\alpha_r\delta_{l-1})\alpha_{l-1}(x) .$$

Thus $\beta_{lr}^* = \beta_{lr} + \alpha_r\delta_{l-1}$, $1 \le l \le r$, and condition *(iii)* is satisfied.

https://doi.org/10.1017/S0004972700024849 Published online by Cambridge University Press

References

[1] Adolf Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen* (Julius Springer, Berlin, 1919).

[2] L. Redéi, *Algebra*, Volume 1 (International Series of Monographs in Pure and Applied Mathematics, 91. Pergamon, Oxford, London, Edinburgh, New York, Toronto, Sydney, Paris, Braunschweig; Akadémiai Kiadó, Hungary; 1967).

[3] G. Szekeres, "A canonical basis for the ideals of a polynomial domain", *Amer. Math. Monthly* 59 (1952), 379-386.

Department of Mathematics,
Pennsylvania State University,
University Park,
Pennsylvania,
USA.